



This manual links to Logix 5000 Controller and I/O Fault Codes and Syslog Messages, [1756-RD001](#); download the spreadsheet now for offline access.



Redundancy Systems

GuardLogix 5580 Controllers

ControlLogix 5580 Controllers

ControlLogix 5570 Controllers



Allen-Bradley

by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.



Identifies information that is useful and can help to make a process easier to do or easier to understand.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

	Preface	11
	About This Publication	11
	Summary of Changes	11
	Additional Resources	12
	 Chapter 1	
Redundancy Systems	High Availability	13
	Logix SIS Redundancy	13
	ControlLogix 5580 Redundancy	14
	ControlLogix 5570 Redundancy	15
	Feature Support	16
	Restrictions	17
	Security Considerations	18
	Redundancy Module MicroSD Card Security	18
	 Chapter 2	
System Components	Redundant Chassis Pair	19
	Redundant Chassis Requirements	19
	Power Supply Requirements	20
	Redundant Controller Requirements	20
	Redundancy Module Requirements	22
	Communication Module Requirements	23
	I/O Modules	25
	Supported Networks	25
	HMI	26
	Optional Software	26
	Other Communication Networks	27
	 Chapter 3	
Logix SIS Redundancy Operation	SIL 2 and SIL 3 Safety Functions	29
	System Qualification and Synchronization	29
	Operation After a Fault	30
	Concurrent Communication to I/O	30
	 Chapter 4	
ControlLogix Redundancy Operation	System Qualification and Synchronization	31
	Possible Communication Delays During Qualification	31
	Synchronization and Fiber Channels	32
	Controller Switchovers	32
	Causes of a Switchover	32
	Operation After a Controller Switchover	32
	Possible Communication Delays During a Switchover	33
	Reduce Data Server Recovery Time	33
	Switchover Response to Keyswitch Mismatch	33

	Fiber Channel Operation	34
	Causes of a Fiber Channel Failure	34
	Operation After a Fiber Channel Switchover in 1756-RM2 Modules	34
	Identify Installed SFP Transceivers	34
	Chapter 5	
Set Up a Redundancy System	Before You Begin	37
	Download Redundancy Firmware	38
	Install Redundancy Firmware	38
	Obtain the Redundancy Module Configuration Tool	39
	Install the RMCT	39
	Access the RMCT	40
	Configuration Requirements for Access to FactoryTalk Linx RMCT	40
	Identify the RMCT Version	41
	Install Redundant Chassis Components	42
	Convert a Standalone Chassis to a Redundant Chassis Pair	42
	Update Firmware	42
	Identify the Primary and Secondary Chassis	43
	Verify Qualification and Synchronization	44
	Download Your Application to the Primary Controller	44
	Reset a Redundancy Module	45
	Remove a Redundant Module	45
	Replace a Redundant Module	45
	Chapter 6	
Configure Redundancy Modules	Protection Mode	47
	Implicit Protection Mode	47
	Restrictions in Implicit Protection Mode	47
	Enter Redundancy Module Identification Information	48
	Configure Redundancy Module Options	48
	Choose an Auto-synchronization Setting	49
	Assign a Chassis ID	50
	Configure User Program Control	50
	(1756-RM3 Modules Only) Configure Fiber Security	50
	Set the Redundancy Module Date and Time	51
	(1756-RM3 Modules Only) Set the Date and Time via Time Synchronization	51
	Set the Date and Time via the RMCT	52
	Set the Date and Time via an MSG Instruction	53
	(1756-RM3 Modules Only) Reset Factory Defaults	54
	(1756-RM3 Modules Only) Disable or Re-enable SFP Fiber Ports	55
	Chapter 7	
Configure the EtherNet/IP Network	Requested Packet Interval (RPI)	57
	1756-EN4TR Module Considerations	57
	1756-EN2T Module Considerations	57
	Concurrent Communication	58
	System Requirements	58
	Configuration Requirements	59

Produced and Consumed Tags	60
Produced and Consumed Tags between Primary and Non-redundant Controllers	61
Static Versus Dynamic IP Addresses	62
IP Address Swapping	62
Determine Whether to Use IP Address Swapping	63
Set Communication Module IP Addresses	63
Reset an IP Address	64
Half/Full Duplex Settings	64
Device Level Ring (DLR)	64
Use DLR in a Redundancy System	64
Parallel Redundancy Protocol (PRP)	65
Use PRP in a Redundancy System	65
CIP Sync Time Synchronization	65
Use Time Synchronization in a Redundancy System	65

Chapter 8

Configure the Redundant Controller

Enable Time Synchronization	69
Crossloads, Synchronization, and Switchovers for Standard Tasks	71
Configure Crossload and Synchronization Settings	71
Standard Task Settings	71
Program Settings	75
Default Settings	75
Recommended Task Types	75
Continuous Task After Switchover	76
Continuous Task with Crossloads at Each Program End	76
Continuous Task with Various Crossloads at Program End	76
Multiple Periodic Tasks	77
Crossloads and Scan Time for Standard Tasks	79
Redundancy Object Attributes for Crossload Time	79
Estimate Crossload Time per Sync Point	80
Watchdog Time for the Safety Task	81
Watchdog Time for Standard Tasks	81
Set Minimum Values for Standard Task Watchdog Time	82

Chapter 9

Programming Best Practices for Standard Tasks

Program to Minimize Scan Times	83
Minimize the Number of Programs	83
Manage Tags for Efficient Crossloads	84
Use Concise Programming	86
(ControlLogix 5570 Only) Use Multiple Controllers	87
Program to Maintain Data Integrity	87
Timer Instructions	87
Array (File)/Shift Instructions	87
Scan-dependent Logic	88
(ControlLogix 5570 Only) Align LINT Members on 8-byte Boundaries	89
Optimize Tasks	92
ControlLogix 5570 Considerations	93

Programming Considerations 96
 Data Transfer 96
 SSV Instruction Operation 96
 Communication Performance 96
 Program-scoped Tags 97
 Instruction Operation 97
 Alarms 97
 Diagnostics 98
 Conduct a Test Switchover 98
 Synchronization After a Switchover 98
 Program Logic to Run After a Switchover 99
 Download the Project 99
 Store a Redundancy Project to Nonvolatile Memory 100
 Store a Project with Controller in Program or Remote Program Mode 100
 Store a Project While a System is Running 101
 Load a Project 101
 Online Edits 102
 Partial Import Online (PIO) 102
 Plan for Test Edits 102
 Assemble Edits with Caution 103
 (ControlLogix 5570 Only) Reserve Memory for Tags and Logic 105
 Calculate RPI Timeout for Standard I/O 106

Initiate Redundancy and System Update Commands

Chapter 10

Initiate Redundancy Commands in the RMCT 107
 Synchronize Secondary 107
 Disqualify Secondary 108
 Initiate Switchover 108
 Become Primary 108
 Initiate Redundancy Commands with MSG Instructions 109
 MSG Instruction Behavior During Qualification and Switchover 111
 Initiate System Update Commands in the RMCT 112
 Lock for Update 112
 Abort System Lock 113
 Initiate a Locked Switchover 113

Monitor and Maintain a Redundancy System

Chapter 11

Reference the Controller Log 115
 Redundancy System Considerations 115
 Track Changes to Components 115
 Use Logic to Monitor Status 116
 Get System Value Instruction 116
 Redundancy Status Bit 117
 (1756-RM2 and 1756-RM Modules Only). Get Attribute Message for Fiber Channel Status 117
 Monitor Communication Module Statistics 118
 CPU Usage 118
 Connections Used 118
 Understand Temperature Monitoring and Fault Behavior 119

Troubleshoot Systems with 1756-RM3 Modules

Chapter 12

View Diagnostic Information in the Logix Designer Application	121
View the Synchronization Log	122
View Module-level Synchronization Status	123
View the Lock for Update Logs	124
View, Save, and Export the Event Log	125
Event Classes	126
Event Log Examples	126
Save System History	128
Export Tech Support Logs	129
Redundancy Module Faults	130
Clear a Fault	131
Redundant Controller Major Fault Messages	131

Troubleshoot Systems with 1756-RM2 Modules

Chapter 13

View Diagnostic Information in the Logix Designer Application	133
View Recent Synchronization Attempts	134
View Module-level Synchronization Status	136
View the Event Log	137
Controller Events	138
Event Classifications	138
Access Extended Information about an Event	140
Interpret Extended Information for an Event	140
Interpret Event Log Information	141
Export Event Log Data	143
Export Diagnostics	145
Contact Rockwell Automation Technical Support	147
Clear a Fault	147
View System Update Logs	148
System Update Lock Attempts	148
Locked Switchover Attempts	149
View System Event History	150
Edit a User Comment for a System Event	151
Save System Event History	151
Event Examples	152
Identify a Lost Partner Network Connection	153
Identify a Lost Redundancy Module Connection	155
Redundancy Module Missing	155
Qualification Failure Caused by Non-redundant Controller	156
Redundancy Module Faults	158
Event Log	158
Module Status Display	159
Recovery Messages	159
Redundant Controller Major Fault Messages	160

Online Firmware Updates	Chapter 14	
	Logix SIS Considerations	161
	Before You Begin	162
	Verify the RMCT Version	162
	Prepare the Controller Project for the Update	162
	Update the Redundancy System Firmware	164
	Prepare the Redundant Chassis for the Firmware Update	165
	Update the Redundancy Module Firmware in the Secondary Chassis	165
	Update the Redundancy Module Firmware in the Primary Chassis	166
	Update Other Module Firmware in the Secondary Chassis	166
	Download the Project to the Secondary Controller	166
	Lock the System for Update and Initiate a Locked Switchover	167
	Update Other Module Firmware in the New Secondary Chassis	168
	Synchronize the Redundant Chassis Pair	168
	EDS Files	169
Status Indicators	Appendix A	
	1756-RM3 Status Indicators	171
	1756-RM2 Status Indicators	173
	1756-RM Status Indicators	175
Redundancy Object Attributes	Appendix B179
Redundancy System Checklists	Appendix C	
	Chassis Configuration Checklist	181
	Remote I/O Checklist	181
	Redundancy Module Checklist	181
	Controller Checklist	181
	EtherNet/IP Checklist	182
	ControlNet Checklist for ControlLogix 5570 Redundancy	182
	Project and Programming Checklist	183
Module Replacement	Appendix D	
	Perform a Direct Module Replacement in the Secondary Chassis	185
	Replace Communication Modules with a New Series	186
	Synchronization and Switchover	
	for Communication Module Series Replacement	186
	Verify Module Compatibility and Synchronization	188
	Replace Redundancy Modules with a New Catalog Number	189
Install Earlier Redundancy Firmware Bundles	Appendix E	
	Install Bundles 30.051_kit1 and 24.053_kit1	191
	Install Bundle 24.052_kit1	192

ControlLogix 5560 Redundancy Considerations	Appendix F	
	ControlLogix 5560 Controllers in Redundant Chassis	193
	Plan for Controller Connections	193
	Estimate Crossload Times	193
	Set Watchdog Time	193
	Instruction Based Alarms (IBA)	193
	Firmware Updates and System Time	194
	Convert from a Non-redundant System	194
ControlNet Considerations	Appendix G	
	ControlNet Modules in Redundant Chassis	195
	Plan for Communication Module Connections	195
	Bridge from an EtherNet/IP Network to a ControlNet Network	195
	ControlNet Configuration Considerations	196
	Use at Least Four ControlNet Network Nodes	197
	Assign Lowest Node Numbers to Remote ControlNet Modules	197
	Set Partnered ControlNet Module Switches to the Same Address	197
	Reserve Consecutive Node Addresses for Partner Modules	198
	Redundant ControlNet Media	198
	Produce/Consume Connections	199
	Network Update Time	200
	NUTs with Multiple ControlNet Networks	200
	Scheduled or Unscheduled Network	201
	Use a Scheduled Network	201
	Use an Unscheduled Network	201
	Add Remote ControlNet Modules While Online	202
	ControlNet Module CPU Usage	202
	ControlNet Module Connections Used	202
	Monitor the ControlNet Network	202
	Keeper Status Causing Synchronize Failure	203
	Check the Module Status Display	203
	Check Keeper Status in RSNetWorx for ControlNet Software	203
	Replace a 1756-CN2 Module with a New Series	205
	Synchronization and Switchover for the ControlNet Modules	205
Convert from a Non-redundant System	Appendix H	
	Update the Configuration in the Logix Designer Application	209
	Replace Local I/O Tags	211
	Replace Aliases to Local I/O Tags	212
	Remove Other Modules from the Controller Chassis	212
	Add an Identical Chassis	212
	Upgrade to Redundancy Firmware	212
	Update the Controller Revision and Download the Project	212
History of Changes	Appendix I	
	Change Log	213
	Index	217

Notes:

About This Publication

This publication provides information about how to set up, configure, program, monitor, and troubleshoot these high availability systems:

- Logix SIS (safety instrumented system) with GuardLogix 5580 controllers
- ControlLogix® 5580 redundancy
- ControlLogix 5570 redundancy

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Added differences in Logix SIS safety levels depending on controller firmware revisions	29, 67
Added important statement about IP swapping and shortcut paths	33
Added the Identify Installed SFP Transceivers section	34
Added the Reset Factory Defaults feature	45, 54
Added important statement about using an MSG instruction to disable or re-enable SFP ports	55
Added requirement for Sequential Function Chart (SFC) in tasks with data synchronization disabled	72
Added crossload times for controller firmware revision 38	80
Revised standard task watchdog time requirement	82

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation. You can view or download publications at rok.auto/literature.

Resource	Description	
Installation	ControlLogix Chassis Installation Instructions, publication 1756-IN621	Describes how to install a ControlLogix chassis.
	ControlLogix Power Supply Installation Instructions, publication 1756-IN619	Describes how to install, remove, and troubleshoot a power supply system.
	ControlLogix Redundant Power Supply Installation Instructions, publication 1756-IN620	Describes how to install, remove, and troubleshoot a redundant power supply system.
	ControlLogix Redundancy Modules Installation Instructions, publication 1756-IN095	Describes how to install and connect 1756-RM3 redundancy modules.
	ControlLogix Redundancy Modules Installation Instructions, publication 1756-IN087	Describes how to install and connect 1756-RM2 redundancy modules.
	1756 EtherNet/IP Communication Modules Installation Instructions, publication 1756-IN050	Describes how to install and monitor the status of 1756 EtherNet/IP™ communication modules.
	ControlLogix 5580 Controllers Installation Instructions, publication 1756-IN043	Provides installation instructions for ControlLogix 5580 controllers.
	GuardLogix 5580 Controllers Installation Instructions, publication 1756-IN048	Provides installation instructions for GuardLogix® 5580 controllers.
	ControlLogix 5570 Controllers Installation Instructions, publication 1756-IN088	Provides installation instructions for ControlLogix 5570 controllers.
Systems and Software	ControlFLASH Plus Quick Start Guide, publication CFP-0S001	Describes how to use the ControlFLASH Plus™ software to upgrade device firmware.
	High Availability Systems Reference Manual, publication HIGHAV-RM002	Provides information to help design and plan high availability systems.
	Logix SIS Safety Reference Manual, publication 1756-RM015	Describes Logix SIS redundancy, which is type-approved and certified for use in safety applications.
	CIP Security with Rockwell Automation Products Application Technique, publication 1756-AT001	Explains how to implement the Common Industrial Protocol (CIP™) Security standard in your industrial automation control system (IACS).
Controllers	ControlLogix and GuardLogix Controllers Technical Data, publication 1756-TD001	Contains specifications on ControlLogix and GuardLogix controllers and redundancy modules.
	Reduce Downtime with Redundant Process Control, publication 1756-PP014	Provides an overview and high-level features of Logix redundant controller solutions.
	ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information to help you design a system, operate a ControlLogix or GuardLogix-based controller system, and develop applications.
	ControlLogix 5570 and 5560 Controllers User Manual, publication 1756-UM001	Provides information to help you design a system, operate a ControlLogix controller system, and develop applications.
	Logix 5000 Controllers Common Procedures Programming Manual, publication 1756-PM001	Provides links to a collection of programming manuals that describe how to use procedures that are common to all Logix 5000® controllers projects.
	ControlLogix and GuardLogix 5580 controllers technical documentation ControlLogix 5570 controllers technical documentation	Quickly access and download technical specifications, installation instructions, and user manuals.
Networks	EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007	Describes Device Level Ring (DLR) topologies, configuration considerations, and diagnostic methods.
	EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006	Describes Parallel Redundancy Protocol (PRP) topologies, configuration considerations, and diagnostic methods.
	Ethernet Reference Manual, publication ENET-RM002	Describes basic Ethernet concepts, infrastructure components, and infrastructure features.
	ControlLogix EtherNet/IP Network Devices User Manual, publication 1756-UM004	Describes how to use ControlLogix EtherNet/IP communication modules with a Logix 5000 controller and communicate with various devices on the EtherNet/IP network.
	ControlNet to EtherNet/IP Migration Reference Manual, publication CNET-RM001	Provides information to migrate from an existing ControlNet network to an EtherNet/IP network.
Guidelines and Certifications	Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
	Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
	Product Certifications website, rok.auto/certifications .	Provides declarations of conformity, certificates, and other certification details.

Redundancy Systems

A redundancy system provides greater availability by establishing redundancy between a pair of controller chassis with identical specific components. While running, the primary controller chassis detects changes in data and synchronizes the data with the secondary controller. The secondary controller is ready to take immediate control if fault occurs.

The following types of control systems can be configured for redundancy:

- Logix SIS (safety instrumented system)
- ControlLogix® 5580
- ControlLogix 5570

High Availability

Availability is the percentage of time that a system is functioning and able to perform its mission. High availability is a characteristic of a system that aims to achieve an agreed level of availability for a higher than normal period.

Controller systems can achieve high availability when specific hardware and configuration requirements are met. For general guidelines for high availability systems, including redundant system components, networks, and other hardware and software considerations, see the High Availability Systems Reference Manual, [HIGHAV-RM002](#).

Logix SIS Redundancy

Logix SIS is designed for safety applications that require high availability. Logix SIS can achieve up to SIL 2 or SIL 3 safety ratings. When redundant controllers are configured for Logix SIS, logic executes as follows:

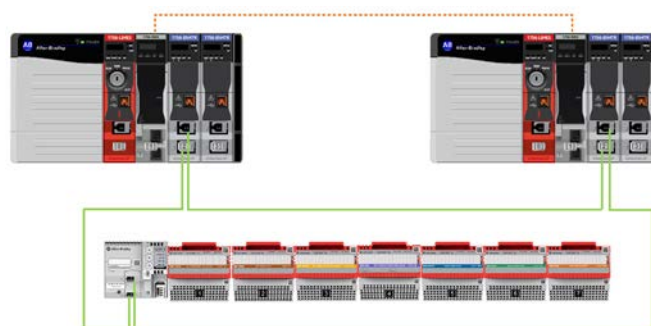
- Both primary and secondary controllers simultaneously execute the safety task and all safety data remains synchronized.
- Only the primary controller executes standard tasks and crossloads standard data to the secondary controller.

The redundant safety controllers can communicate with a mix of standard and safety I/O modules in a remote chassis. For safety I/O communication, concurrent communication must be configured between 1756-EN4TR modules in the redundant chassis and the remote safety I/O modules.

For more information about Logix SIS, see the following.

Topic	See
Required system components	Chapter 2
Logix SIS system operation	Chapter 3
SIL 2/3 requirements and safety considerations	Logix SIS Safety Reference Manual, publication 1756-RM015

Figure 1 - Logix SIS Redundancy



ControlLogix 5580 Redundancy

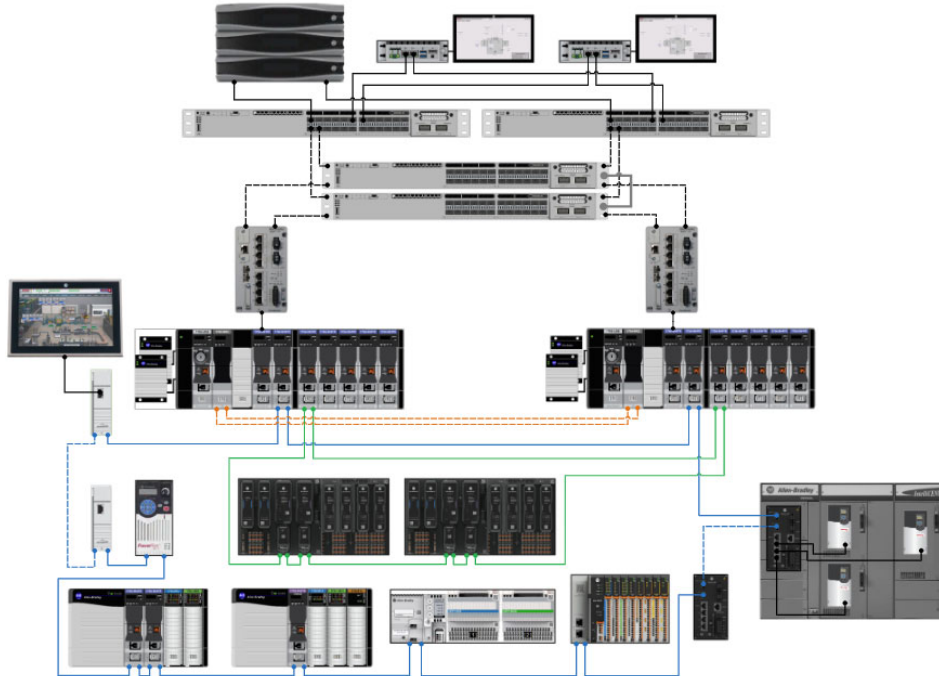
ControlLogix 5580 redundancy is designed for non-safety applications that require high availability. When redundant controllers are configured for redundancy, the primary controller executes standard tasks and crossloads standard data to the secondary controller.

The redundant controllers can communicate with only standard I/O modules in a remote chassis via concurrent or non-concurrent communication.

For more information about ControlLogix 5580 redundancy, see the following.

Topic	See
Required system components	Chapter 2
ControlLogix system operation	Chapter 4

Figure 2 - ControlLogix 5580 Redundancy System



ControlLogix 5570 Redundancy

ControlLogix 5570 redundancy can be used in non-safety and SIL 2 safety applications that require high availability. When redundant controllers are configured for redundancy, the primary controller executes standard tasks and crossloads standard data to the secondary controller.

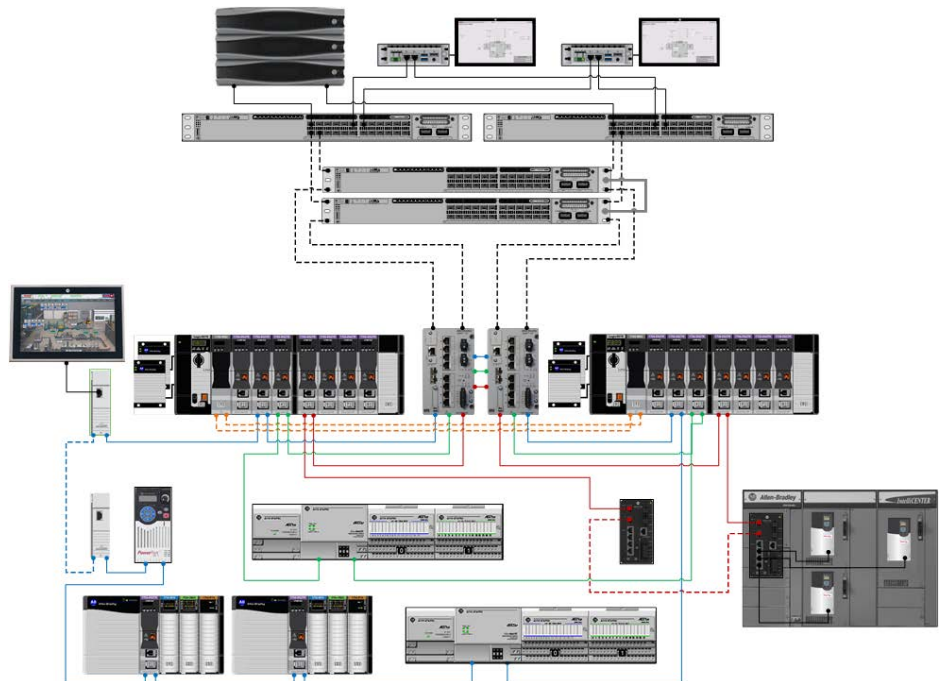
The redundant controllers can communicate with only standard I/O modules in a remote chassis via non-concurrent communication.

IMPORTANT If you use ControlLogix 5570 redundancy for SIL 2 and want to move to Logix SIS for SIL 2/3, there is no direct migration path. Logix SIS uses different hardware components and programming than ControlLogix 5570 redundancy.

For more information about ControlLogix 5570 redundancy, see the following.

Topic	See
Required system components	Chapter 2
ControlLogix system operation	Chapter 4
SIL 2 requirements and safety considerations	ControlLogix SIL 2 Applications Safety Reference Manual, publication 1756-RM001

Figure 3 - ControlLogix 5570 Redundancy System



Feature Support

The following table lists the features available for Logix SIS, ControlLogix 5580, and ControlLogix 5570 redundancy systems. For feature support specific to redundancy modules, see [Table 6](#).

For more product comparison details, see the Replacement Guidelines: Logix 5000 Controllers Reference Manual, publication [1756-RM100](#).

Table 1 - Feature Support in Redundancy Systems

Feature	Logix SIS	ControlLogix 5580	ControlLogix 5570
SIL 2 safety certification	Yes	No	Yes
SIL 3 safety certification	Yes	No	No
CIP Security™	Yes	Yes	No
CIP Sync™	Yes	Yes	Yes
Produced/consumed safety tags	No	No	No
Produced/consumed standard tags	Yes	Yes	Yes
Produced unicast connections	Yes	Yes	Yes
Consumed unicast connections	No	No	No
Produced multicast connections	Yes	Yes	Yes
Consumed multicast connections	Yes	Yes	Yes
EtherNet/IP™ network for redundant chassis pair	Yes	Yes	Yes
ControlNet® network for redundant chassis pair	No	No	Yes
Controllers use the same firmware revision for redundancy and simplex (non-redundancy)	Yes	Yes	No
PlantPAX® 5.0 for Process controllers	No	Yes	No
FactoryTalk® applications for Ethernet communication modules	Yes	Yes	Yes
SequenceManager™ for Process controllers	No	Yes	No
PhaseManager™	Yes	Yes	Yes
Firmware Supervisor	No	No	No
EtherNet/IP Socket Interface	Yes	Yes	Yes
Parallel Redundancy Protocol (PRP)	Yes	Yes	Yes
Device Level Ring (DLR)	Yes	Yes	Yes
Messaging to PLC-2®, PLC-3®, PLC-5®, SLC™, and other legacy controllers	No	No	Yes

Restrictions

There are restrictions that you must consider when using a redundancy system. For system component requirements and restrictions, such as communication modules and remote I/O modules, see [System Components](#).

Most of these restrictions apply to all redundancy system revisions:

- Redundancy systems do not support the following:
 - OPC UA
 - Motion features
 - License-based source and execution protection
 - The front Ethernet port on a controller
 - The Match Project to Controller feature in the Logix Designer application
- The redundant controller program cannot contain these tasks:
 - Event tasks
 - Inhibited tasks

For recommendations and requirements that are related to programming the redundant controller, see [Programming Best Practices for Standard Tasks](#).
- You cannot use consumed unicast connections in a redundancy system. You can use produced unicast connections that remote consumers consume.
- Outputs controlled by Immediate Output (IOT) instructions will not be updated by the execution of the IOT instruction. We recommend that you do not use IOT instructions in a redundancy system.
- The HMIBC instructions are not supported in a redundancy system.
- Listen Only connections are not supported for FLEX 5000® I/O.
- Listen Only connections are not supported for highly integrated HART devices.

There is no ability for another controller to create Listen Only connections or dual-own these type of connections.
- These legacy communication networks are not supported with a Logix SIS or ControlLogix 5580 redundant chassis pair: DeviceNet®, RIO, DH+™.

Security Considerations

To help maintain a secure system, follow these guidelines:

- Limit physical access to authorized personnel.
- Implement physical barriers, such as locked cabinets.
- Only purchase products from official suppliers.
- Only download firmware and software from the Rockwell Automation official download portal at rok.auto/pcdc.

To secure networks and communication and data, follow these guidelines:

- Implement network technologies that filter, block, and control access to help secure networks.
- Configure authorization policies to define conditions for remote access.
- Select control products that offer security options.

For more information, see the following.

Resource	Description
System Security Design Guidelines Reference Manual, publication SECURE-RM001	Provides guidance on how to conduct vulnerability assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.
Configure System Security Features User Manual, publication SECURE-UM001	Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.
CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001	Describes how to plan and implement a Rockwell Automation system that supports the CIP Security protocol.
FactoryTalk Security Application Technique, publication SECURE-AT002	Describes how to use FactoryTalk Security to implement authentication and authorization in your industrial automation system. Describes how to enforce product-specific security for Studio 5000 Logix Designer®, FactoryTalk View, and FactoryTalk AssetCentre.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Provides guidelines for how to design, implement, and manage industrial Ethernet networks.

Redundancy Module microSD Card Security

1756-RM3 redundancy modules have a microSD™ card for the primary purpose of storing Tech Support logs that Rockwell Automation can use to investigate the cause of a fault.

The microSD card is secured in the following ways:

- Major fault data for the 1756-RM3 is stored on the microSD card in the RockwellAutomation folder. All sensitive data in this location is encrypted and only Rockwell Automation can decode the encrypted data.
- Data is saved to the microSD card in only one direction: from the internal memory of the redundancy module to the microSD card.
- Data stored on the microSD card cannot be read by the redundancy module firmware.

System Components

Redundancy operation requires that the components of the system adhere to specific requirements. Before you set up your system, make sure that you know the requirements and restrictions of each component.

For more information about how to achieve high availability with system components, see the High Availability Systems Reference Manual, publication [HIGHAV-RM002](#).

Redundant Chassis Pair

Communication between components that match in a redundant chassis pair makes redundancy possible. In a redundant chassis pair, one chassis operates as a primary chassis and the other as a secondary chassis.

The redundant chassis pair is connected to other system components, such as one or more remote I/O chassis or human machine interfaces (HMIs).

Redundant Chassis Requirements

For a redundant chassis pair, you can use any ControlLogix® or ControlLogix-XT™ chassis of the same size. For example, if the primary chassis uses a 1756-A4 chassis, the secondary chassis must use a 1756-A4 chassis.

Each redundant chassis in a pair must contain the components in the following table. If the chassis is used as a redundant gateway, then a controller is not required.

Table 2 - Required Chassis Components

Required Component	Modules Allowed in Each Chassis
Controller	
Logix SIS and ControlLogix 5580	1, max
ControlLogix 5570	2, max
Redundancy module	1, max
Communication module	1, min 7, max

You can also use any number of optional slot filler modules, catalog number 1756-N2.

IMPORTANT Do not place I/O modules in a redundant chassis.

These configuration parameters must match for the components in a redundant chassis pair during normal system operation:

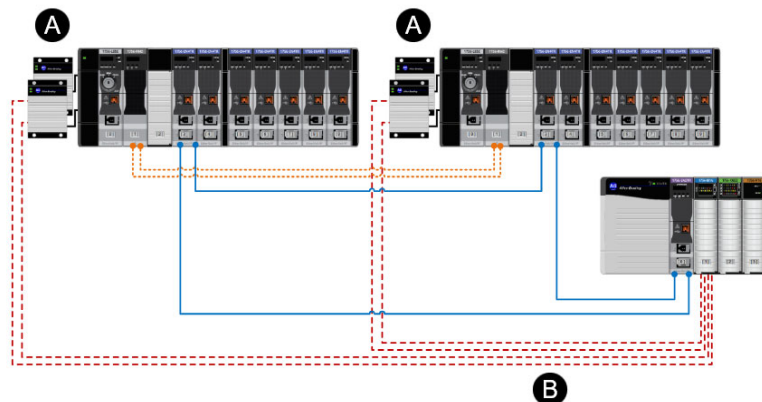
- Module type.
- Chassis size (all sizes are supported)
- Slot placement.
- Firmware revision.

Power Supply Requirements

For each redundant chassis, use single or redundant power supplies. Redundant power supplies reduce single points of failure and increase system availability.

Each power supply includes the option to add annunciator wiring to connect the power supplies to remote input modules. Power supply annunciator wiring enables quick isolation and detection of failures, which directly impacts system maintainability. For more information, see the ControlLogix Redundant Power Supply Installation Instructions, publication [1756-IN620](#).

Figure 4 - Redundant Power Supplies



Item	Description
A	1756-PA75R or 1756-PB75R
B	Annunciator wiring

Redundant Controller Requirements

Follow these requirements for redundant controllers:

- (Logix SIS and ControlLogix 5580 redundancy). Place only one controller in the same slot in each redundant chassis.
- (ControlLogix 5570 redundancy). Place up to two controllers in the same slots in each redundant chassis. When you use two controllers in the same chassis, they must be of the same product family. For example, you cannot place a ControlLogix 5570 controller and a ControlLogix 5580 controller in the same chassis. The series and catalog numbers of the controllers in the same chassis do not need to match.
- Use identical series, catalog numbers, and redundancy firmware revisions for partner controllers between the primary and secondary chassis.
- (Logix SIS and ControlLogix 5580 redundancy). Do not connect anything to the embedded Ethernet port on the front of the controller. When redundancy is enabled, the port is disabled.
- Set the keyswitch on the front of both controllers to the same position, such as RUN or REM. A keyswitch mismatch on redundant controllers affects the switchover response. See [Switchover Response to Keyswitch Mismatch](#).

To size a controller, you can use the following free tools from Rockwell Automation:

- Access the cloud-based Advisor platform from <https://advisor.rockwellautomation.com/>
- Download Integrated Architecture Builder from [ab.com](#).

When designing a PlantPAX® system, use the [PlantPAX System Estimator \(PSE\)](#). The PSE is a free wizard that is built into Integrated Architecture Builder.

Table 3 - Supported Controllers

Redundancy System	Cat. No.
Logix SIS	1756-L81ES, 1756-L82ES, 1756-L83ES, 1756-L84ES, 1756-L85ES 1756-L81ESK, 1756-L82ESK, 1756-L83ESK, 1756-L84ESK 1756-L81EXTS, 1756-L82EXTS, 1756-L83EXTS, 1756-L84EXTS 1756-L81ESXT, 1756-L82ESXT, 1756-L83ESXT, 1756-L84ESXT IMPORTANT: 1756-L8SP, 1756-L8XTSP, and 1756-L8SPK safety partners do not support Logix SIS redundancy.
ControlLogix 5580	1756-L81E, 1756-L82E, 1756-L83E, 1756-L84E, 1756-L85E 1756-L81EXT, 1756-L82EXT, 1756-L83EXT, 1756-L84EXT, 1756-L85EXT 1756-L81EK, 1756-L82EK, 1756-L83EK, 1756-L84EK, 1756-L85EK 1756-L81E-NSE, 1756-L82E-NSE, 1756-L83E-NSE, 1756-L84E-NSE, 1756-L85E-NSE 1756-L81EP, 1756-L83EP, 1756-L85EP 1756-L81E-NSEXT, 1756-L82E-NSEXT, 1756-L83E-NSEXT, 1756-L84E-NSEXT, 1756-L85E-NSEXT 1756-L81EPXT, 1756-L83EPXT, 1756-L85EPXT
ControlLogix 5570	1756-L71, 1756-L72, 1756-L73, 1756-L73XT, 1756-L74, 1756-L75

Table 4 - Controller Firmware Requirements

Redundancy System	Controller Firmware Revision
Logix SIS	37 or later
ControlLogix 5580	33 or later
ControlLogix 5570	1756-L71 controllers require firmware revision 20.054 or later. All other catalog numbers require firmware revision 19.053 or later.

ControlLogix 5570 Controller Memory Constraints

Each ControlLogix 5570 controller must have enough data memory to store twice the amount of tag data that is associated with a redundant controller project.

Each controller must have enough I/O memory to store twice the amount of I/O memory used. To check the available I/O memory, access the Memory tab of the Controller Properties dialog box in the programming software.

For more information about data and I/O memory, see the Knowledgebase Technote [Understanding ControlLogix Redundancy Memory Usage](#).

Plan for Controller Communication

To plan for controller communication, consider the following limitations:

- Logix SIS safety controllers and ControlLogix 5580 controllers support a limited number of EtherNet/IP™ nodes for communication on the EtherNet/IP network. The maximum supported nodes vary depending on the controller catalog number. To determine the supported EtherNet/IP nodes for your controller, see the ControlLogix and GuardLogix Controllers Technical Data, publication [1756-TD001](#).
- ControlLogix 5570 controllers provide 500 total connections.

If you use the controller at or very near its connection or node limit, it can be difficult to synchronize the redundant chassis.

Redundancy Module Requirements

A pair of redundancy modules is required to link the redundancy chassis pair. Place one redundancy module in the same slot of each redundant chassis. The partner redundancy modules monitor events in each chassis and initiate system responses as required.

IMPORTANT Use only direct, end-to-end connections between the fiber ports of partner redundancy modules. For example, do not use the fiber ports on a redundancy module to connect to a Stratix® switch or other device.

Partner redundancy modules must have the same catalog number.

Table 5 - Supported Redundancy Modules

Redundancy System	Cat. No.
Logix SIS	1756-RM3, 1756-RM3XT, 1756-RM2, 1756-RM2XT
ControlLogix 5580	1756-RM3, 1756-RM3XT, 1756-RM2, 1756-RM2XT
ControlLogix 5570	1756-RM3, 1756-RM3XT, 1756-RM2, 1756-RM2XT, 1756-RM

The 1756-RM3-2SFP module is functionality equivalent to a 1756-RM3 module but comes with two small form-factor pluggable (SFP) fiber-optic transceivers. The 1756-RM3-2SFP module is intended to be one catalog number for a functional replacement of a 1756-RM2 module in an existing redundancy system.

For redundancy module and accessory specifications, see the ControlLogix and GuardLogix Controllers Technical Data, publication [1756-TD001](#).

EtherNet/IP Features

Redundancy modules support the following EtherNet/IP features. For information about these EtherNet/IP features, see [Configure Redundancy Modules](#).

Table 6 - Redundancy Module EtherNet/IP Features

Cat. No.	Features			
	Communication Rate, Max	Protected Mode	Fiber Security	CIP Sync™
1756-RM3, 1756-RM3XT	1000 Mbps	Yes	Yes	Yes
1756-RM2, 1756-RM2XT	1000 Mbps	No	No	No
1756-RM	100 Mbps	No	No	No

Communication Module Requirements

At least one communication module is required in the same slot of each redundant chassis to support the redundant system network. Follow these requirements for communication modules:

- You must use enhanced communication modules in redundancy systems. Enhanced communication modules contain a 2 or 4 in their catalog number. For example, the 1756-EN2T or 1756-EN4TR modules.

For modules compatible with your version of controller firmware, access controller release notes from the Product Compatibility and Download Center at rok.auto/pcd. For example, in the Logix Designer application version 34 or later, you can use 1756-EN4TR modules in a ControlLogix 5580 redundant chassis. In earlier versions, you can use 1756-EN4TR modules only in a remote ControlLogix I/O chassis.

- Do not use standard communication modules. Standard communication modules contain a B in their catalog number. For example, the 1756-ENBT module.
- Use any combination of up to seven enhanced communication modules in each redundant chassis.
- Do not use the USB ports of communication modules to access the redundant system network while the system is online. Use of the USB ports while online can result in a loss of communication of traffic through the USB port after a switchover.
- Use the same firmware levels in a partnered set. The series for communication modules is not required to match in a partnered set. However, if your application requires a feature specific to a module series level, you must use the same series level for each module. For example, only the 1756-EN2T/C communication module offers the double-data rate (DDR) feature. You must use 1756-EN2T/C modules or later in each chassis of the redundant chassis pair to use DDR.
- For communication between a Logix SIS redundant chassis pair and FLEX 5000® safety I/O, you must use a 1756-EN4TR, 1756-EN4TRK, or 1756-EN4TRXT communication module that is configured for concurrent communication.

For more information about concurrent communication in Logix SIS, see [Concurrent Communication](#).

- For all guidelines related to ControlNet® communication in a ControlLogix 5570 redundancy system, see [Appendix G](#).

Table 7 - Supported Communication Modules

Redundancy System	Cat. No.
Logix SIS	1756-EN4TR, 1756-EN2F/C, 1756-EN2T/D, 1756-EN2TR/C, 1756-EN2TP 1756-EN4TRK, 1756-EN2FK/C, 1756-EN2TK/D, 1756-EN2TRK/C, 1756-EN2TPK 1756-EN4TRXT, 1756-EN2TXT, 1756-EN2TRXT, 1756-EN2TPXT
ControlLogix 5580	1756-EN4TR, 1756-EN2F, 1756-EN2T, 1756-EN2TR, 1756-EN2TP 1756-EN4TRK, 1756-EN2FK, 1756-EN2TK, 1756-EN2TRK, 1756-EN2TPK 1756-EN4TRXT, 1756-EN2TXT, 1756-EN2TRXT, 1756-EN2TPXT
ControlLogix 5570	1756-EN2F, 1756-EN2T, 1756-EN2TR, 1756-EN2TP, 1756-EN2TXT 1756-EN2FK, 1756-EN2TK, 1756-EN2TRK, 1756-EN2TPK 1756-CN2, 1756-CN2R, 1756-CN2RK, 1756-CN2RXT

IMPORTANT

For communication modules, signed and unsigned firmware are available. Signed modules provide the assurance that only validated firmware can be upgraded into a module. Once signed firmware is installed, subsequent firmware updates must be signed also. There are no functional/feature differences between signed and unsigned communication modules.

Products are shipped with unsigned firmware. To obtain signed firmware, upgrade the firmware for your product. To obtain signed and unsigned firmware, go to <https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?crumb=113>.

Plan for Communication Module Connections

A CIP™ connection is a point-to-point communication mechanism that is used to transfer data between a producer and a consumer. These mechanisms are examples of CIP connections:

- Logix 5000® controller message transfer to Logix 5000 controller
- I/O or produced tag
- Program upload
- RSLinx® DDE/OPC client
- PanelView™ polling of a Logix 5000 controller

EtherNet/IP communication modules use CIP connection to connect devices. Three CIP connections are reserved for redundancy. You can use the remaining connections in any manner that your application requires.

To determine the total number of CIP connections supported by your communication module, see the 1756 ControlLogix Communication Modules Specifications Technical Data, publication [1756-TD003](#).

I/O Modules

A redundancy system supports I/O modules in a remote chassis. You cannot use I/O modules in a redundant chassis.

Supported Networks

The following networks are supported between the redundant chassis and a remote I/O chassis without bridging.

Table 8 - Supported Networks for Remote I/O

Redundancy System	Network
Logix SIS	EtherNet/IP
ControlLogix 5580	EtherNet/IP
ControlLogix 5570	EtherNet/IP, ControlNet

For all guidelines related to ControlNet networks, see [Appendix G](#).

Supported Products

The following table lists I/O products that you can use in a remote chassis that is connected to a redundant chassis pair. The table is not a complete list of supported I/O products and some restrictions exist. For more information, see the Knowledgebase Technote [Rockwell Automation Logix Products Not Supported by ControlLogix Redundancy](#).

Table 9 - Supported Products for I/O in a Remote Chassis

Redundancy System	Standard I/O	Safety I/O
Logix SIS	5034 PointMax™ I/O 5094 FLEX 5000 5015 FLEXHA 5000™ I/O 1756 ControlLogix I/O 1715 Redundant I/O 1794 FLEX™ I/O 1734 POINT I/O™	5094 FLEX 5000 safety I/O
ControlLogix 5580	5034 PointMax I/O 5094 FLEX 5000 I/O 5015 FLEXHA 5000 I/O 1756 ControlLogix I/O 1715 Redundant I/O 1794 FLEX I/O 1734 POINT I/O	Not supported
ControlLogix 5570	5094 FLEX 5000 I/O 1756 ControlLogix I/O 1715 Redundant I/O 1794 FLEX I/O 1734 POINT I/O	Not supported

To use 1756 ControlLogix I/O, 1794 FLEX™ I/O, or 1715 Redundant I/O in ControlLogix 5570 SIL 2 safety applications, see the ControlLogix SIL 2 Applications Safety Reference Manual, publication [1756-RM001](#).

HMI

Depending on the network that is used to connect the redundant system to HMI, plan for certain placement and configuration requirements. You can connect an HMI to a primary chassis over either of these networks:

- EtherNet/IP
- ControlNet with ControlLogix 5570 redundancy

IMPORTANT To help prevent anomalous behavior, do not target active communication at the secondary chassis.

To communicate with HMI, the following methods are available:

- IP address swapping—Supported by all HMI products. For more information, see [IP Address Swapping](#).
- Redundant controller shortcut paths—Supported by only FactoryTalk View Site Edition with FactoryTalk Linx software. For more information, see the High Availability Systems Reference Manual, publication [HIGHAV-RM002](#).

This table describes redundant system considerations for HMI on the EtherNet/IP network.

Table 10 - HMI Considerations for Redundancy Systems

HMI	Considerations
<ul style="list-style-type: none"> • OptixPanel™ graphic terminal • FactoryTalk® Optix™ software 	Only IP address swapping is supported.
PanelView Standard terminal	Same as a non-redundant system.
<ul style="list-style-type: none"> • PanelView Plus terminal • VersaView® industrial computer that runs the Windows® CE operating system 	Use FactoryTalk Linx software, version 5.0 or later.
FactoryTalk View Site Edition software with FactoryTalk Linx software	<ul style="list-style-type: none"> • Use FactoryTalk Linx communication software, version 5.0 or later. • Keep the HMI and both redundant chassis on the same subnet. • To help reduce data server recovery switchover time, consider using redundant controller shortcut paths.
<ul style="list-style-type: none"> • FactoryTalk View Site Edition software with RSLinx Classic software • Any other HMI client software that uses RSLinx Classic software 	Limit the number of RSLinx servers that a controller uses to 1...3 servers. One server is best.

Optional Software

Depending on your redundancy system program, configuration, and components, you can use the following software.

System Component	Software
Alarms	FactoryTalk Alarms and Events
Batches or recipes	FactoryTalk Batch
HMI	<ul style="list-style-type: none"> • FactoryTalk Optix • FactoryTalk View Site Edition • FactoryTalk View Machine Edition • FactoryTalk Linx software
Various FactoryTalk services	FactoryTalk Services Platform

Other Communication Networks

You can bridge to other communication networks outside of the redundant chassis. You can bridge these networks via a remote chassis:

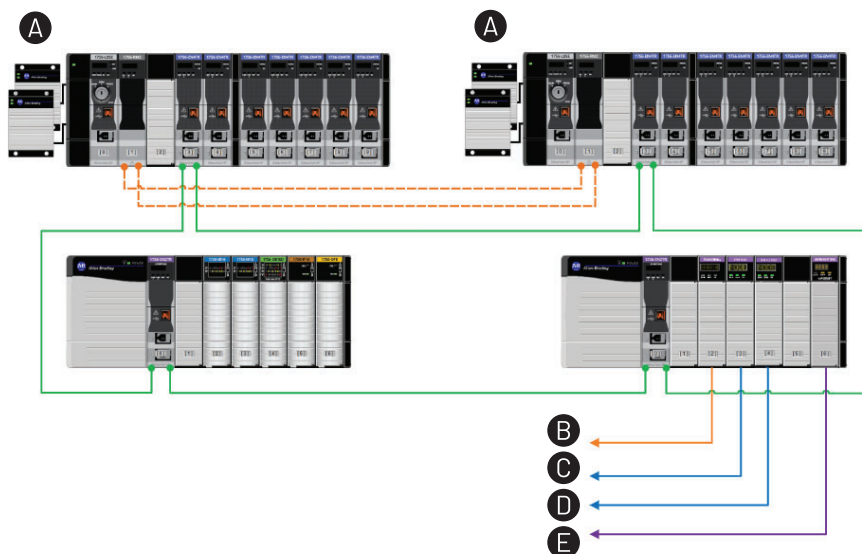
- DeviceNet®
- Universal remote I/O with ControlLogix 5570 redundancy
- Data Highway Plus™ with ControlLogix 5570 redundancy

In ControlLogix 5580 and Logix SIS redundancy, you can put DeviceNet modules in a remote chassis but DeviceNet devices may not be bumpless connection during a switchover event. For more information, see Knowledgebase Technote [ControlLogix 5580 Redundancy with DeviceNet](#).

IMPORTANT Do not use the redundant chassis to bridge between networks. Bridging through the redundant chassis to the same or different networks or routing messages through a redundant chassis is not supported.

In redundancy firmware revisions earlier than 30.051, you can connect HMI to the redundant chassis pair via a bridge from an EtherNet/IP network to a ControlNet network to help prevent a brief loss of communication with the redundant chassis pair if a switchover occurs. For more information, see [Possible Communication Delays During a Switchover](#).

Figure 5 - Chassis Bridge from EtherNet/IP to Remote I/O Networks



Item	I/O Network
A	No I/O
B	DeviceNet
C	RIO
D	DH+/RIO
E	Third party

The following tables show the system components that you can use with each network that is connected to a redundancy system. If you use a network from a third-party vendor, the vendor is responsible for testing and validation.

Table 11 - Communication Network Components for Logix SIS or ControlLogix 5580 Redundancy

Network	Connection to Redundancy System	I/O	HMI
EtherNet/IP	Directly to redundant chassis	Yes	Yes
	Via a bridge	No	Yes
ControlNet	Directly to redundant chassis	No	No
	Via a bridge	No	No
DeviceNet	In controller chassis	No	No
	Via a bridge	Yes	Yes
Universal remote I/O	Via a bridge	No	No
Data Highway Plus	Via a bridge	No	No
Third party	In controller chassis	No	No
	Via a bridge	Yes	Yes

Table 12 - Communication Network Components for ControlLogix 5570 Redundancy

Network	Connection to Redundancy System	I/O	HMI
EtherNet/IP	Directly to redundant chassis	Yes with redundancy firmware revision 19.052 or later	Yes
	Via a bridge	No	Yes
ControlNet	Directly to redundant chassis	Yes	Yes
	Via a bridge	No	Yes
DeviceNet	Via a bridge	Yes	Yes
	In controller chassis	No	No
Universal remote I/O	Via a bridge	Yes	Yes
Data Highway Plus	Via a bridge	Yes	Yes
Third Party	In controller chassis	No	No
	Via a bridge	Yes	Yes

Logix SIS Redundancy Operation

Logix SIS uses redundant safety controllers to provide continuous operation after a single-channel fault. This chapter describes the operation of redundant safety controllers that execute the safety task. You can also use redundant safety controllers to execute standard tasks with no safety function. Redundancy operation for standard tasks within a safety controller and Logix SIS fiber channel operation is the same as ControlLogix® redundancy.

Logix SIS redundancy supports SIL 2 and SIL 3 safety functions:

- To support a SIL 3 or high-demand SIL 2 safety function, redundant SIL 2 controllers must operate together. If one controller fails, the system must be repaired within your mean repair time (MRT).
- If redundant operation is interrupted, the primary safety controller operates as a SIL 2, single-channel controller, and the secondary safety controller no longer participates in the safety function. Standard tasks continue to operate.

IMPORTANT

Be aware of the following differences in controller firmware revisions:

- With firmware revision 37, the safety level in the controller properties must be set to SIL2/PLd.
Even when your system complies with a SIL 3 safety function, the SafetySILConfiguration attribute always shows a SIL 2 value. This value is expected because it reflects the safety level in the controller properties. A SIL2/PLd safety level is the required configuration for safety controllers that are enabled for redundancy.
 - With firmware revision 38 or later, the safety level displays the following static value: SIL3/PL3 when synchronized or disqualified within MRT; SIL2/PLd when disqualified
Even when your system complies with a SIL 2 safety function, the SafetySILConfiguration attribute always shows a SIL 3 value.
-

For details about SIL requirements, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

SIL 2 and SIL 3 Safety Functions

System Qualification and Synchronization

When the redundant system is first started, the redundancy modules run checks on the redundant chassis. These checks determine the following:

- Both chassis have the correct modules and firmware to establish a redundant system
- A safety application exists in the primary safety controller in a safety-protected state

This stage of checks is referred to as qualification.

IMPORTANT

During qualification, the safety function is temporarily muted up to 1 second + 1 safety task period.

During qualification, the primary safety controller transfers the following to the secondary safety controller:

- The safety application
- The safety signature, if one exists

For detailed information about the safety signature and safety function mute time, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

IMPORTANT	<p>The redundancy system can end the qualification process for the following reasons:</p> <ul style="list-style-type: none"> • If a safety partner module is installed in either chassis. Safety partner modules, such as 1756-L8SP, are not supported in Logix SIS redundancy. • If the system cannot validate the safety signature of a safety application in the secondary controller. • If the safety function is muted for more than 1 second + 1 safety task period. In this case, the primary safety controller resumes the safety function alone.
------------------	--

After the redundancy modules complete qualification, synchronization can take place. Synchronization is a state in which the redundancy modules execute these tasks:

- Verify the connection between redundancy modules
 - Verify that the redundant chassis continue to meet qualification requirements
 - Verify that partner EtherNet/IP™ communication modules can communicate to each other over the EtherNet/IP network
 - Synchronize data between the redundant safety controllers, also called crossloading
- This data is crossloaded:
- Updated tag values
 - Forced values
 - Online edits
 - Other project information

The primary and secondary safety controllers execute the safety task simultaneously and synchronize at the beginning and end of the safety task. As a result, safety data remains synchronized between the controllers. For more information about concurrent execution of the safety task, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

For important information about synchronization and concurrent communication to I/O, see [Concurrent Communication to I/O](#).

Operation After a Fault

Logix SIS redundancy can have the following types of faults:

- Single-channel faults

Single-channel faults are typically caused by firmware or hardware failures. After a single-channel fault on a redundant controller, the safety function continues to operate on the other controller. The faulted controller is disqualified, stops RUN mode, and must be requalified before redundancy operation can resume.
- Safety task faults, which can be recoverable or nonrecoverable

Safety task fault behavior is described in the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

Concurrent Communication to I/O

When synchronized, the primary and secondary safety controllers in the redundant chassis pair maintain unicast, concurrent communication with the same I/O devices. Concurrent communication provides seamless failover for any redundant pair of hardware components. A 1756-EN4TR module is required in each redundant chassis for concurrent communication to I/O in Logix SIS redundancy.

IMPORTANT	<p>During safety controller synchronization, the primary controller skips production of one safety output packet on each output connection. The adapter and I/O modules detect these skipped packets and increment the corresponding diagnostic tag. The ConcurrentConnectionsLostPackets tag increments once for each output connection to the adapter and I/O module.</p>
------------------	---

For concurrent communication system and configuration requirements, see [Concurrent Communication](#).

ControlLogix Redundancy Operation

This chapter describes redundancy operation for the following systems:

- ControlLogix® 5580
- ControlLogix 5570

System Qualification and Synchronization

A ControlLogix redundancy system provides greater availability by establishing redundancy between a pair of controller chassis with identical specific components. While running, the primary controller chassis detects changes in data and synchronizes the data with the secondary controller. The secondary controller is ready to take immediate control if events, such as a controller fault, occur.

When the redundant system is first started, the redundancy modules run checks on the redundant chassis. These checks determine if both chassis have the correct modules and firmware to establish a redundant system. This stage of checks is referred to as **qualification**.

After the redundancy modules complete qualification, synchronization can take place. **Synchronization** is a state in which the redundancy modules execute these tasks:

- Verify that the connection between redundancy modules is ready to facilitate a switchover
- Verify that the redundant chassis continue to meet qualification requirements
- Verify that partner EtherNet/IP™ communication modules can communicate to each other over the Ethernet network
- (ControlLogix 5570 only). Verify that partner ControlNet™ communication modules can communicate to each other over the ControlNet network
- Synchronize data between the redundant controllers, also called **crossloading**.

This data is crossloaded:

- Updated tag values
- Forced values
- Online edits
- Other project information

Depending on your system configuration, synchronization takes place at the end of each program that is run within the controller project or at other intervals that you specify.

Possible Communication Delays During Qualification

Some communication delays can occur during qualification. The existence and duration of these delays depend on these factors:

- Quantity and types of tags on scan in FactoryTalk® Linx software
- Client screen and tag update rates, such as in FactoryTalk Live Data/FactoryTalk Historian
- Number of data subscribers, such as FactoryTalk Alarms and Events and FactoryTalk Batch
- Size of the redundant controller application
- Network traffic

Synchronization and Fiber Channels

If a fiber channel between partnered redundancy modules fails or is undergoing repair, synchronization is preserved:

- The repair of a fiber channel can be performed online while the redundant chassis pair is running and synchronized. To aid online repairs, the fiber cable connections and SFP transceiver can be removed and inserted under power.
- A redundant channel is not required for synchronization. You can synchronize the redundant chassis pair with just one channel connected. The redundant channel can be installed later while the chassis is running synchronized.

Controller Switchovers

During redundant system operation, if certain conditions occur on the primary chassis, primary control is switched to the secondary chassis. This process is called a switchover. Switchovers occur as fast as 20 ms.

Causes of a Switchover

These conditions cause a switchover:

- Loss of power
- Major fault on the controller
- Removal or insertion of any module
- Failure of any module
- Loss of an EtherNet/IP connection

The loss of an EtherNet/IP connection only causes a switchover if it results in a lonely state. In a lonely state, the EtherNet/IP module cannot see any devices on the network.

- A program-prompted command to switchover
- A command that is issued via the Redundancy Module Configuration Tool (RMCT)

Operation After a Controller Switchover

After a switchover occurs, the new primary controller continues to execute programs. For more information about how tasks execute after a switchover, see [Crossloads, Synchronization, and Switchovers for Standard Tasks](#).

IMPORTANT If you require communication messaging to point to the primary controller when reading/writing to the redundancy system, do not target message instructions to modules in the secondary chassis.

Your application can require some programming considerations and potential changes to accommodate a switchover. For more information on these considerations, see, [Program Logic to Run After a Switchover on page 99](#).

IMPORTANT During a switchover of the fiber channels of the redundancy module, scan time encounters a delay of ~10 ms.

Possible Communication Delays During a Switchover

A brief communication interruption up to 30 seconds occurs between FactoryTalk Linx software and the redundant chassis pair when a switchover occurs. After the switchover is complete, communication resumes automatically.

These connection types can experience the communication delay when the switchover occurs:

- HMI to redundant chassis pair
- FactoryTalk Batch server to redundant chassis pair
- FactoryTalk Alarms and Events Service to redundant chassis pair

IMPORTANT For ControlLogix 5570 redundancy:

- Before firmware revision 30.051, the communication delays apply only when communication is exclusively over EtherNet/IP networks.
 - With firmware revision 30.051 or later, the communication delays apply to both EtherNet/IP and ControlNet® networks.
-

Reduce Data Server Recovery Time

Any software that uses tag data, such as HMI displays, data loggers, alarm systems, or historians, requires data server recovery time. Data server recovery time reduction is important to increase the availability of the system.

To help reduce data server recovery time during a switchover, you can configure redundant controller shortcut paths between a FactoryTalk Linx data server and a redundant ControlLogix controller. Redundant controller shortcut paths are available in FactoryTalk Linx version 6.00 or later.

To retain communication when a redundancy switchover occurs, you can configure two shortcut paths to the primary and secondary Logix 5000® controllers in a ControlLogix redundancy system, revision 31.5x. For details about how to implement this feature, see the FactoryTalk Linx Getting Results Guide, publication [LNXENT-GROO1](#).

IMPORTANT The communication modules that are used for this shortcut path cannot be configured for IP address swapping mode.

Switchover Response to Keyswitch Mismatch

The position of the keyswitch on redundant controllers must match. Mismatched keyswitch positions affect the switchover response, as described in the following table.

Table 13 - Switchover Response to Keyswitch Mismatch

Switch Position on Primary Controller	Switch Position on Secondary Controller	Primary Controller Response	Secondary Controller Response
RUN	REM (Run)	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in RUN mode.
REM (Run)	RUN	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in RUN mode.
RUN	PROG	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in PROGRAM mode.
REM (Run)	PROG	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in PROGRAM mode.
PROG	REM (Run)	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in PROGRAM mode.
REM (Program)	PROG	Primary becomes secondary and synchronizes.	Secondary becomes primary with the system in PROGRAM mode.
PROG	RUN	Primary becomes secondary and does not synchronize.	Secondary becomes primary with a major fault in the new primary: (Type 12) Redundancy Fault (Code 34) keyswitch in RUN invalid on switchover.
REM (Program)	RUN	Primary becomes secondary and does not synchronize.	Secondary becomes primary with a major fault in the new primary: (Type 12) Redundancy Fault (Code 34) keyswitch in RUN invalid on switchover.

Fiber Channel Operation

The dual SFP ports on the redundancy module operate as a redundant communication channels between partner redundancy modules:

- On 1756-RM3 modules, communication occurs on both channels. If one channel fails, communication persists on the other channel. Channel switchovers do not occur on 1756-RM3 modules.
- On 1756-RM2 modules, one channel operates as the active channel and the other channel operates as the backup channel. If the active channel fails, a channel switchover occurs and communication shifts to the backup channel, which then becomes the new active channel.

When you connect the fiber channels between partner redundancy modules, connect matching ports. For example, connect Link 1 on the primary module to Link 1 on the secondary module.

Causes of a Fiber Channel Failure

Any of the following can cause a loss of operation between fiber channels:

- Signal attenuation along the fiber cable path that is routed between the partner redundancy modules
- A broken or damaged fiber cable that is routed between the partner redundancy modules
- Improper or loosely fit cable connector
- SFP transceiver fault
- Removal or loose connection of the SFP transceiver
- Data communication error that is signaled by a failed CRC check

In 1756-RM2 modules, a loss of operation between the active channels triggers a switchover to the backup channels if the backup channels still have normal operation.

Operation After a Fiber Channel Switchover in 1756-RM2 Modules

Because of the fiber channel switchover, the redundant chassis pair remains synchronized even after a failure of the active channel. Chassis synchronization is lost only when both of the channels have failed or are disconnected.

The fiber channel switchover can occasionally extend the completion of data communication packets between the partner redundancy modules. Therefore, the scan time of the controller can occasionally experience a delay of 10 ms or less.

Identify Installed SFP Transceivers

In the FactoryTalk Linx RMCT, version 10.01 and later, you can identify the SFP transceivers that are installed in the dual SFP ports from the Module Info tab. The SFP Type Link 1 and SFP Type Link 2 fields display one of the following values:

- SFP Not Present
- SFP Not Supported
- 1783-SFP1GSX
- 1783-SFP1GLX
- 1783-SFP1GEXE
- 1783-SFP1GZX

For SFP transceiver technical specifications, see the ControlLogix and GuardLogix Controller Specifications Technical Data, publication [1756-TD001](#).

Figure 6 - SFP Transceiver Identification

Module Info | Configuration | Synchronization | Synchronization Status | System Update | Event Log

Redundancy Module Identification

Vendor: Rockwell Automation/Allen-Bradley
 Product Type: Redundancy Product
 Product Code: 4
 Revision: 21.11.119
 CIP Serial Number: 015D156B
 Catalog Number: 1756-RM3
 Manufacture Date: 2024/07/10
 Hardware Revision: 4.000
 Warranty Number: 321598065
 Series: A
 SFP Type Link 1: 1783-SFP1GLX
 SFP Type Link 2: SFP not Present
 Product Name: CLX Redundancy Premium Module

Status

General State: OK
 Major Fault: None
 Minor Fault: Yes

Event No.	Time Stamp	Severity	Code	Status
72	12/31/19...	Minor...	Fa...	Cleared
71	12/31/19...	Minor...	Fa...	Reported
70	12/31/19...	Minor...	No...	Cleared
69	12/31/19...	Minor...	No...	Reported
68	12/31/19...	Minor...	Fa...	Cleared
67	12/31/19...	Minor...	No...	Reported
66	12/31/19...	Minor...	Fa...	Cleared
65	12/31/19...	Minor...	Fa...	Reported
64	12/31/19...	Minor...	No...	Cleared
63	12/31/19...	Minor...	No...	Reported

Clear Fault

User-Defined Identity

Name:

Description:

Location:

Chassis B: Primary with No Secondary CH1: Not determined CH2: Not determined
 Auto-Synchronization State: Always

OK Apply Help

Notes:

Set Up a Redundancy System

The setup process of a redundancy system consists of the following:

- Firmware bundle installation
- Redundancy Module Configuration Tool (RMCT) installation
- Redundant chassis component installation and firmware updates
- Identification of the primary and secondary chassis
- Qualification and synchronization verification

After setup, you can reset, remove, and replace redundancy modules as needed.

Before You Begin

Before you set up a redundancy system, do the following:

- Make sure that the redundant chassis pair has the required matching components. See [Chapter 2](#). For best performance, place the redundancy module in the chassis as close as possible to the controller.
- Read and understand the safety and environmental considerations explained in the installation instructions for each component.
- Download and install the compatible versions of the Studio 5000 Logix Designer® application, communication software, and ControlFLASH Plus® software.

For information on how to download and install ControlFLASH Plus software, see the ControlFLASH Plus Quick Start Guide, publication [CFP-QS001](#).

IMPORTANT If communication software is already on your system, be sure to shut it down before you install or update software.

- Review the release notes for the firmware bundle that you are installing. Make sure that you have compatible hardware and the correct firmware revisions.
- Determine the IP address for each of your Ethernet/IP™ communication modules. Both communication modules in the redundant chassis pair usually have the same IP address. See [IP Address Swapping](#).

Download Redundancy Firmware

To download redundancy firmware, follow these steps.

1. Go to the Product Compatibility and Download Center (PCDC) at rok.auto/pcdc.
2. Search for the redundancy firmware bundle that corresponds to your redundancy system.

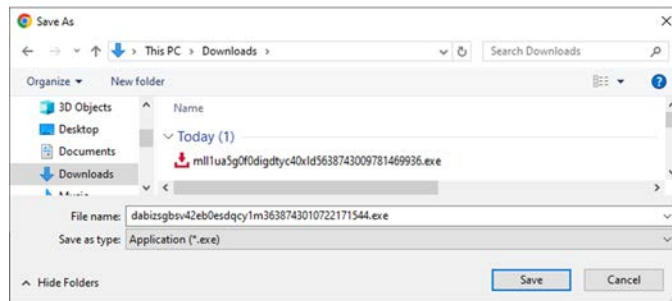
Redundancy System	Search Text
Logix SIS	Logix SIS Bundle
ControlLogix® 5580	1756-L8x Enhanced Redundancy Bundle
ControlLogix 5570	1756-Lxx Enhanced Redundancy Bundle

3. Select and download the firmware bundle revision.

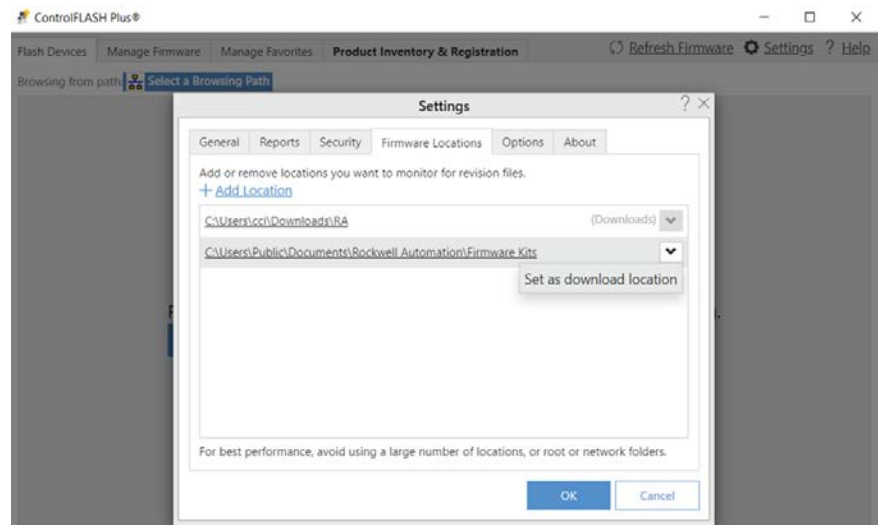
Install Redundancy Firmware

To install redundancy firmware, follow these steps.

1. Run the downloaded EXE file.



The executed file installs a DMK firmware file in the download location specified in your ControlFLASH Plus settings.



2. Verify that the DMK file is in the ControlFLASH Plus firmware kits location. You can manually move the DMK file if needed.

or

For the following earlier firmware revisions, see [Appendix E](#) for installation instructions:

- ControlLogix 5580 revisions earlier than 34.011_kit1
- ControlLogix 5570 revisions earlier than 34.051_kit1

Obtain the Redundancy Module Configuration Tool

The Redundancy Module Configuration Tool (RMCT) enables online operation and configuration of ControlLogix redundancy modules. Depending on your redundancy system, you can use the following:

- FactoryTalk® Linx RMCT
- RSLinx® RMCT

For compatible versions of FactoryTalk Linx RMCT or RSLinx RMCT with your redundancy system, see these resources:

- Release notes for your redundancy bundle or redundancy module on the Product Compatibility and Download Center (PCDC) at rok.auto/pcdc.
- Knowledgebase Technote [Redundancy Module Configuration Tool \(RMCT\)](#).

There are multiple ways to obtain the RMCT:

- Download it from the Product Compatibility and Download Center (PCDC).
- Download it as part of the redundancy bundle; however, not all bundles include the RMCT:
 - FactoryTalk Linx RMCT is not included in Logix SIS bundles or 1756-L8x enhanced redundancy bundles 34.0T1_kit1 or later.
 - RSLinx RMCT is included in 1756-L8x enhanced redundancy bundles 33 only.
 - RSLinx RMCT is included in 1756-Lxx enhanced redundancy bundles 33 or earlier.
- Download the FactoryTalk Linx RMCT as part of the Studio 5000 Logix Designer application.

For details about obtaining the RMCT, see the Knowledgebase Technote [Redundancy Module Configuration Tool \(RMCT\)](#).

Install the RMCT

FactoryTalk Linx RMCT must be installed on the same computer as the FactoryTalk Linx Network Browser. You can access FactoryTalk Linx RMCT only from the FactoryTalk Linx Network Browser.

To install the RMCT, follow these steps.

1. Browse to the RMCT directory on your computer.
2. Double-click setup.exe.
3. On the RMCT Setup dialog box, select Next.
4. When the installation is complete, select Finish.

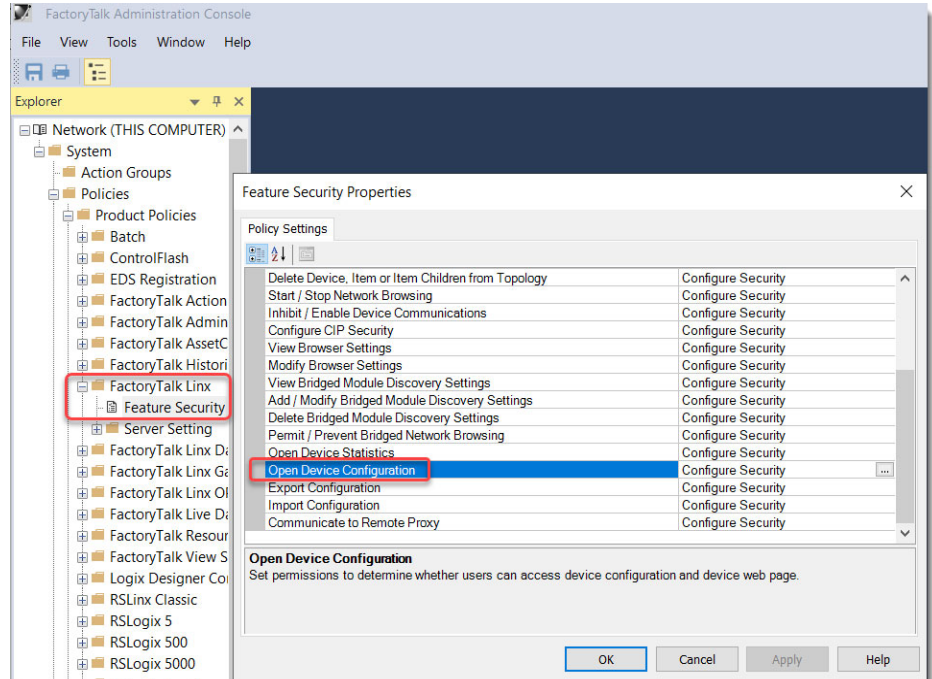
Access the RMCT

Once you have installed the RMCT, you can launch the tool from the FactoryTalk Linx Network Browser or from RSLinx software, depending on your environment.

Configuration Requirements for Access to FactoryTalk Linx RMCT

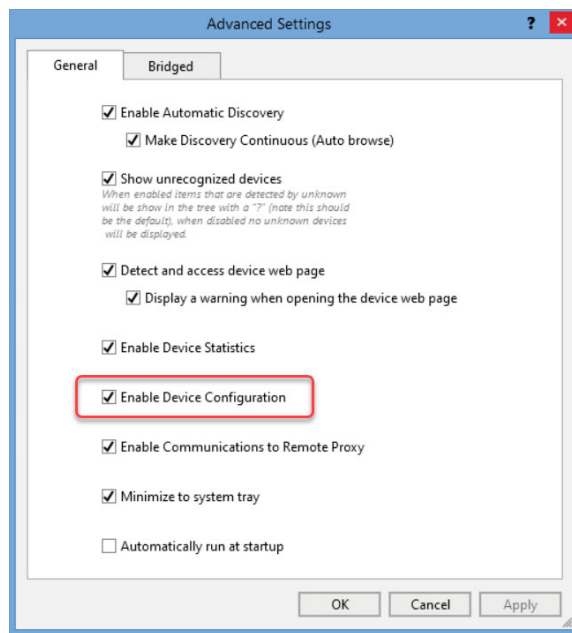
If you use FactoryTalk Security, you must have Open Device Configuration permission to access the tool. To configure Open Device Configuration permission, open FactoryTalk Administration Console, and then go to System > Policies > Product Policies > FactoryTalk Linx > Feature Security.

Figure 7 - Open Device Configuration Setting



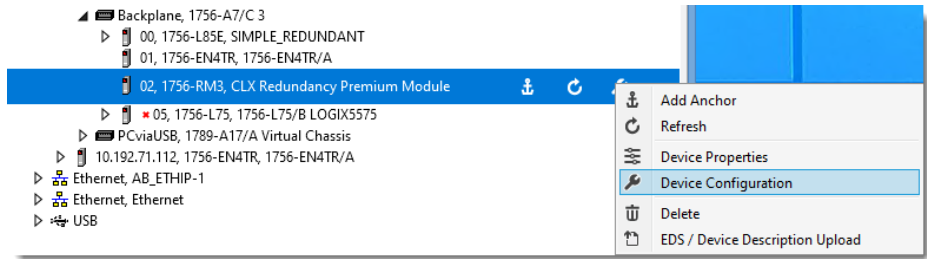
To access the RMCT in FactoryTalk Network Browser, the Enable Device Configuration setting must be selected. To verify that this setting is selected, open FactoryTalk Network Browser, and then open Advanced Settings.

Figure 8 - Enable Device Configuration Setting



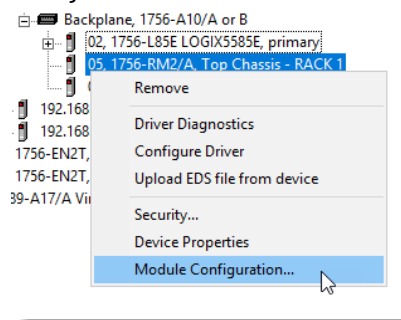
To access the RMCT, follow these steps.

1. Launch FactoryTalk Network Browser or RSLinx communication software.
2. Browse to your redundancy module.
3. If you are using FactoryTalk Linx Network Browser, right-click the redundancy module and select Device Configuration.



or

If you are using RSLinx software, right-click the redundancy module and select Module Configuration.



IMPORTANT

If you cannot see the Device Configuration menu option, then the compatible version of the RMCT is not installed. For more information, see [Identify the RMCT Version](#).

Identify the RMCT Version

You must use a version of the RMCT that is compatible with your redundancy module firmware. With RMCT version 20.054 or later, the RMCT receives compatibility information from the redundancy module firmware. If there is incompatibility, the RMCT shows only the Module Info tab and indicates the version that the firmware is compatible with. For more information about RMCT compatibility, see Knowledgebase Technote [Redundancy Module Configuration Tool \(RMCT\)](#).

The RMCT launches at the version that is compatible with the redundancy module firmware that is installed. If you have not updated your redundancy module firmware after updating your RMCT version, the RMCT version that is indicated can differ from the updated version that you installed. You can also check the RMCT version that is installed on your computer via Control Panel.

To identify the version of the RMCT that you have installed, follow these steps.

1. Access the RMCT.
2. Right-click the title bar and choose About.

The version that appears on the About dialog box is the earliest RMCT version that you need based on your bundle. The RMCT always shows the latest version that is installed. Later versions are backwards compatible with earlier versions.

Install Redundant Chassis Components

When you install redundant chassis components, be sure to match the slot locations of partner modules in each redundant chassis.

IMPORTANT Do not power on either chassis until you have installed all modules in both chassis.

For installation instructions, see the [Additional Resources](#).

1. Install the power supply or redundant power supplies for the first chassis.
2. Install and connect the redundancy modules in both chassis.
3. Install EtherNet/IP communication modules in the first chassis.
4. Install one controller in the first chassis.
5. Install the power supply or redundant power supplies in the second chassis.
6. Install the second chassis Ethernet/IP communication modules.
7. Install one controller in the second chassis of the redundant pair.

Convert a Standalone Chassis to a Redundant Chassis Pair

To convert a standalone chassis to a redundant chassis pair, follow these steps.

1. Insert a redundancy module in a spare slot in the standalone chassis.
2. Configure an identical chassis with compatible modules in the same slot as the standalone chassis.

For details about how to convert from a non-redundant system, see [Appendix H](#).

Update Firmware

Use ControlFLASH Plus software to update the firmware of each module in each chassis. For information on how to download, install, and use ControlFLASH Plus software, see the ControlFLASH Plus Quick Start Guide, publication [CFP-QS001](#).

IMPORTANT

- Apply power only to the chassis in which you are updating firmware.
- Redundancy module firmware that is contained in the redundancy firmware bundle is designed for use with redundancy modules.
- All modules in both chassis must use firmware from the same redundancy firmware bundle.

To update the firmware in each chassis, following these steps.

1. Apply power to the chassis.
2. Set the keyswitch on the controller to PROG.
3. Wait for the modules to complete their start-up scrolling status messages, and then check the status indicators.
During this time, the redundancy module conducts internal operations to prepare for an update.
4. Launch ControlFLASH Plus software and update the communication module that is the gateway to the other modules.
5. Update the redundancy module.
6. Once the firmware update is complete, verify that the redundancy module status displays PRIM, which indicates a successful update.
7. Use ControlFLASH Plus software to update the rest of the modules in the chassis.
8. Verify a successful update of each module with firmware revisions that match the revision in the firmware bundle.
9. Power off the chassis.

Identify the Primary and Secondary Chassis

IMPORTANT

- Do not apply power to the chassis until you have read the instructions for identifying the primary chassis. Applying power to the chassis in the correct order is crucial to identifying the primary and secondary chassis.
 - Make sure that both communication modules are set appropriately.
 - As a best practice, do not load an application until the primary and secondary racks are synchronized.
 - Before you identify the primary chassis and qualify the system, install the latest firmware. See [Update Firmware](#).
 - A secondary chassis stops functioning if it contains modules or firmware that are not compatible with redundancy systems.
-

To identify the initial primary and secondary chassis of a redundant chassis pair, complete these steps.

1. Verify that power is removed from both chassis.
2. Apply power to the chassis that you want to identify as the primary chassis and wait for the PRIM status message to appear on the front panel of the module.
3. Verify that all module pairs are at compatible firmware revision levels.
4. Apply power to the chassis that you want to identify as the secondary chassis.
5. Verify primary and secondary chassis designations by viewing the redundancy module status message display.

For information about status messages on the display, see [Appendix A](#).

Verify Qualification and Synchronization

After you identify the primary and secondary chassis and apply power to the redundant chassis pair, the redundancy modules run a series of checks and qualify the redundancy system. The qualification process begins automatically.

While qualification occurs, the status message on the module display transitions from DISQ (disqualified) to QFNG (qualifying) to SYNC (synchronized). The process completes in 1...3 minutes.

To verify the qualification and synchronization status, refer to the status messages on the modules in the redundant chassis pair as described in the following tables.

Table 14 - Synchronized System

Primary Chassis Display		Secondary Chassis Display	
Redundancy Module	Controller and Communication Module	Redundancy Module	Controller and Communication Module
PRIM	PwQS	SYNC	QS

Table 15 - Qualifying System

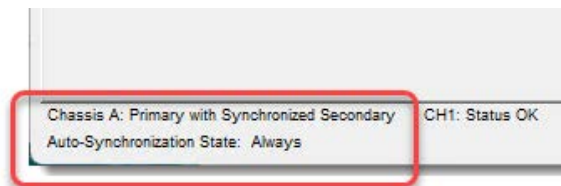
Primary Chassis Display		Secondary Chassis Display	
Redundancy Module	Controller and Communication Module	Redundancy Module	Controller and Communication Module
PRIM and QFNG	PQgS	QFNG	QgS

Table 16 - System with a Primary and Disqualified Secondary

Primary Chassis Display		Secondary Chassis Display	
Redundancy Module	Controller and Communication Module	Redundancy Module	Controller and Communication Module
PRIM	PwDS	DISQ	CMPT (modules compatible) or DSNP (no partner present)

In the RMCT, you can view the status of your system in the bottom-left corner of the dialog box.

Figure 9 - Redundancy System Status in RMCT



Download Your Application to the Primary Controller

After you verify that the system is synchronized, you can download your application to the primary controller. The primary controller automatically crossloads the application to the secondary controller.

Reset a Redundancy Module

There are two ways to reset a redundancy module:

- Cycle power to the chassis.

IMPORTANT Do not cycle power to the chassis if it causes you to lose control of your process.

- Remove the module from the chassis and reinsert the module.
- (1756-RM3 modules only). Reset the module to factory defaults in the FactoryTalk Linx RMCT, version 10.01 or later. See [\(1756-RM3 Modules Only\) Reset Factory Defaults](#).

IMPORTANT The redundancy module does not have secure reset functionality to make data nonrecoverable. To address critical security concerns about data recovery, Rockwell Automation recommends physically destroying a device when decommissioned.

Remove a Redundant Module

To remove a redundant module, push the locking clips at the top and bottom of the module and slide the module out of the chassis.

IMPORTANT If you remove a redundancy module, you lose redundancy functionality.
If you want to resume system operation with an identical module, you must install the new module in the same slot.

Replace a Redundant Module

To replace a redundant module, refer to one of the following procedures in [Appendix D](#):

- Perform a direct module replacement in the secondary chassis
- Perform a communication module series replacement
- Perform a redundancy module catalog number replacement

Notes:

Configure Redundancy Modules

No configuration is required for the operation of fiber channels on the redundancy modules:

- In 1756-RM3 modules, communication occurs on both channels. If one channel fails, communication persists on the other channel with no delay.
- In 1756-RM2 modules, the firmware automatically manages the selection of active and backup channels.

The default configuration of the redundancy modules lets you synchronize your redundant chassis without additional configuration. If needed, you can configure the following:

- User-defined identification of the redundancy module
- Redundancy module options in the Redundancy Module Configuration Tool (RMCT):
 - Change the Auto-synchronization setting
 - Assign a chassis ID
 - Configure user program control
 - Disable or re-enable fiber security on 1756-RM3 modules
- Date and time settings
- Disable or re-enable SFP fiber ports on 1756-RM3 modules

Protection Mode

Protection Mode is a state where the device is operational but has implemented defenses against disruptive changes that could take the product out of service.

Implicit Protection Mode

All 1756-RM3 catalog numbers enter Implicit Protection Mode when the redundant chassis pair is synchronized. Implicit Protection Mode helps prevent configuration changes that can affect system behavior and cause unintended and unforeseen changes.

This security enhancement is automatically triggered when the redundant chassis pair is in a synchronized state:

- For more information about synchronization in Logix SIS, see [page 29](#).
- For more information about synchronization in ControlLogix® redundancy, see [page 31](#).

In Implicit Protection Mode, the device deactivates services that could disrupt the operation of the device, but the device continues to function. For example, configuration operations or firmware updates are disabled so that they do not impact the operation of the device.

Restrictions in Implicit Protection Mode

When the redundancy module is in implicit Protection Mode, the mode prevents the following actions:

- Disable or re-enable fiber security
- Disable or re-enable SFP fiber ports
- Update the module firmware
- Perform any module resets, remote or out-of-the-box

Enter Redundancy Module Identification Information

You can enter general identification information about the redundancy module that is connected to the RMCT:

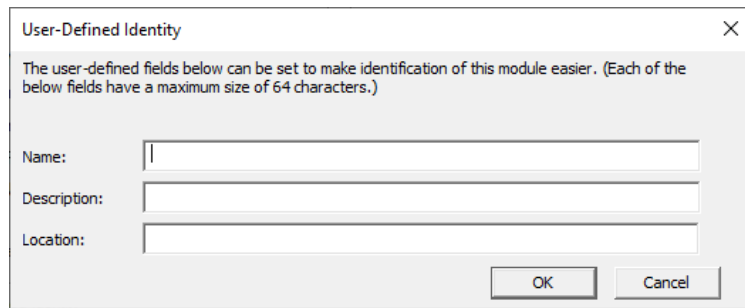
- Identification information is not crossloaded to the partner redundancy module.
- Identification information is maintained in nonvolatile memory, so that the chassis identity is retained through power cycles.

By default, identification parameters are empty.

To enter identification information for a redundancy module, follow these steps.

1. Access the RMCT.
2. Select the Module Info tab.
3. In the User-Defined Identity area, select Change.
4. Enter the identification information and select OK.

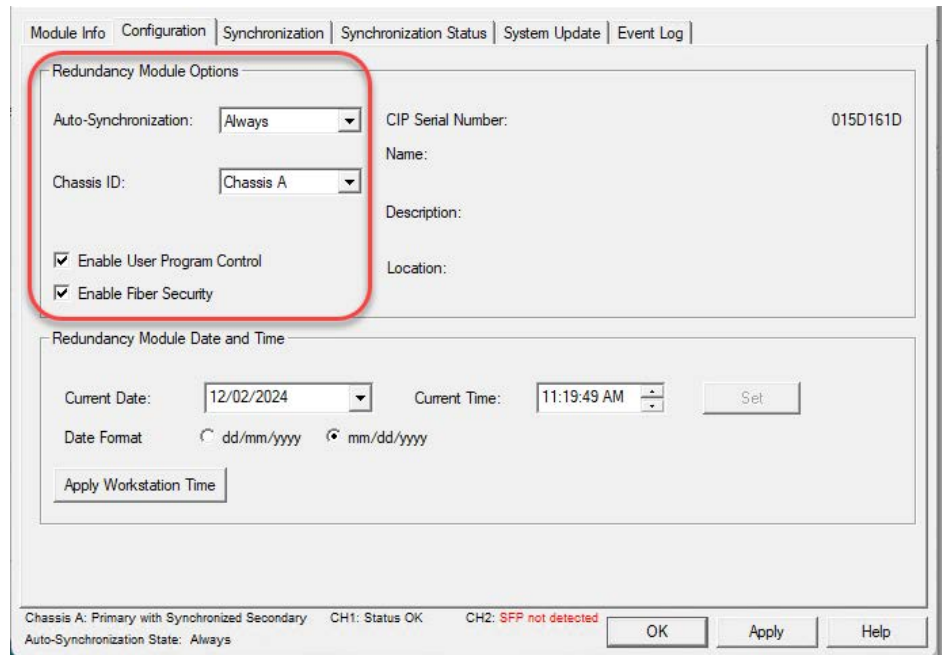
Figure 10 - Module Identification



Configure Redundancy Module Options

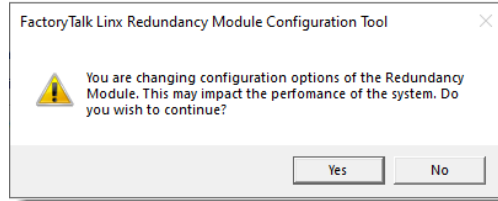
On the Configuration tab of the RMCT, you can configure the following options for a redundancy module:

- Auto-synchronization
- Chassis ID
- User program control
- Fiber security for 1756-RM3 catalog numbers



To configure redundancy module options, follow these steps.

1. Access the RMCT.
2. Select the Configuration tab.
3. Select the configuration options for your redundancy application as described in the following sections.
4. Select Apply.
5. When the following message appears, select Yes to confirm the change.



Choose an Auto-synchronization Setting

The setting that you choose for auto-synchronization determines a significant part of your redundancy system behavior. Use the setting that is recommended for your system as follows.

Table 17 - Auto-synchronization Setting

Redundancy System	Recommended Setting
Logix SIS	Never IMPORTANT: If you want to use the Always or Conditional setting, you must consider the impact to safety reaction calculations as described in the Logix SIS Safety Reference Manual, publication 1756-RM015 .
ControlLogix 5580	Always
ControlLogix 5570	Always

IMPORTANT

Before you modify your redundancy system, verify that the Auto-synchronization setting is correct. This verification helps prevent system errors.

For example, if you update your redundant system firmware, verify that this setting is Never or Conditional before disqualifying the secondary chassis. If the Auto-synchronization setting is Always, you cannot properly disqualify your chassis and conduct the update.

Use the following table to determine the auto-synchronization setting for your application.

Table 18 - Auto-synchronization Settings

Setting	Synchronization Behavior
Never	The system remains in the same state, either synchronized or disqualified, until one of these events takes place: <ul style="list-style-type: none"> • A command is issued from the RMCT to either synchronize or disqualify. • The controller commands synchronization or disqualification by using an MSG instruction. For this action to occur, Enable User Program Control must be selected. • A fault on the primary causes a switchover.
Always	The system automatically synchronizes regularly. If you attempt to disqualify the system by using the Disqualify Secondary command, the resulting disqualification is temporary as the system automatically qualifies and synchronizes again. If the controller disqualifies the system, the resulting disqualification is also temporary.
Conditional	The system behavior depends on the following: <ul style="list-style-type: none"> • If your Auto-synchronization setting is Conditional and your Auto-synchronization state is 'Conditional, Enabled', then the system continually attempts to synchronize. • If your Auto-synchronization setting is Conditional and your Auto-synchronization state is 'Conditional, Disabled', then the system does not automatically attempt to synchronize. To change from 'Conditional, Enabled' to 'Conditional, Disabled', select Disqualify Secondary on the Synchronization tab. To change from 'Conditional, Disabled' to 'Conditional, Enabled', select Synchronize Secondary on the Synchronization tab.

Assign a Chassis ID

To identify the physical chassis for a redundancy module as Chassis A or Chassis B, assign a chassis ID:

- If you change the chassis ID of the primary redundancy module, the secondary module is automatically assigned the other chassis ID.
- The chassis ID for a redundancy module becomes associated with its physical chassis, regardless of its primary or secondary control designation.

Configure User Program Control

User program control determines how redundancy modules respond to commands from the controller:

- To configure the redundancy modules to accept all valid commands via an MSG instruction from a Logix controller, enable user program control.
- To configure the redundancy modules to reject all commands from a Logix controller, disable user program control.

User program control is disabled by default.

(1756-RM3 Modules Only) Configure Fiber Security

Fiber security enables secure communication between partner 1756-RM3 modules.

IMPORTANT	Fiber security is enabled by default and can cause slower system performance, such as degraded scan time and qualification time. However, the switchover time is not affected. To avoid impact to system performance, you can disable the feature.
------------------	---

Fiber security cannot be disabled or re-enabled if the redundancy system is in Protection Mode. To exit Protection Mode, disqualify the secondary chassis by using the Disqualify Secondary command on the Synchronization tab of the secondary redundancy module. For more information about Protection Mode, see [page 18](#).

Whenever the fiber security configuration is changed, an event is logged in the event log.

Set the Redundancy Module Date and Time

The redundancy module date and time determines the time stamp that is recorded in event logs for the RMCT.

IMPORTANT We recommend that you set the redundancy module date and time when you commission a system. We also recommend that you periodically check the date and time settings to make sure that they match the settings of the controller. Regular verification of the date and time keeps the event logs of the redundancy modules accurate. Incorrect date and time information complicates troubleshooting if an event or error occurs on your redundant system.

The following methods can be used to set the date and time of a redundancy module:

- CIP Sync™ Time Synchronization for 1756-RM3 modules only
- Manual settings in the RMCT
- Custom MSG instruction in the controller program

IMPORTANT If the redundancy module receives its time via Time Synchronization, the time that is received from the Grandmaster overrides the date and time set manually in the RMCT or by an MSG instruction.

To understand the result of power loss on date and time settings, refer to the following table.

Power Loss Scenario	Result
Power is cycled to a redundancy module without a qualified partner	<ul style="list-style-type: none"> • In a 1756-RM3 module, the date and time settings are not retained. • In a 1756-RM2 module, the module powers up with the date and time that it had when the power was lost.
Power is cycled to a redundancy module with a qualified partner and the partner remains active during the power cycle	The date and time is transferred from the active partner to the other module during power-up.
Both partner modules shut off during a power failure	Date and time settings are not retained.

(1756-RM3 Modules Only) Set the Date and Time via Time Synchronization

With 1756-RM3 redundancy modules, you can use CIP Sync™ time synchronization, also known as Precision Time Protocol (PTP), to sync the redundancy module date and time with a Grandmaster in the same chassis. The redundancy module can only receive time from the Grandmaster and cannot transmit time. Time synchronization is automatically enabled in the redundancy module and no further configuration is possible.

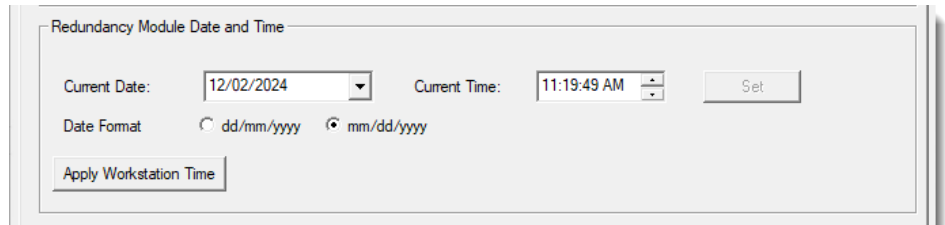
To enable time synchronization on the redundant controller, see [Enable Time Synchronization](#). For more information about CIP Sync time synchronization in redundancy systems, see [CIP Sync Time Synchronization](#).

Set the Date and Time via the RMCT

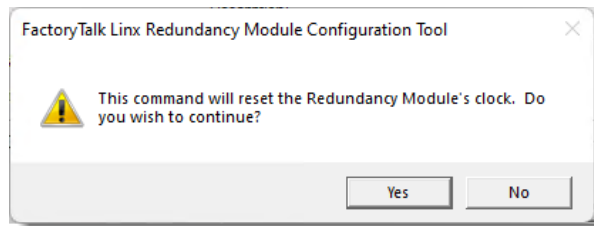
In the RMCT, you can set the date and time for the redundancy module.

To set the date and time via the RMCT, follow these steps.

1. Access the RMCT.
2. Select the Configuration tab.
3. In the Redundancy Module Date and Time area, set the time by using one of these methods:
 - Manually select the current date, current time, and date format, and then select Set.
 - or
 - Select Apply Workstation Time to use the date and time of the workstation.



4. When the following message appears, select Yes.

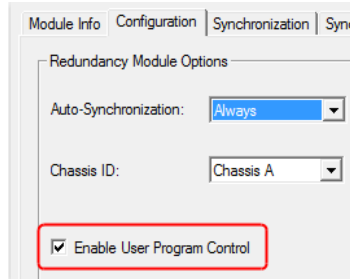


Set the Date and Time via an MSG Instruction

For some applications, consider programming the redundant controller to set the redundancy module date and time via an MSG instruction.

To set the date and time via an MSG instruction, follow these steps.

1. On the Configuration tab of the RMCT, verify that Enable User Program Control is selected for the redundancy module.



2. In the program for the redundant controller, create an MSG instruction.
3. On the Communication tab of the Message Configuration dialog box, configure the path to the redundancy module and verify that the Connected checkbox is cleared.

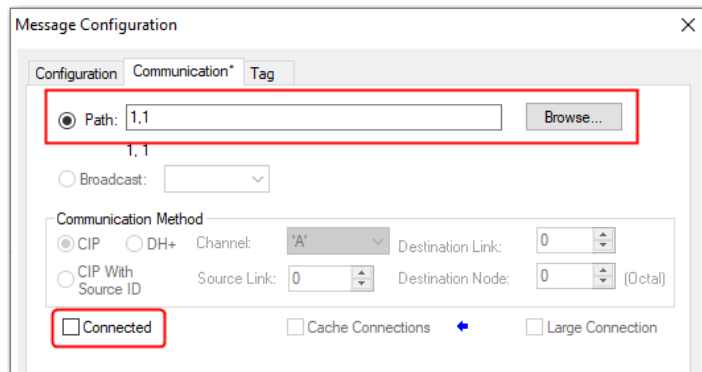


Table 19 - Date and Time Communication Parameters

Parameter	Value
Path	1,[slot number of the redundancy module] For example, enter 1,1 for a redundancy module in slot 1 of the chassis.
Connected	Leave the Connected checkbox cleared.

4. On the Configuration tab of the Message Configuration dialog box, configure the MSG instructions with the following parameters depending on the redundancy module catalog number.

Table 20 - 1756-RM3 Date and Time Configuration Parameters

Parameter	Value
Message Type	CIP™ Generic
Service Type	SSV
Service Code	10
Class	x43
Instance	1
Attribute	3 (System time in microseconds from epoch) 4 (System time in nanoseconds from epoch)
Source Element	LTIME
Source Length	8
Destination Element	None - no value needed.

Table 21 - 1756-RM2 Date and Time Configuration Parameters

Parameter	Value
Message Type	CIP Generic
Service Type	Custom
Service Code	10
Class	8b
Instance	1
Attribute	b
Source Element	WallClockTime[0] WallClockTime is a DINT[2] array that stores the CurrentValue of the WallClockTime object
Source Length	8
Destination Element	None - no value needed.

(1756-RM3 Modules Only) Reset Factory Defaults

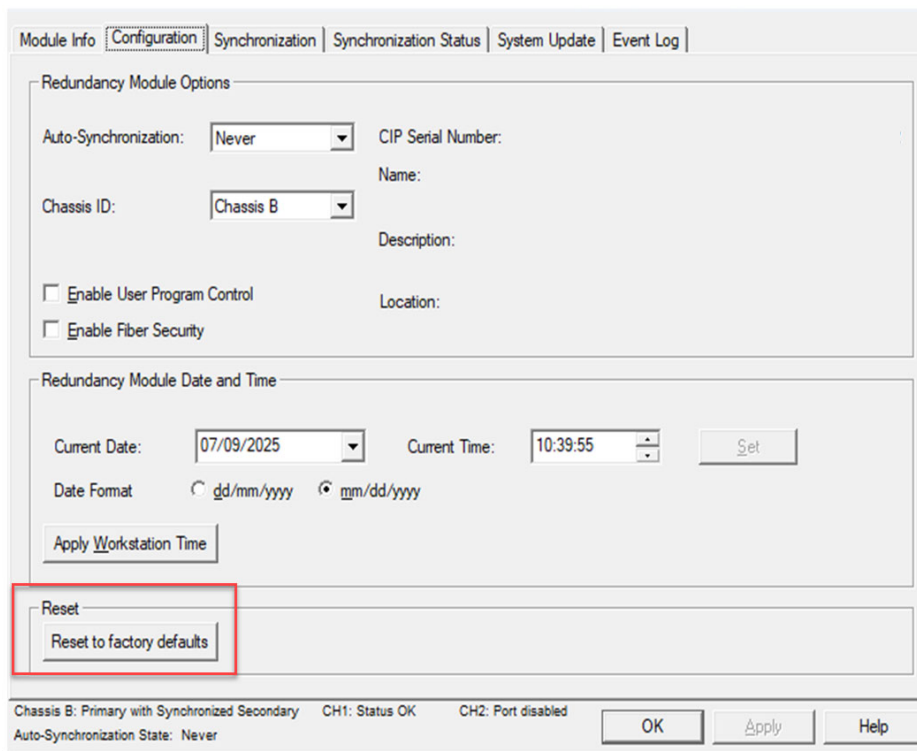
On the Configuration tab in the FactoryTalk Linx RMCT, version 10.01 or later, you can reset the redundancy module to its factory defaults when the redundant chassis pair is in a disqualified state.

After a reset, the following settings are restored on the redundancy module.

Table 22 - Factory Default Settings

Setting	Default
Module identification information (name, description, location)	Blank
Auto-synchronization	Conditional
Auto-synchronization state	Enabled
Chassis ID	Chassis A
Enable User Program Control	Disabled
Enable Fiber Security	Enabled

Figure 11 - Reset to Factory Defaults



(1756-RM3 Modules Only) Disable or Re-enable SFP Fiber Ports

If you do not plan to use one of the redundant SFP ports on a 1756-RM3 module, you can disable the port via an MSG instruction and re-enable the port when needed.

IMPORTANT The MSG instruction is allowed only when the redundant chassis pair is not synchronized. If the redundant chassis pair is synchronized, the message attempt fails and the port status and the port remain in their current state of being enabled or disabled.

IMPORTANT One SFP port must remain active on each redundancy module. If you are only using one SFP port on each module, you cannot disable the active ports.

To disable or re-enable an SFP port via an MSG instruction, follow these steps.

1. In the program for the redundant controller, create an MSG instruction.
2. On the Communication tab of the Message Configuration dialog box, configure the path and verify that the Connected checkbox is cleared, and then click Apply.

IMPORTANT The MSG must be sent to **both** partner redundancy modules, and the path to the secondary redundancy module cannot go through the redundancy module connection.

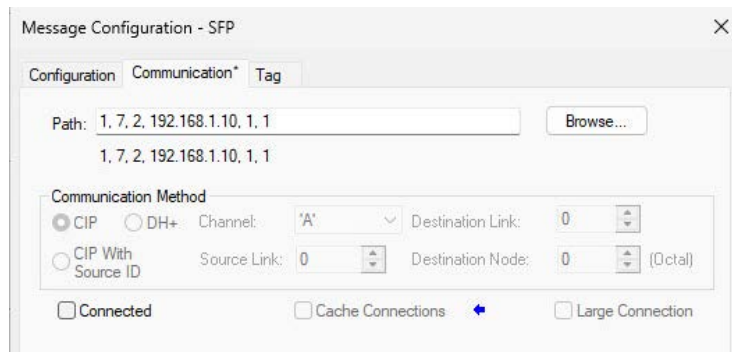


Table 23 - Communication Parameters—Disable or Re-enable SFP Port

Parameter	Value
Path	Primary: 1, [slot of primary redundancy module] Secondary: 1, 2, 2, [IP address of secondary communication module], 1, [slot of secondary redundancy module]
Connected	Leave the Connected checkbox cleared.

- On the Configuration tab of the Message Configuration dialog box, configure the MSG instruction with the following parameters, and then click Apply.

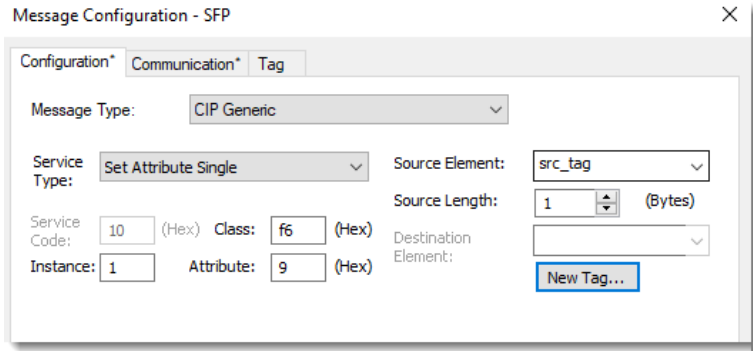


Table 24 - Configuration Parameters—Disable or Re-enable SFP Port

Parameter	Value
Message Type	CIP Generic
Service Type	Set Attribute Single
Service Code	None - no value needed
Class	F6 (EthernetLinkObject)
Instance	1 (port 1) 2 (port 2)
Attribute	9 (AdminState)
Source	Source tag - DINT - 1 (enable port), 2 (disable port)
Source Length	1
Destination Element	None - no value needed

Configure the EtherNet/IP Network

Before you begin to configure the communication modules in the redundant chassis pair, verify the following:

- The redundancy modules are installed and connected in the redundant chassis.
- The partner communication modules are able to communicate to each other over the Ethernet network.
- You know the subnet mask and gateway address for the Ethernet network on which the redundant communication modules operate.

Requested Packet Interval (RPI)

The RPI for I/O connections in a redundant-enabled controller tree is configured the same way as with a simplex controller. The RPI rates of I/O connections impact the loading of the associated EtherNet/IP™ communications modules:

- In controller firmware revisions earlier than 20.054, the RPI for I/O connections in a redundancy-enabled controller must be less than or equal to 375 ms.
- In controller firmware revision 20.054 or later, the RPI can be the same as a non-redundant chassis.

1756-EN4TR Module Considerations

For all communication module catalog numbers beginning with 1756-EN4TR, keep the RPI rate for I/O connections such that the I/O packet rate is under 80% of the maximum (50,000 packets/second).

1756-EN2T Module Considerations

This table describes CPU usage considerations for all communication module catalog numbers beginning with 1756-EN2T.

CPU Utilization Percent	Action
0...80%	No action is required. Important: This range is the optimal rate.
Greater than 80%	<ul style="list-style-type: none"> • Take steps to reduce your CPU utilization. • Adjust the RPI of your connections. • Reduce the number of devices that are connected to your module. • Add another communication module to the redundant chassis pair (7, max) Important: Your communication module can function at 100% CPU capacity, but at or near this rate, you run the risk of CPU saturation and performance degradation.

Concurrent Communication

Concurrent communication provides seamless failover for any redundant pair of hardware components. With concurrent communication, data transmission between supported controllers and I/O modules can be redundant at the logical and physical levels. For details about concurrent communication operation, see the ControlLogix EtherNet/IP Network Devices User Manual, publication [1756-UM004](#).

Concurrent communication can be used with the following I/O:

- FLEXHA 5000™ I/O modules
- FLEX 5000® safety I/O modules

You must use any of the following communication modules to establish concurrent communication with FLEXHA 5000 I/O modules and FLEX 5000 safety I/O modules:

- 1756-EN4TR
- 1756-EN4TRK
- 1756-EN4TRXT

System Requirements

The following tables provide the supported firmware revisions for concurrent communication system components.

Table 25 - Firmware Revisions for Concurrent Communication with FLEXHA 5000 I/O Modules

Redundancy System	Controller	1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT Modules	FLEXHA 5000 EtherNet/IP Adapters	FLEXHA 5000 I/O Modules
Logix SIS	37.011 or later	7.001 or later	3.011 or later	3.011 or later
ControlLogix® 5580	35 or 36 (all revisions)	5 or 6 (all revisions)	2 or earlier (all revisions)	2 or earlier (all revisions)
	37.011 or later	7.001 or later	3.011 or later	3.011 or later
ControlLogix 5570	Not supported	—	—	—

Table 26 - Firmware Revisions for Concurrent Communication with FLEX 5000 Safety I/O Modules

Redundancy System	Controller	1756-EN4TR, 1756-EN4TRK, 1756-EN4TRXT Modules	FLEX 5000 EtherNet/IP Adapter	FLEX 5000 Safety I/O Modules
Logix SIS	37.011 or later	7.001 or later	6.011 or later	All revisions
ControlLogix® 5580	Not supported	—	—	—
ControlLogix 5570	Not supported	—	—	—

Configuration Requirements

To configure 1756-EN4TR, 1756-EN4TRK, or 1756-EN4TRXT modules for concurrent communication, apply the following settings:

- In the device definition and on the physical modules, set the communication modules to use different IP addresses.
- In the device definition, set the Concurrent Communication setting to Yes.

Figure 12 - Concurrent Communication Setting

The screenshot shows the 'Device Definition' dialog box for a 1756-EN4TR module. The 'Concurrent communication' dropdown menu is highlighted with a red circle and is set to 'Yes'. Other settings include: Device type: 1756-EN4TR 1756 Ethernet Bridge, 2-Port, Twisted-pair Media; Revision: 5.001; Name: Ethernet_IP_comm_module; Electronic keying: Compatible Module; Rack connection: None; Time sync and motion connection: Yes; Ethernet Address Module 1: 192.168.1.101; Ethernet Address Module 2: 192.168.1.102; Slot: 1; Redundant: Chassis Pair. Buttons for OK, Cancel, and Help are visible at the bottom right.

When you apply the preceding settings, the following occurs automatically:

- IP address swapping is disabled.
- The connection type is set to unicast.
- The I/O modules automatically connect to the communication module with concurrent communication. No additional configuration is required.
- Class 1 connections to I/O modules that do not support concurrent communication require an additional communication adapter that is not configured for concurrent communication. Class 3 connections are supported, however.

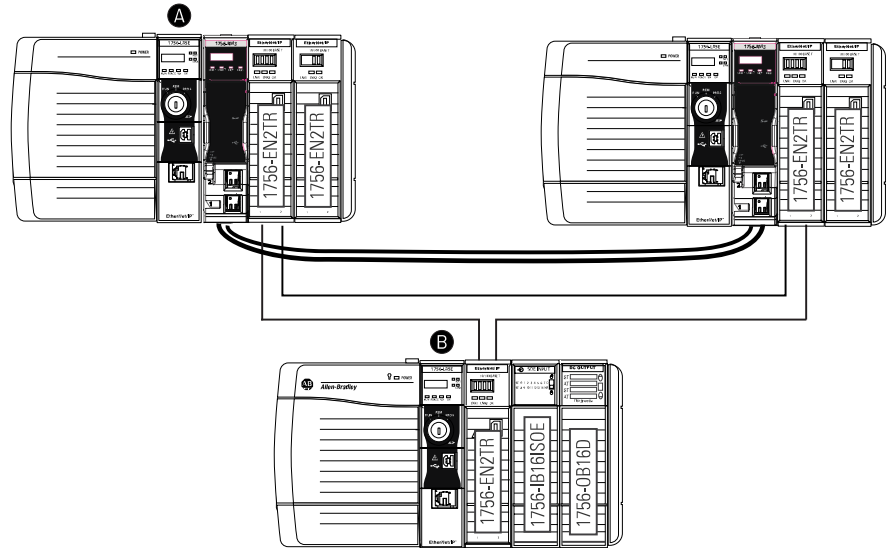
Produced and Consumed Tags

Produced and consumed safety tags are not supported in Logix SIS redundancy.

In redundancy systems, controllers let you produce (send) and consume (receive) system-shared tags over an EtherNet/IP network.

IMPORTANT A redundant controller can produce tags to a standard controller using unicast or multicast. Redundant controllers must always consume tags using multicast.

Figure 13 - Example System Using Produced and Consumed Tags

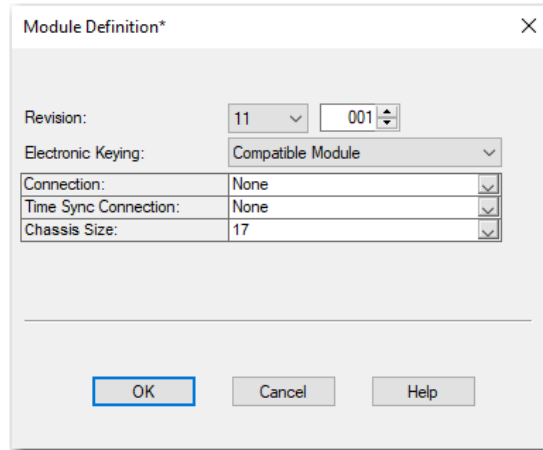


Item	Description
A	Controller 1 produced tag
B	Controller 2 consumed tag

Produced and consumed tags in redundancy systems have the following requirements and restrictions:

- You cannot bridge produced and consumed tags over two networks. For two controllers to share produced or consumed tags, both must be attached to the same network.
- Produced and consumed tags use connections in the controllers and the communication modules.
- Because the use of produced and consumed tags uses connections, the number of connections available for other tasks, such as the exchange of I/O data, is reduced.
- The number of connections available in a system depends on the type of controller and types of communication modules. Closely track the number of produced and consumed connections to leave as many as necessary for other system tasks.
- When configuring a tag to be consumed by a redundant controller, the tag configuration in the remote controller (the producer) and the consumer controller in the redundant chassis pair must be configured to be multicast.
- When configuring a tag to be produced by a redundant controller, the tag can be configured as multicast if there are multiple consumers or unicast if there is one consumer.

IMPORTANT To avoid a drop in connection during a switchover, when you add a communication module for the redundant chassis to the I/O tree of a remote consuming controller, change the Connection setting from Rack Optimized to None.



Produced and Consumed Tags between Primary and Non-redundant Controllers

The connection between the primary redundant controller and non-redundant controllers in a remote chassis can drop briefly during a switchover under these conditions:

- Certain non-redundant controllers or communication modules in the remote chassis do not meet minimum firmware requirements.
- and
- The redundant controllers produce tags over the EtherNet/IP network that the non-redundant controllers in the remote chassis consume.

The following tables list the minimum firmware revisions that are required for affected devices. For devices not listed, there are no minimum firmware requirements.

Table 27 - Remote Chassis Controller Requirements

Controller in Remote Chassis	Minimum Firmware Revision
CompactLogix® 1769-L2x	19.011
CompactLogix 1769-L3xE	

Table 28 - Remote Chassis Communication Module Requirements

Communication Module in Remote Chassis	Minimum Firmware Revision
1756-EN4TR	2.001
1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	4.002
1756-ENBT	6.001
1768-ENBT	4.001
1788-ENBT	3.001

Static Versus Dynamic IP Addresses

A static IP address is manually assigned, and does not change. A dynamic IP address is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server and can change over time.

We recommend that you use static IP addresses for communication modules in redundancy systems. You cannot use dynamic IP addresses with IP address swapping.



ATTENTION: If you use dynamic IP addresses and a power outage, or other network failure occurs, modules that use dynamic IP addresses can be assigned new addresses when the failure is resolved. If the IP addresses change, your application could experience a loss of control or other serious complications with your system.

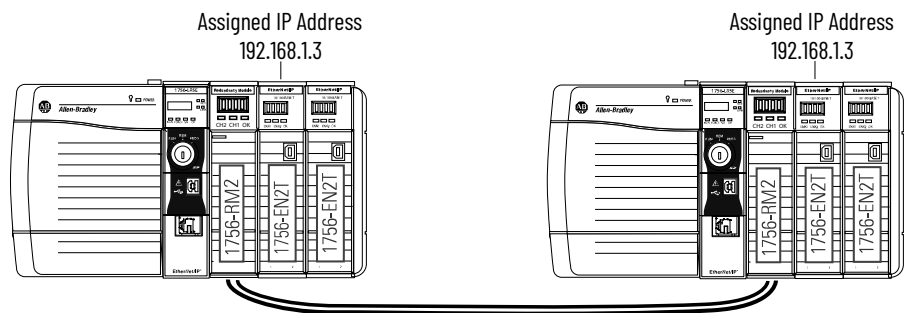
IP Address Swapping

IP address swapping enables a partnered set of communication modules that are on the same subnet to swap IP addresses during a switchover.

IMPORTANT IP address swapping does not apply to systems that use concurrent communication, such as Logix SIS with FLEX 5000 safety I/O or ControlLogix 5580 systems with FLEXHA 5000 I/O.

The following example shows partnered communication modules during initial configuration.

Figure 14 - IP Addresses During Initial Configuration

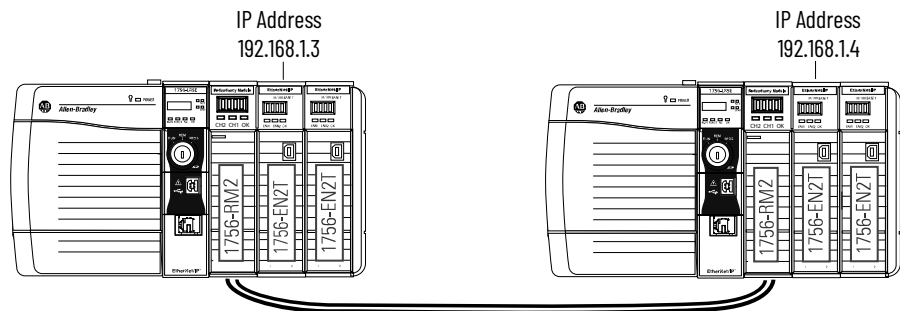


When redundancy operation begins, the primary communication module uses the IP address that is assigned during initial configuration. The secondary communication module automatically changes its IP address to the next highest value. When a switchover occurs, the communication modules swap IP addresses.

EXAMPLE If you assign IP address 192.168.1.3 to both communication modules, on initial system operation, the secondary EtherNet/IP communication module automatically changes its IP address to 192.168.1.4

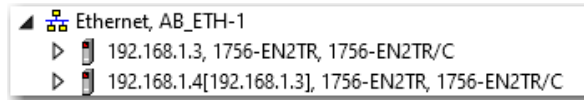
The following example shows partnered communication modules after system operation begins.

Figure 15 - IP Addresses After System Operation Begins



The following figure shows the partnered communication modules in the communication software after system operation begins.

Figure 16 - IP Addresses in Communication Software



Determine Whether to Use IP Address Swapping

Use the following table to determine whether your application requires IP address swapping.

Configuration	Required Applications	Considerations
IP address swapping	<ul style="list-style-type: none"> Remote I/O Produced/consumed connections 	<p>Plan to use consecutive IP addresses for partnered communication modules. Configure the IP address, subnet mask, and gateway address for each partnered communication module with the same values. Do not assign IP addresses to communication modules outside the partnered set to values that conflict with values that are used in the partnered set.</p> <p>EXAMPLE: The partnered set uses IP addresses 192.168.1.3 and 192.168.1.4. Use 192.168.1.5 or higher for all communication modules outside the partnered set.</p>
Non IP address swapping	<ul style="list-style-type: none"> Your system uses concurrent communication. Your system uses dynamic IP address assignments. You want to minimize data server communication recovery time during a switchover. Partnered set of communication modules are on different subnets. If you use different subnets, you are responsible for programming your system to use the address and subnet of the new primary chassis if a switchover occurs. 	<p>If you do not use IP address swapping, plan to use two IP addresses. Assign unique IP address values for partnered communication modules. To help differentiate IP address swapping modules from other configurations, we recommend that you avoid setting the IP addresses for the partnered modules to the following format: aaa.bbb.ccc.ddd and aaa.bbb.ccc.(ddd+1).</p> <p>EXAMPLE: The partnered set uses IP addresses 192.168.1.3 and 192.168.1.5. Use 192.168.1.6 or higher for all communication modules outside the partnered set.</p>

Set Communication Module IP Addresses

By default, EtherNet/IP communication modules ship with the rotary switches set to 999 and with Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP) enabled.

Use any of these tools to set the IP addresses for your EtherNet/IP communication modules:

- Rotary switches on the module
- Communication software
- Programming software
- BOOTP/DHCP utility

Reset an IP Address

You can reset the IP address of an EtherNet/IP communication module to the factory default value. To return to the factory default, follow these steps.

1. Set the rotary switches on the module to 888.
 2. Restart the communication module.
 3. Set the switches on the module to the desired address.
- or
- Set the switches to 999.

Half/Full Duplex Settings

A redundancy system uses the duplex settings of the primary communication module. After a switchover, the duplex settings of the new primary communication module are used. By default, the duplex setting is set to automatic. We recommend that you use this setting whenever possible.

To avoid communication errors, configure the primary and secondary communication modules with the same duplex settings. If you use different duplex settings on partnered communication modules, then communication errors can occur after a switchover.

Device Level Ring (DLR)

DLR is an EtherNet/IP protocol that is defined by ODVA. DLR provides a means to detect, manage, and recover from a single fault in a ring-based network.

A DLR network includes the following types of ring nodes.

Node	Description
Ring supervisor	<p>A ring supervisor provides these functions:</p> <ul style="list-style-type: none"> • Manages traffic on the DLR network • Collects diagnostic information for the network <p>A DLR network requires at least one node to be configured as ring supervisor. By default, the supervisor function is disabled on supervisor-capable devices.</p>
Ring participants	<p>Ring participants provide these functions:</p> <ul style="list-style-type: none"> • Process data that is transmitted over the network. • Pass on the data to the next node on the network. • Report fault locations to the active ring supervisor. <p>When a fault occurs on the DLR network, ring participants reconfigure themselves and relearn the network topology.</p>
Redundant gateways (optional)	<p>Redundant gateways are multiple switches that connect to a DLR network and also connect together through the rest of the network. Redundant gateways provide DLR network resiliency to the rest of the network.</p>

Depending on their firmware capabilities, devices and switches can operate as supervisors or ring nodes on a DLR network. Only some devices, such as switches, can operate as redundant gateways.

For more information about DLR, see the EtherNet/IP Device Level Ring Application Technique, publication [ENET-AT007](#).

Use DLR in a Redundancy System

For supported DLR I/O network topologies and design guidelines for high availability systems, including ControlLogix 5580 redundancy and Logix SIS, see the High Availability Systems Reference Manual, [HIGHAV-RM002](#).

Parallel Redundancy Protocol (PRP)

PRP is defined in international standard IEC 62439-3 and provides high-availability in Ethernet networks. PRP technology creates seamless redundancy by sending duplicate frames to two independent network infrastructures, which are known as LAN A and LAN B.

A PRP network includes the following components.

Component	Description
LAN A and LAN B	Redundant, active Ethernet networks that operate in parallel.
Double attached node (DAN)	An end device with PRP technology that connects to LAN A and LAN B.
Single attached node (SAN)	An end device without PRP technology that connects to LAN A or LAN B. A SAN does not have PRP redundancy.
Redundancy box (RedBox)	A switch with PRP technology that connects devices without PRP technology to LAN A and LAN B.
Virtual double attached node (VDAN)	An end device without PRP technology that connects to LAN A and LAN B through a RedBox. A VDAN has PRP redundancy and appears to other nodes in the network as a DAN.
Infrastructure switch	A switch that connects to either LAN A or LAN B and is not configured as a RedBox.

For more information about PRP, see the EtherNet/IP Parallel Redundancy Protocol Application Technique, publication [ENET-AT006](#).

Use PRP in a Redundancy System

For supported PRP I/O network topologies and design guidelines for high availability systems, including ControlLogix 5580 redundancy and Logix SIS, see the High Availability Systems Reference Manual, [HIGHAV-RM002](#).

CIP Sync Time Synchronization

CIP Sync™ time synchronization provides a mechanism to synchronize clocks between controllers, I/O devices, and other automation products in your architecture with minimal user intervention. CIP Sync uses Precision Time Protocol (PTP) to establish a Time Transmitter/Time Receiver relationship among the clocks for each PTP-enabled component in the system. One clock, which is known as the Grandmaster, sets the clock to which all other devices on the network synchronize their clocks.

Use Time Synchronization in a Redundancy System

The following considerations apply to time synchronization in a redundancy system:

- If you enable time synchronization for controllers in a redundant chassis pair, you must also enable time synchronization for one of the communication modules in the redundant chassis pair so that all devices have one path to the Grandmaster. To enable time synchronization for communication modules, change the Time Sync Connection from None (default) to Time Sync and Motion.

If time synchronization is enabled for any controller in the primary chassis of a disqualified redundant chassis pair and no other device in the primary chassis has time synchronization enabled, the redundant chassis pair attempts to qualify. However, in these application conditions, the attempt to synchronize fails and the application remains in the qualifying state for up to 10 minutes before failing qualification. If viewed in the RMCT, the system status remains at 85% complete.

- While time synchronization can handle multiple paths between Time Transmitter and Time Receiver clocks, the most effective method is to configure the redundant paths so that time synchronization is enabled in only the minimum required number of communication modules. We recommend that time synchronization has exactly one path through the system with no loops.

- If the primary controller is the Grandmaster, the redundancy system automatically manages the clock attributes so that the controller in the primary chassis is always set to be the Grandmaster instead of the secondary controller.

IMPORTANT We recommend that the Grandmaster is outside of the redundant chassis pair if possible. If there are time sensitive devices that depend on the clock, there can be a step in the time during switchover.

- When a switchover occurs, the Grandmaster status transfers from the original primary controller to the new primary controller. This transfer can take longer to complete than if Grandmaster status was transferred between devices in a non-redundant system.

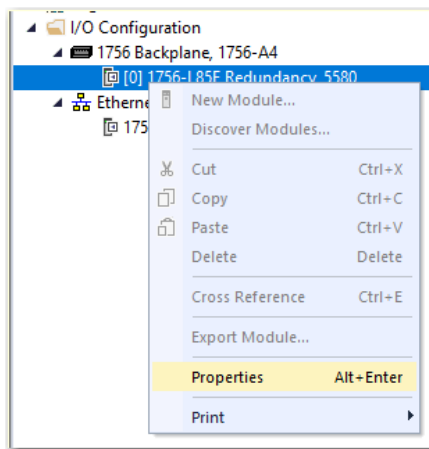
Configure the Redundant Controller

Redundant controllers both use the same controller program. You do not need to create a separate project for each controller.

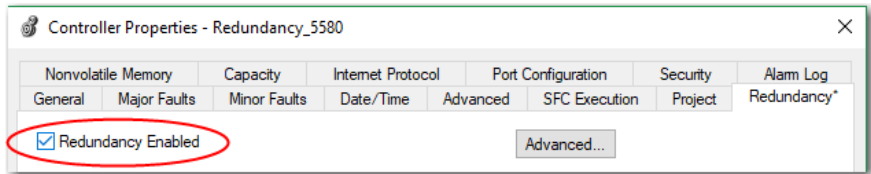
IMPORTANT Unless a workflow dictates that the controller in the secondary chassis requires modification, only interface with the controller in the primary chassis.

To configure your controllers to operate in a redundant system, complete these steps.

1. Open or create a project for your redundant controller.
2. Access the Controller Properties dialog box for the controller.



3. Select the Redundancy tab, and then select the Redundancy Enabled checkbox. To edit the Redundancy Enabled setting, you must be offline.



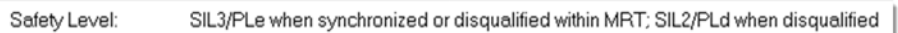
4. For a safety controller with firmware revision 37, select the Safety tab and verify that the safety level is set to SIL2/PLd.



While Logix SIS does support SIL 3 safety functions, the configuration setting must be SIL2/PLd when a safety controller is enabled for redundancy in firmware revision 37.

With firmware revision 38 or later, the safety level is automatically set to the following static value:

SIL3/PL3 when synchronized or disqualified within MRT; SIL2/PLd when disqualified



For more information, see [SIL 2 and SIL 3 Safety Functions](#).

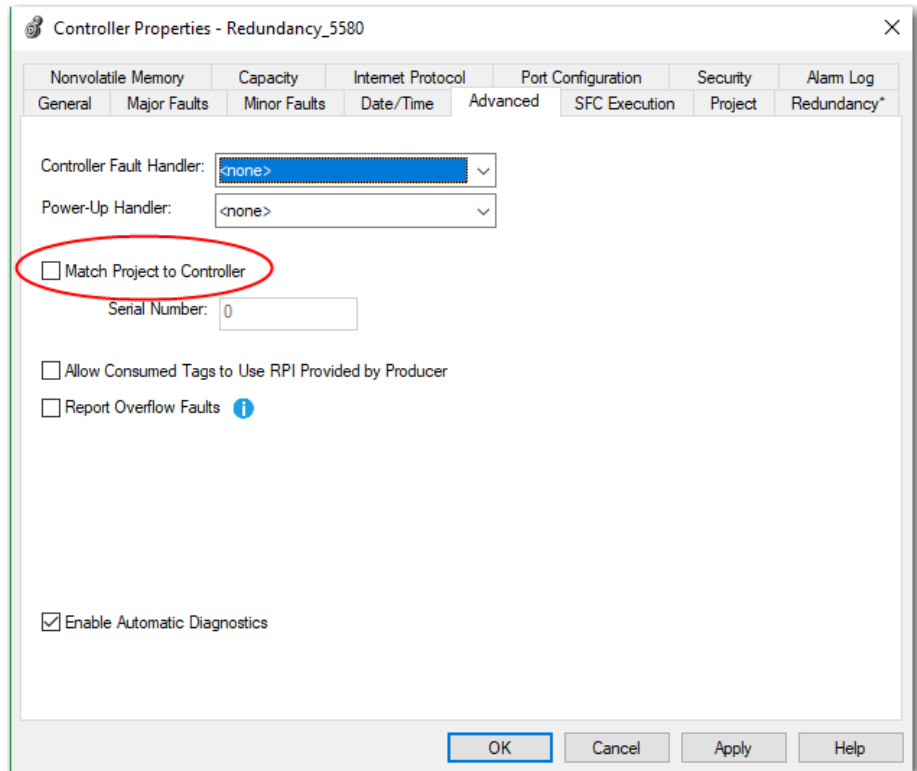
5. If you plan to modify the controller while online, see [Plan for Test Edits](#) for information about the parameters available in the Advanced settings.

6. Select the Advanced tab, verify that Match Project to Controller is cleared and select Apply.

IMPORTANT

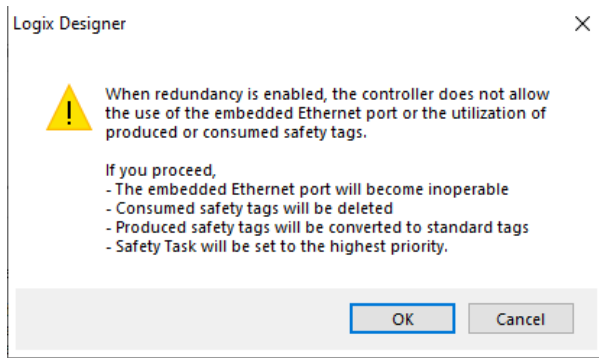
Do not select the Match Project to Controller parameter with redundancy. If you select Match Project to Controller, you cannot go online with, download to, or upload from the new primary controller after a switchover.

The serial number of the new primary controller is not the same as the serial number of the old primary controller and the project cannot be matched to the newly switched to controller.



7. When a warning message appears, carefully read the implications of enabling redundancy on the controller, and select OK to proceed.

The implications of enabling redundancy vary depending on the type of controller. For information about feature support and restrictions in redundancy systems, see [Chapter 1](#).



8. On the Controller Properties dialog box, select OK.

You have completed the minimum configuration that is required for redundant controllers.

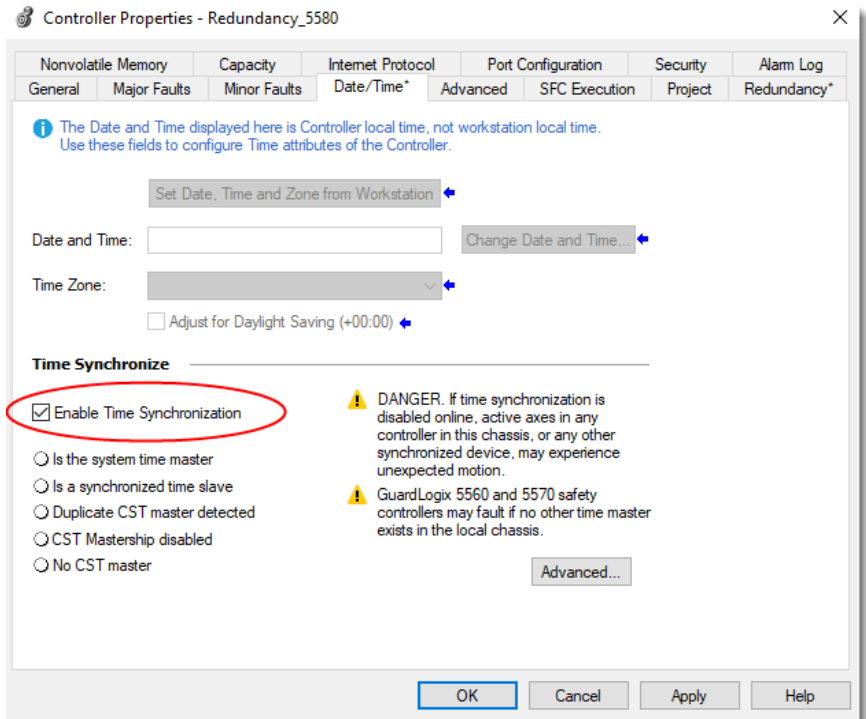
Enable Time Synchronization

CIP Sync™ time synchronization is not required for redundancy to function.

- IMPORTANT**
- If you use 1756-RM2 redundancy modules and earlier, do not use CIP Sync™ time synchronization if it is not required. The feature can increase crossload time and use a significant amount of processing power in the redundancy module. Only use time synchronization if required by an application element, such as Logix tag-based alarms or Sequence of Event (SOE) modules in a remote chassis.
 - If you use 1756-RM3 redundancy modules, time synchronization does **not** impact crossload time or processing power.

If your application requires time synchronization, follow these steps.

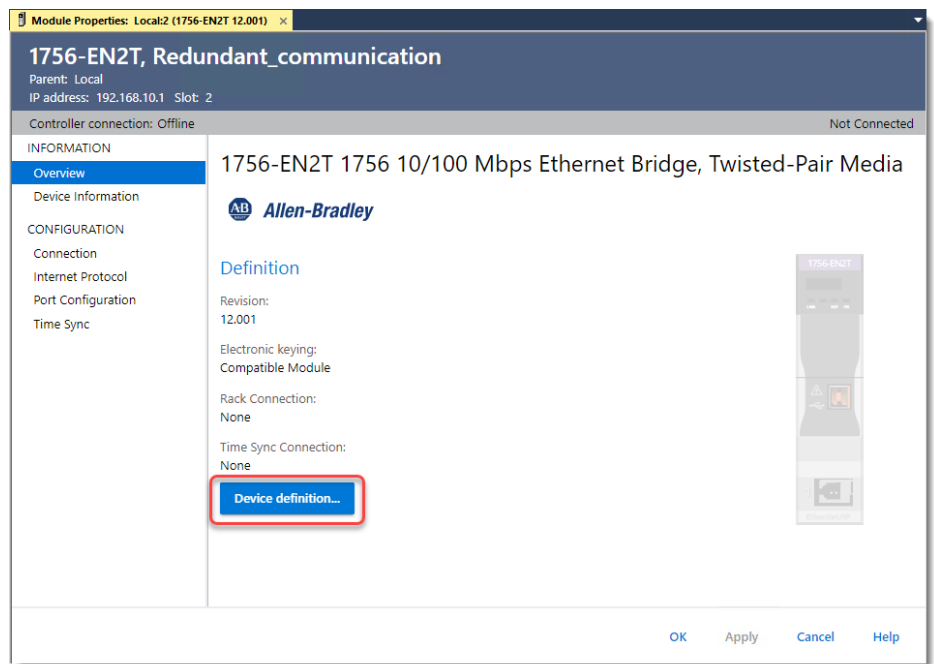
1. On the Date/Time tab in the controller properties, select Enable Time Synchronization.



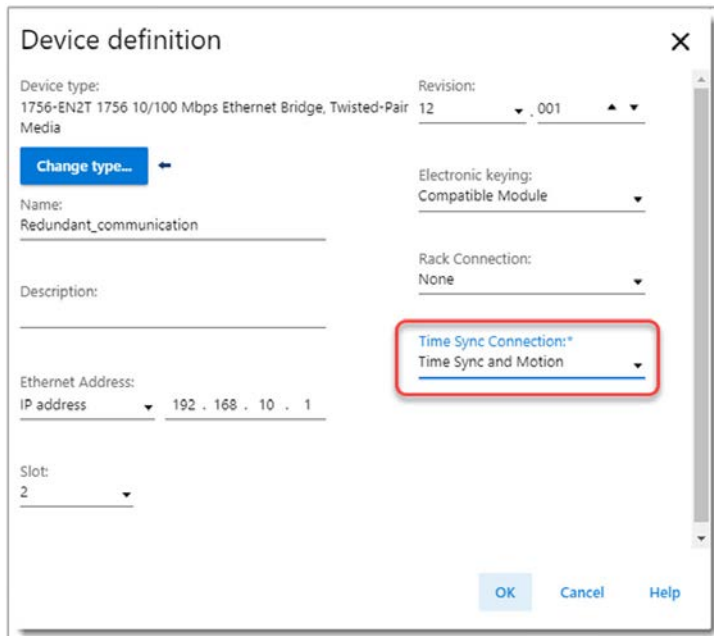
2. Select Apply and then OK.
3. When a message appears, select Yes.
4. Open the module properties for the communication module.

5. Select Overview and then Device definition.

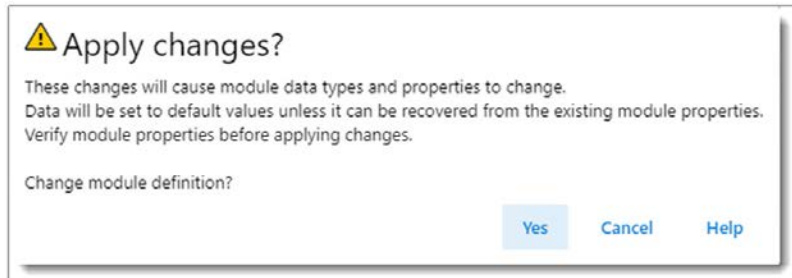
IMPORTANT At least one communication module requires this configuration if time synchronization is enabled on the controller. For more information, see the Knowledgebase Technote [Troubleshooting ControlLogix Redundancy Systems](#).



6. From the Time Sync Connection menu, select Time Sync and Motion and then OK.



7. When the following warning appears, select Yes.



Crossloads, Synchronization, and Switchovers for Standard Tasks

The operation of crossloads, synchronization, and switchovers described in the following sections applies only to standard tasks in Logix SIS, ControlLogix® 5580, and ControlLogix 5570 redundancy systems.

IMPORTANT The safety task in Logix SIS uses concurrent execution on both controllers and does not operate the same as standard tasks. However, like standard tasks, the safety task executes slower in redundancy systems due to cross-compare diagnostics.

Crossloading or synchronization points are points where the primary controller transfers data to the secondary controller. Crossload and synchronization points keep the secondary controller ready to assume control if there is a fault on the primary controller.

Before you configure your redundant controller, be aware of the impact of crossloads and synchronization on the execution of a task or program after a switchover. If you understand these concepts, you can create programming that best meets the needs for your redundant application.

Configure Crossload and Synchronization Settings

In a redundancy system, crossload and synchronization points within the Studio 5000 Logix Designer® project are configurable. You can limit which tasks or programs crossload and synchronize data after execution. In many applications, changes to this setting can reduce the overall impact to the task scan time by reducing the number of times data is crossloaded.

Standard Task Settings

In Logix Designer version 37 or later, you can improve standard task scan time by disabling data synchronization for a task. When data synchronization is disabled, no data is transferred to the secondary controller after the task executes, including the last program in its program list.

IMPORTANT At least one standard user task in your application must have data synchronization enabled. The highest priority standard task with data synchronization enabled can achieve a seamless switchover.

Disabling data synchronization is useful for tasks that do not need to retain their state after a switchover.

IMPORTANT We recommend that you do not disable data synchronization for tasks that use SSV instructions. If the task contains SSV instructions, the task can experience spikes in scan times while those instructions are synchronized.

Before disabling data synchronization for a task, consider the following implications:

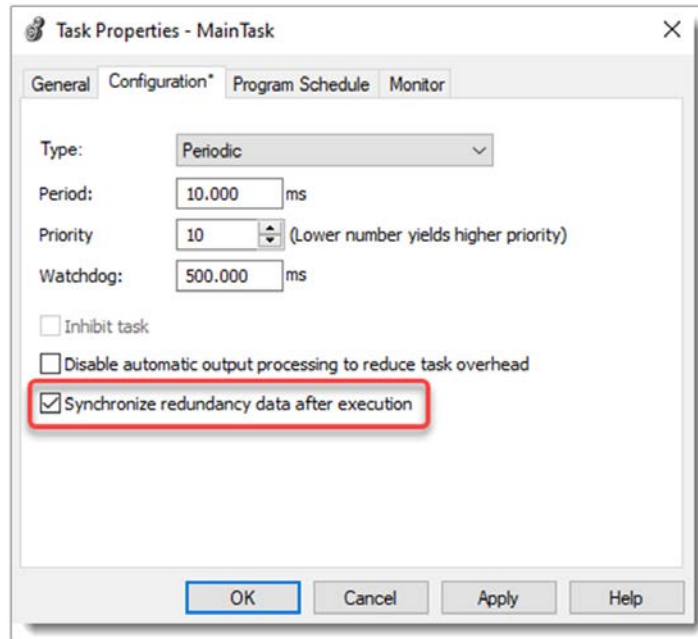
- No changes to standard tag values within the task are synchronized with the secondary controller:
 - No changes to program-scoped tags are directly synchronized.
 - Changes to controller-scoped tags are synchronized in another standard task's sync point.
- Avoid the following elements in tasks with data synchronization disabled:
 - Alarm instruction
 - Equipment phase
 - MSG instruction
 - Sequential function chart (SFC)

IMPORTANT When in a task with data synchronization disabled, an SFC requires a Reset SFC (SFR)/Pause SFC (SFP) following a switchover to function properly.

- For a consistent production of outputs, output values are not transferred to the I/O module until another task with data synchronization enabled completes its scan.
- If you choose to disable data synchronization for a task, the data synchronization setting for all programs under the task is ignored.
- If a switchover occurs during a task with data synchronization disabled, the following occurs:
 - The new primary controller begins execution of the task starting with the first program in its program list. Depending on the application, programming may be required to make data on the new primary usable. See [Program Logic to Run After a Switchover](#).
 - The task does not maintain its periodic execution rate through the switchover. When it is scheduled to run, it starts immediately and does not depend on the remaining time in its period. Going forward, the task resumes its periodic rate.
- If a task with data synchronization disabled shares data with a task that synchronizes data, special logic may be required during the first scan. For example, copying controller-scoped tag values changed by a 'sync-disabled' task to or from standard tags mapped to safety tags should not be done during the first scan.

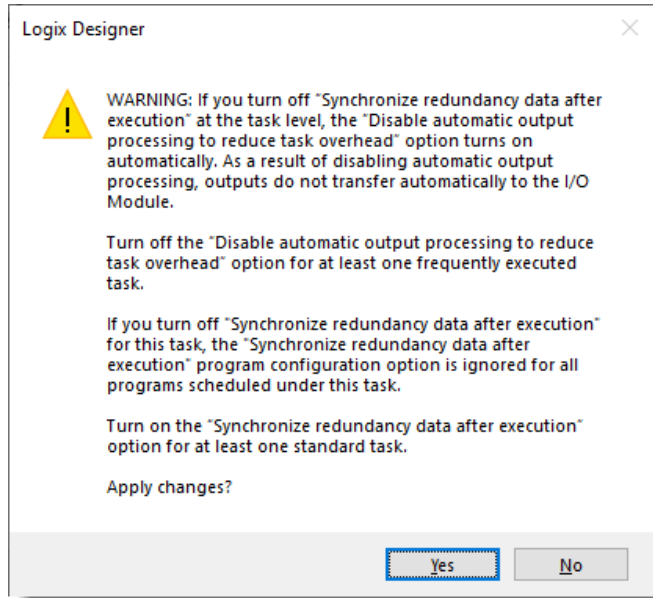
You can change the data synchronization setting for a standard task on the Configuration tab of the task properties. The setting can be modified only when offline.

Figure 17 - Data Synchronization Setting for a Task



When you disable data synchronization for a task, the following warning appears to confirm the changes.

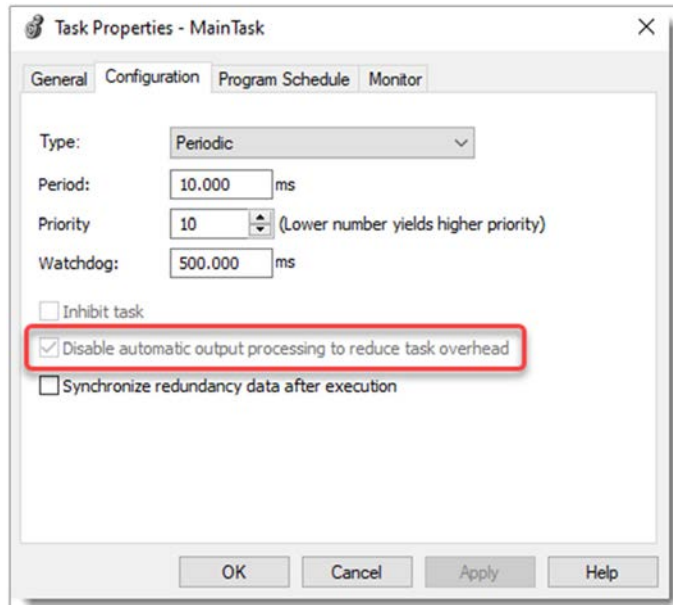
Figure 18 - Disable Task Data Synchronization Warning



When you apply the changes, the Disable automatic processing to reduce task overhead checkbox becomes enabled and the setting cannot be changed.

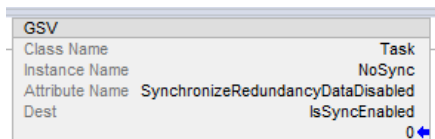
IMPORTANT The Disable Automatic Processing to Reduce Task Overhead setting must **not** be enabled for at least one frequently executed standard task.

Figure 19 - Disable Automatic Output Processing



You can monitor the data synchronization setting for a task by using the SynchronizeRedundancyDataDisabled attribute in a Get System Value (GSV) instruction.

Figure 20 - Monitor Data Synchronization Setting



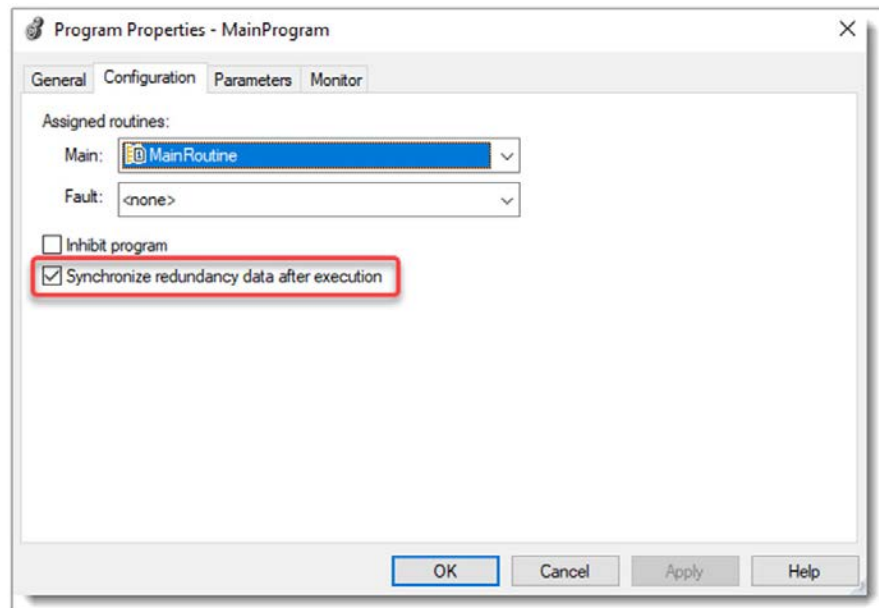
Program Settings

If you reduce the number of crossload and synchronization points, the switchover time becomes longer as more programs must be rescanned after the switchover.

Synchronization is performed at the end of the last program in the program list of the task, regardless of the Synchronize Data after Execution setting for the program.

You can change the synchronization setting for a program on the Configuration tab of the program properties.

Figure 21 - Data Synchronization Setting for a Program



Default Settings

The default setting for standard tasks and programs in a redundancy project is for a crossload to occur at the end of each task and program execution. However, for an **equipment phase**, the default setting is that the crossload does not execute at the end of the phase.

Before you change the default crossload and synchronization settings, read the sections that follow so you have a complete understanding of the implications.

Recommended Task Types

To make synchronization, crossloads, and HMI updates as fast as possible, avoid using a continuous task. Instead, the best practice is to use periodic tasks. The fewer periodic tasks, the better the performance.

IMPORTANT We recommend avoiding a continuous task for applications that are larger or have heavy communication. For more information, see [Programming Best Practices for Standard Tasks](#).

Only the single highest-priority periodic task provides bumpless output switching on switchover.

Continuous Task After Switchover

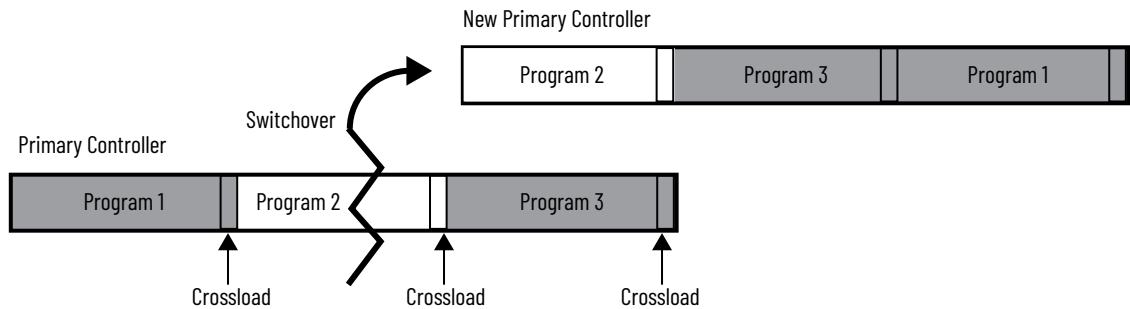
After a switchover occurs within a controller project that contains only a continuous task, the new primary controller begins executing at the last crossload and synchronization point. Depending on your crossload and synchronization setting, the program that the new primary controller begins with can be the following:

- The program that the switchover interrupted
- The program that immediately follows the last crossload and synchronization point

Continuous Task with Crossloads at Each Program End

This diagram demonstrates how programs set to crossload and synchronize at each program-end are executed after a switchover. As shown, the new primary controller begins executing at the beginning of the program that the switchover interrupted. This process is the switchover execution that happens with the default crossload and synchronization setting for a program.

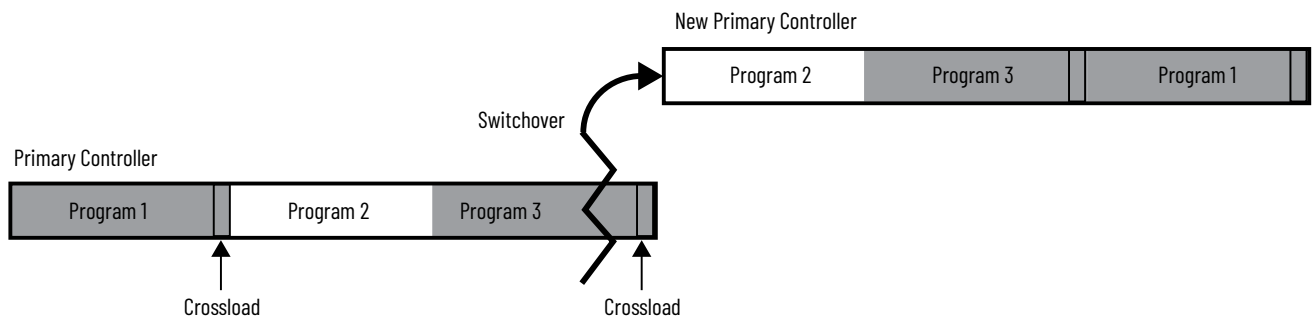
Figure 22 - Crossloads at Each Program End



Continuous Task with Various Crossloads at Program End

This diagram shows how programs set to crossload and synchronize at various intervals are executed after a switchover. In this example, the new primary controller begins executing the program that follows the last crossload and synchronization point.

Figure 23 - Various Crossloads at Program End



For information about how to change the point in a task where a crossload occurs, see [Configure Crossload and Synchronization Settings](#).

Multiple Periodic Tasks



ATTENTION: If you use multiple periodic tasks, program all crucial outputs within the highest-priority task. Failure to program outputs in the highest-priority task can result in outputs that change state if a switchover occurs.

In a project where multiple periodic tasks are used, the point where program execution begins after a switchover depends on the following:

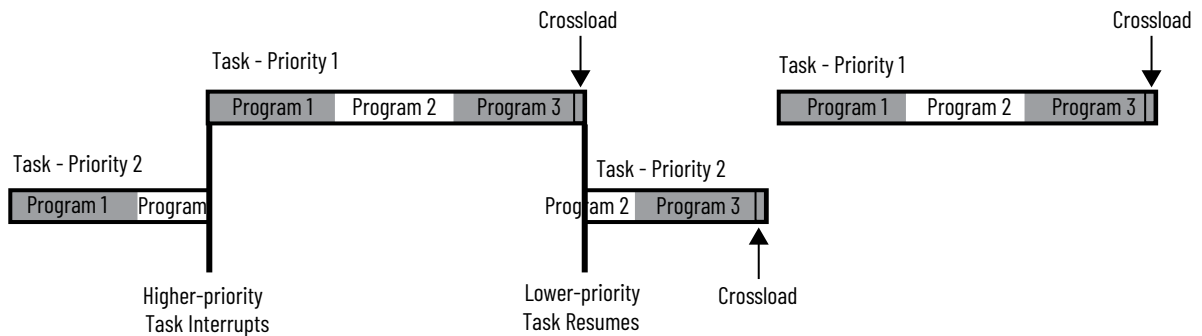
- Crossload and synchronization settings
- Task priority settings

As with the continuous task, the controller begins executing at the program that follows the last crossload and synchronization point.

A higher priority task can interrupt a lower priority task. If a switchover occurs during or just after the higher priority task executes and the lower priority task has not been completed, then the lower priority task and programs are executed from the point at which the last crossload occurred.

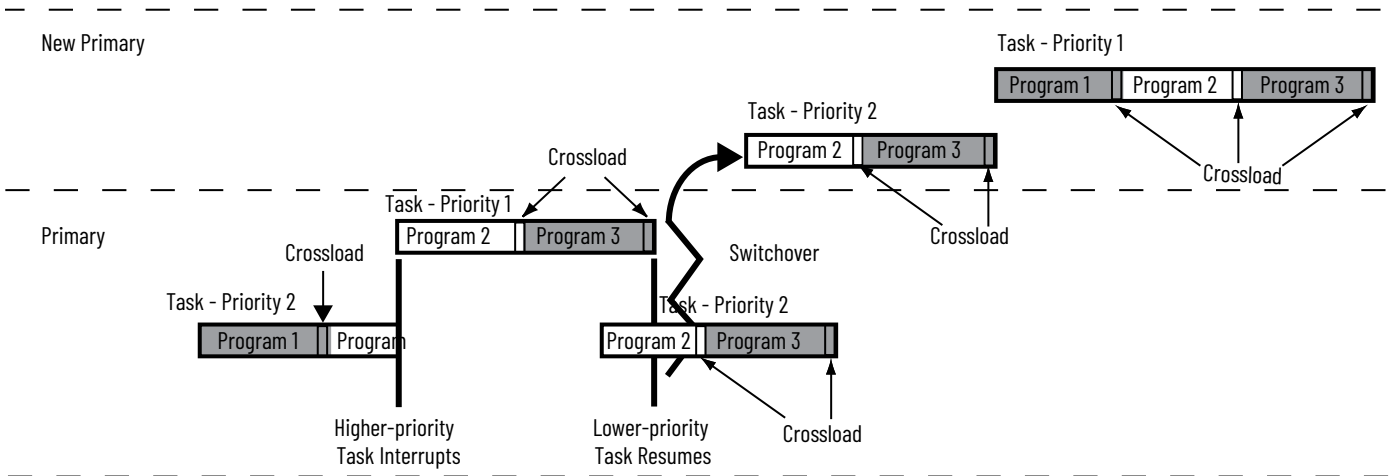
This diagram demonstrates how tasks at different priorities execute if a switchover occurs while a lower priority task is executing. The crossload and synchronization points in this example are set to occur only at the end of the last program within the tasks. The points are not set to occur at the end of each program.

Figure 24 - Normal Periodic Task Execution (No Switchover)



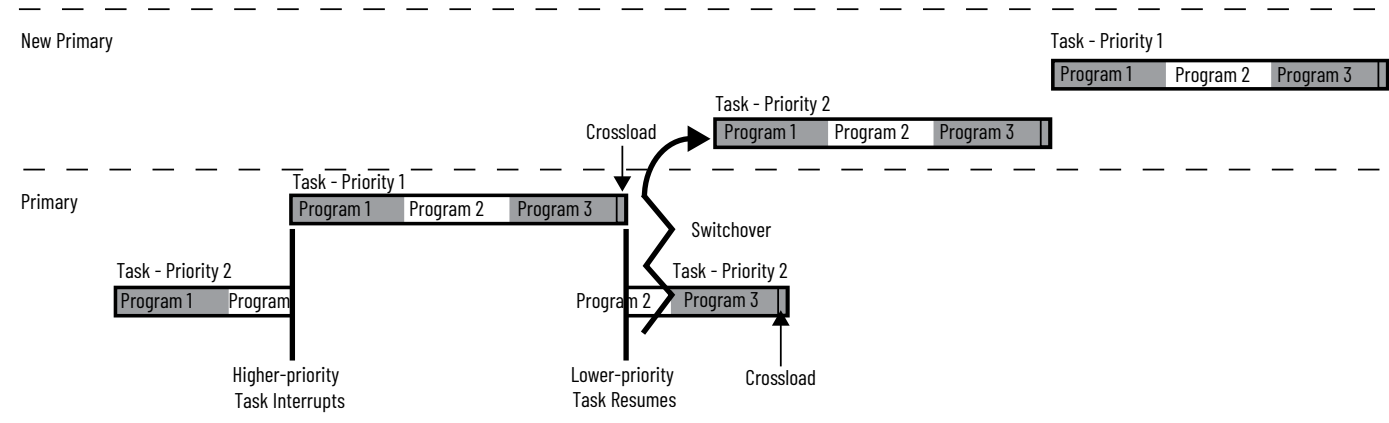
The following diagram shows a lower priority task that has not been completed and a switchover occurs. The lower priority task and programs are executed from the beginning of the program where the switchover occurred. This result is because the program uses the default configuration and crossloads and synchronization points occur at the end of each program.

Figure 25 - Configured to Crossload After Programs



The following diagram shows a lower priority task that has not been completed and a switchover occurs. The lower priority task and programs are executed from the beginning and not at the program where the switchover occurred. This result is because the crossloads and synchronization points were not configured to occur at the end of each program.

Figure 26 - Configured Not to Crossload After Programs



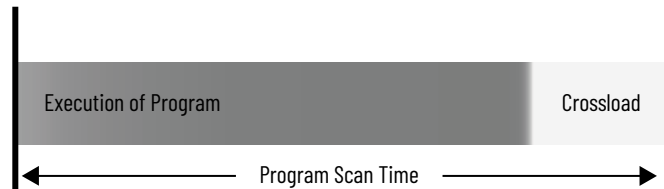
For more information about programs and tasks with controllers, see the Logix 5000 Controllers Tasks, Programs, and Routines Programming Manual, publication [1756-PM005](#).

Crossloads and Scan Time for Standard Tasks

It is important to plan for controller crossloads because the length of the crossloads affects the scan time of your program. A crossload is a transfer of data from the primary controller to the secondary controller. The crossload can occur at the end of each program or at the end of the last program in a task.

The scan time of your program or phase is a total of the program execution time and the crossload time. The following diagram demonstrates this concept.

Figure 27 - Crossload and Scan Time



The amount of time that is required for a crossload depends primarily on the amount of data that is crossloaded. During a crossload, any tag that has been written to during the program execution is crossloaded, even if the tag value has not changed.

The crossload requires time to transfer tag value changes. The crossload also requires a small amount of overhead time to communicate information about the program being executed.

Redundancy Object Attributes for Crossload Time

Before you complete calculations to estimate the crossload time, use a Get System Value (GSV) instruction to read certain attributes of the redundancy object. These attributes provide data transfer sizes that are measured in DINTs (4-byte words). You can use these sizes to estimate crossload time.

To get redundancy object attributes, the secondary chassis is not required to be in operation. If the secondary chassis is not in operation, the attribute values indicate the data sizes that would be transferred if the secondary chassis was in operation.

Table 29 - Crossload Data Size Attributes

Attribute	Description
LastDataTransferSize	Obtains the transfer size of the previous crossload and synchronization point that occurred before the program that contains the GSV instruction.
MaxDataTransferSize	Obtains the maximum data size that is transferred from the program that the GSV executes within. This data includes program-scoped data and controller-scoped data that was changed after the previous synchronization point.

To measure the crossloaded data from the last program in the program list of the task, add a program at the end of the task that acquires the LastDataTransferSize value from the program that was formerly at the end of the task.

Estimate Crossload Time per Sync Point

A sync point is a mechanism that the primary controller uses to keep the secondary controller in sync. By default, at the end of each program scan in a standard task, the primary controller sends the secondary controller the sync point and the secondary controller responds by moving its execution pointer to match the primary controller. The default for phases is not to send a sync point.

Before you estimate the crossload time of your controllers for each program in a standard task, obtain the following:

- The size of the last data transfer
- The maximum size of data that is transferred

Crossload time equations are derived from tests that are performed on the latest supported firmware revisions.

The following equations apply when a ControlLogix 5580 controller or Logix SIS safety controller is paired with a redundancy module in both chassis of a redundant chassis pair.

Table 30 - Crossload Times for ControlLogix 5580 or Logix SIS Controllers

Controller Firmware Revision	Redundancy Module	Crossload Time per Sync Point (ms)
33	1756-RM2	$(DINTs * 0.000360) + 0.44$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000397) + 0.32$ ms With fiber security disabled: $(DINTs * 0.000366) + 0.23$ ms
34	1756-RM2	$(DINTs * 0.000338) + 0.51$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000395) + 0.37$ ms With fiber security disabled: $(DINTs * 0.000339) + 0.27$ ms
35	1756-RM2	$(DINTs * 0.000339) + 0.52$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000394) + 0.37$ ms With fiber security disabled: $(DINTs * 0.000339) + 0.26$ ms
36	1756-RM2	$(DINTs * 0.000357) + 0.53$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000396) + 0.39$ ms With fiber security disabled: $(DINTs * 0.000356) + 0.27$ ms
37	1756-RM2	$(DINTs * 0.000352) + 0.45$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000400) + 0.33$ ms With fiber security disabled: $(DINTs * 0.000352) + 0.24$ ms
38	1756-RM2	$(DINTs * 0.000327) + 0.45$ ms
	1756-RM3	With fiber security enabled: $(DINTs * 0.000413) + 0.33$ ms With fiber security disabled: $(DINTs * 0.000335) + 0.24$ ms

The following equations apply when a ControlLogix 5570 controller is paired with a redundancy module in both chassis of a redundant chassis pair.

Table 31 - Crossload Times for ControlLogix 5570 Controllers

Redundancy Module	Crossload Time per Sync Point (ms)
1756-RM3	With fiber security enabled: $(DINTs * 0.000652) + 0.30$ ms With fiber security disabled: $(DINTs * 0.000584) + 0.26$ ms
1756-RM2	$(DINTs * 0.000550) + 0.39$ ms
1756-RM/B	$(DINTs * 0.00043) + 0.3$ ms
1756-RM/A	$(DINTs * 0.00091) + 0.6$ ms Where DINTs is the size of the data transferred measured in 4-byte words.

Watchdog Time for the Safety Task

Logix SIS safety controllers have a safety task watchdog parameter that impacts the controller reaction time and execution of the safety task during loss of redundancy. For an explanation of the safety task watchdog and configuration guidelines, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

Watchdog Time for Standard Tasks

Watchdog time for standard tasks in redundancy applications must be longer than tasks in nonredundancy applications because more time is required to conduct crossloads and synchronization.

IMPORTANT To help prevent issues with online edits or locked switchovers during an online firmware update, do not set a watchdog time longer than 10 seconds for a continuous task.

The way programs execute in the event of a switchover is another reason for a longer watchdog time. A program can execute a second time after a switchover. This action depends on when the switchover occurs in the task or program and in the task crossload and synchronization.

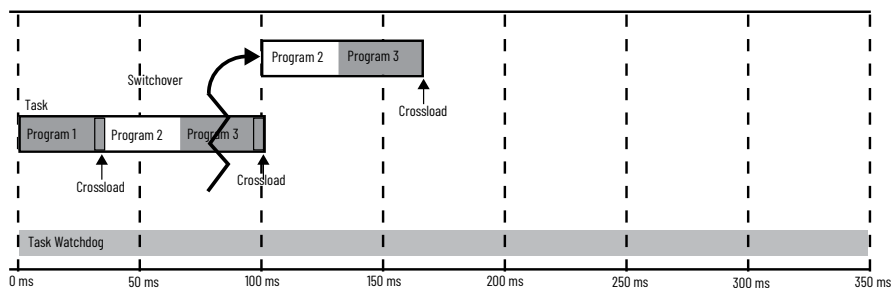
If a program executes a second time, the length of time that is required for the program scan is increased. However, the watchdog timer is not reset and continues to countdown from the beginning of the task that the old primary controller started. Therefore, the watchdog timer must be configured to account for the potential of additional program scans.

For ControlLogix 5570 redundancy, we recommend that you reevaluate the watchdog times in your application in these scenarios:

- You add a second controller to a redundant chassis.
- You modify an application in a second controller that is already in a redundant chassis.

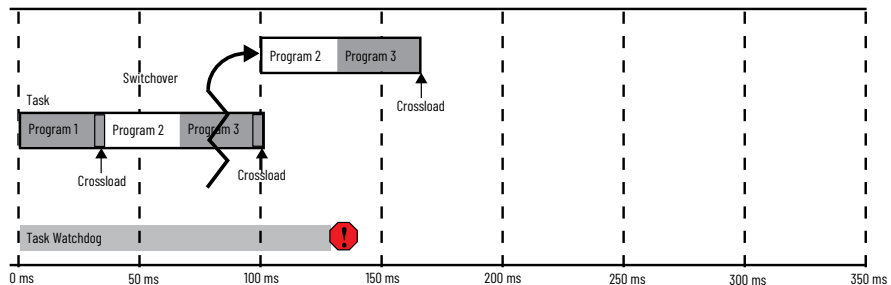
If there is a watchdog timeout, a major fault (type 6, code 1) results. If this fault occurs after a switchover, the control system fails-to-safe or to the configured hold state.

Figure 28 - Configured for Redundancy Switchover



If there is a watchdog timeout, a major fault (type 6, code 1) results. If this fault occurs after a switchover, the control system fails-to-safe or to the configured hold state.

Figure 29 - Not Configured for Redundancy Switchover



Set Minimum Values for Standard Task Watchdog Time

To set the initial task tuning of the controller, follow these steps.

IMPORTANT This process works only when there is no Continuous task that is configured in the Logix application.
While performing these tests, the HMI and any other external systems must be connected to the Logix controller and actively executing communications.

1. Monitor the Max Scan Time for each task while the redundant chassis pair is synchronized.
2. Set the watchdog times for each task to three times the max scan time or 50 ms, whichever is greater.
3. For Logix SIS and ControlLogix 5580 redundancy, configure each task period by using the L_CPU Add-On Instruction. For more information, see the Knowledgebase Technote [L_CPU AOI Download](#).

or

For ControlLogix 5570 redundancy, configure each task period by using the Logix 5000[®] Task Monitor Tool. For more information, see the PlantPAx Distributed Control System Configuration and Implementation User Manual, publication [PROCES-UM100](#).

- a. Adjust the task periods of each so that the maximum scan time is less than 80% of the task period rate.
- b. Adjust the task periods so that the Logix CPU% utilization is never above 80%.

IMPORTANT Verify that there are no task overlaps.

Programming Best Practices for Standard Tasks

Apply these best practices to standard tasks in redundancy systems. For best practices that apply to the safety task in Logix SIS, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

Program to Minimize Scan Times

There are several aspects of your program that must be as efficient as possible to facilitate the fastest possible switchover. Total program scan time impacts system switchover time.

These methods make your program more efficient and minimize program scan times:

- Minimize the number of programs
- Manage tags for efficient crossloads
- Use concise programming
- Use multiple controllers in ControlLogix® 5570 redundancy systems

Minimize the Number of Programs

When programming a redundant controller, use the fewest programs possible, especially if you plan to crossload data and synchronize the controllers after the execution of each program.

If you must crossload data at the end of each program, follow these programming best practices to minimize the crossload impact on the program scan time:

- Use only one or a few programs.
- Divide each program into routines. A routine does not cause a crossload or increase the scan time.
- Use the main routine of each program to call the other routines of the program.
- If you use multiple tasks for different scan periods, use only one program in each task.

Figure 30 - Multiple Routines (Preferred)

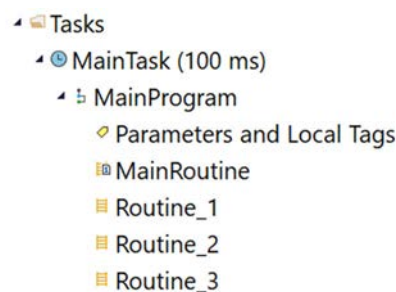
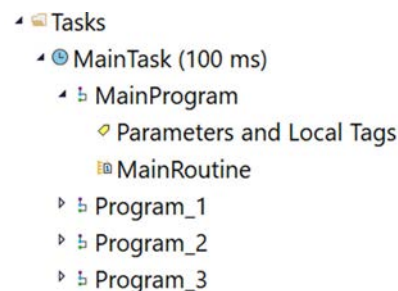


Figure 31 - Multiple Programs (Not Preferred)



Manage Tags for Efficient Crossloads

Use the following guidelines to manage your data tags for more efficient crossloads and reduce the amount of time for crossloads to execute.

Delete Unused Tags

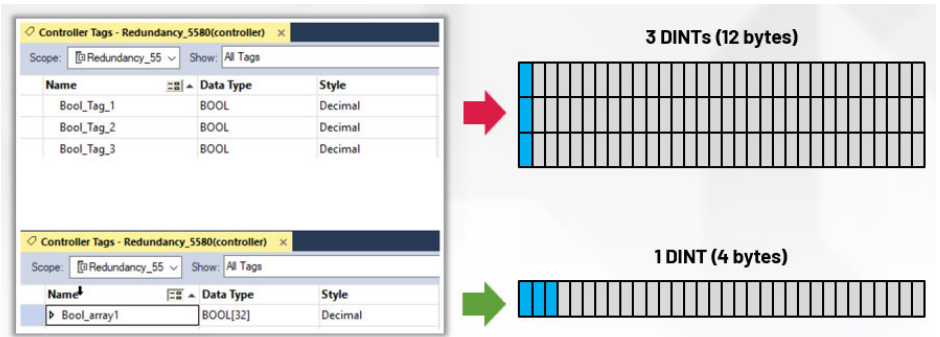
To reduce the size of the tag database, delete unused tags. A smaller database takes less time to crossload.

Use Arrays and User-defined Data Types

If you use arrays and user-defined data types, the tags use smaller 4-byte (32-bit) words for all data in the type or array. If you create an individual tag, the controller reserves 4 bytes (32 bits) of memory even if the tag uses only 1 bit.

Arrays and user-defined data types help conserve the most memory with BOOL tags. However, we also recommend that you use them for your SINT, INT, DINT, REAL, COUNTER, and TIMER tags.

Figure 32 - Example Savings with the Use of an Array



If you have already created individual tags and programming that uses those tags, consider changing the individual tags to alias tags that reference the elements in an array.

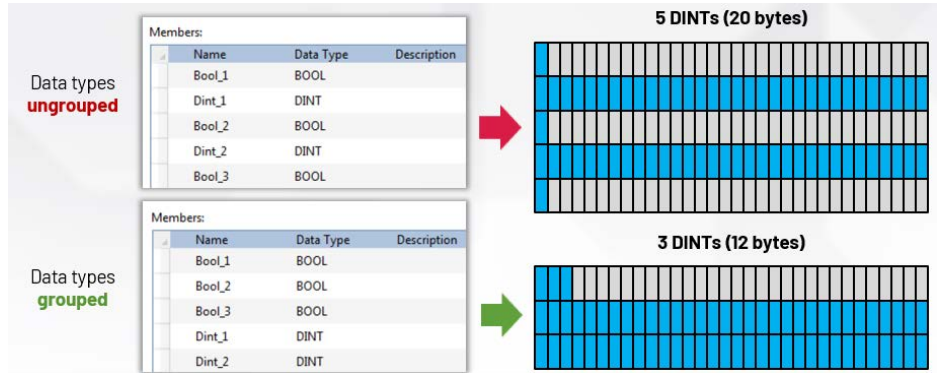
If you choose this method, your programming can still reference the individual tag names, but the crossload transfers the base array.

For more information about how to work with arrays, user-defined data types, and alias tags, see the Logix 5000 Controllers I/O and Tag Data Programming Manual, publication [1756-PM004](#).

Group Data Types Together in User-defined Data Types

When you create a user-defined data type in your redundancy program, group like data types together. Groups of like data types compresses the data size and helps reduce the amount of data that is transferred during a crossload. Group data into types that equal 32 bits as much as possible. For example, 32 BOOLs equals 32 bits.

Figure 33 - Example of Bytes Saved by Grouping Like Data



Group Data into Arrays of User-defined Data Types by Frequency of Update

To minimize crossload time, group your data by how frequently it is written to. Even if the data value does not change, if the tag is actively written to by a MOV/MOVE, OTE, or data table write, for example, it counts as a data change.

For example, if your application uses DINTs that you use only as constants to initialize your logic, BOOLs that you update every scan, and REALs that you update every second, you can create a separate user-defined data type for each type of tag that is used at different points in the application. Using separate user-defined data types for each group, rather than grouping all tags together in one user-defined data type, helps to minimize the amount of data that is transferred during the crossload.

Figure 34 - Data Types by Frequency of Use

Name	Data Type
-My_Bools	My_Bools_UDT
-My_Bools.Bool_1	BOOL
-My_Bools.Bool_2	BOOL
-My_Bools.Bool_3	BOOL
-My_Constants	My_Constants_UDT
+My_Constants.Constant_1	DINT
+My_Constants.Constant_2	DINT
+My_Constants.Constant_3	DINT
-My_Reals	My_Reals_UDT
-My_Reals.Real_1	REAL
-My_Reals.Real_2	REAL
-My_Reals.Real_3	REAL

Figure 35 - One Data Type

Name	Data Type
-My_Data	My_Data_UDT
+My_Data.Constant_1	DINT
+My_Data.Constant_2	DINT
+My_Data.Constant_3	DINT
-My_Data.Bool_1	BOOL
-My_Data.Bool_2	BOOL
-My_Data.Bool_3	BOOL
-My_Data.Real_1	REAL
-My_Data.Real_2	REAL
-My_Data.Real_3	REAL

Use DINT Tags Instead of SINT or INT Tags when Possible

We recommend that you use the DINT data type instead of the SINT or INT data types because the controller usually works with 32-bit values (DINTs or REALs). When processing, the controller converts SINT or INT tag values to DINT or REAL values. When processing is complete, the controller converts the value back to a SINT or INT value.

The controller automatically converts these data types while executing and processing a program. No additional programming is required. However, while this conversion process is transparent to you, it requires additional processing time that impacts your program scan time and your switchover time.

Use Concise Programming

Use these recommendations to create concise programming. Concise programming makes your program execute faster and reduces your program scan time.

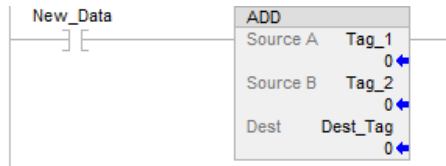
Execute an Instruction Only When Needed

Because many instructions write tag values whenever executed, strategic and economical use of instructions is needed. Strategic programming techniques include the following:

- Use preconditions to limit the execution of instructions.
- Combine preconditions when possible.
- Divide programming into subroutines that are called only when required.
- Run noncritical code every two or three scans instead of during every scan.

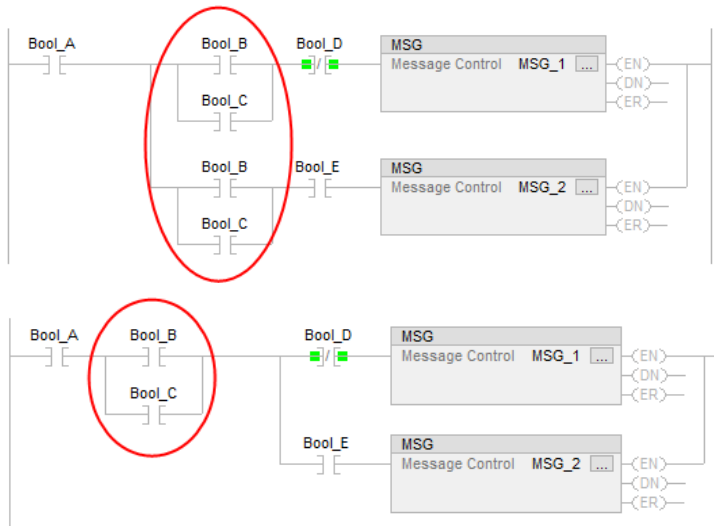
For example, precondition an ADD instruction to run only when the controller gets new data. As a result, the Dest_Tag is crossloaded only when the ADD instruction produces a new value.

Figure 36 - Precondition Used with ADD Instruction



Along with preconditions, try to group instructions together that use the same precondition. In this example, the four preconditions in the two branches can be combined to precede the two branches. Doing so reduces the number of precondition instructions from four to two.

Figure 37 - Efficient Precondition Use



(ControlLogix 5570 Only) Use Multiple Controllers

For non-PlantPAx systems that use ControlLogix 5570 redundancy, consider using two controllers per redundant chassis. If you use multiple controllers, you can strategically program between the controllers so the program execution and scan times are faster.

Program to Maintain Data Integrity

Some instructions and techniques can cause data loss or corruption. Avoid these instructions and techniques when programming a redundant controller:

- Timer instructions
- Array (File)/Shift instructions
- Scan-dependent logic
- (ControlLogix 5570 only). Align LINT members on 8-byte boundaries

Timer Instructions

After a switchover, timer-based instructions, such as TON, TOF, and RTO, continue to time with the same time base as before the switchover.

Array (File)/Shift Instructions

This section only applies when the instructions are modifying controller-scoped data. When there are interruptions to Array (File)/Shift instructions by a task with the same or higher priority and then a switchover event occurs, it could result in an incomplete data shift and corrupted data.

These Array (File)/Shift instructions can result in corrupt data if there is a switchover:

- Bit Shift Left (BSL)
- Bit Shift Right (BSR)
- FIFO Unload (FFU)
- File Arithmetic and Logic (FAL)
- File Bit Comparison (FBC)
- Diagnostic Detect (DDT)
- File Sort (SRT)

If Array (File)/Shift Instructions are used, these system behaviors can occur:

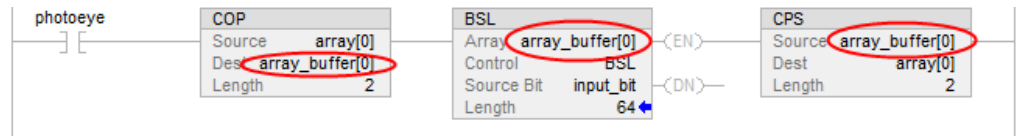
- If a higher priority task interrupts an Array (File)/Shift instruction, the partially shifted array values are crossloaded to the secondary controller.
- If a switchover occurs before the instruction completes its execution, data remains only partially shifted.
- After a switchover, the secondary controller starts executing at the beginning of the program. When it reaches the partially executed instruction, it shifts the data again.

Buffering Critical Data

If you cannot place Array (File)/Shift instructions that modify controller-scoped data in the highest-priority task, consider using a buffer with Copy File (COP) and Synchronous Copy File (CPS) instructions to maintain the integrity of the array of data.

The programming example that is shown here shows the use of a COP instruction to move data into a buffer array. The BSL instruction uses the data in that buffer array. The CPS instruction updates the array tag and maintains data integrity because a higher priority task cannot interrupt it. If a switchover occurs, the source data (array tag) remains unaffected.

Figure 38 - Buffer to Maintain Data During Shift



For more information about BSL, BSR, COP, CPS, DDT, FAL, FBC, FFU, and SRT instructions, see the Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

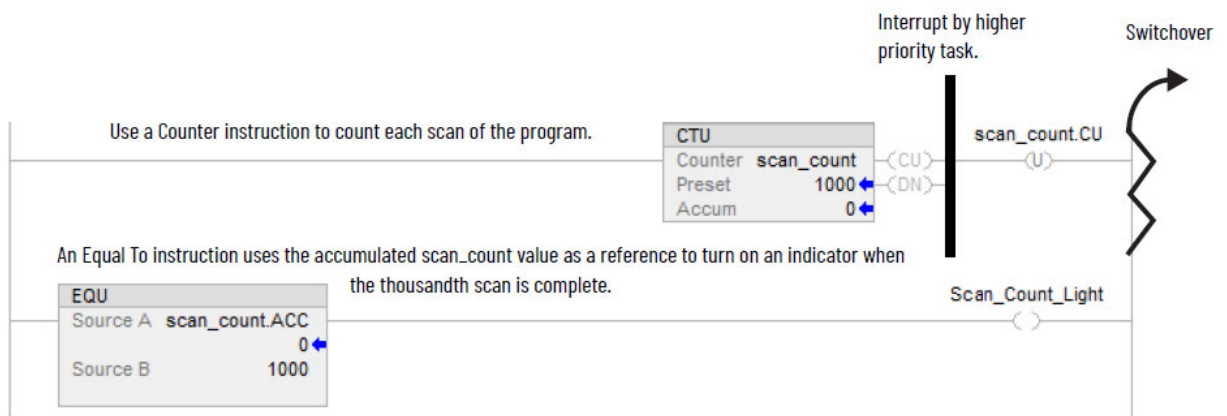
Scan-dependent Logic

If you use controller-scoped tags and program a lower priority task so that one instruction is dependent on another instruction that occurs elsewhere in your program, a task interrupt and switchover can disrupt your programming. The disruption can occur because the higher priority task can interrupt the lower priority task and then a switchover can occur before the lower priority task is completed.

When the lower priority task is executed from the beginning by the new primary controller after the switchover, the dependent instruction can fail to execute at the most recent value or state.

For example, if a higher priority task interrupts the logic that is shown in this example, the value of scan_count.ACC is sent to the secondary controller at the end of the program in the higher priority task. If a switchover occurs before the primary controller completes the EQU/EQ instruction, the new primary controller starts its execution at the beginning of the program and the EQU/EQ instruction misses the last value of scan_count.ACC. As a result, any programming that uses the Scan_Count_Light tag can also execute by using incorrect data.

Figure 39 - Scan-dependent Logic

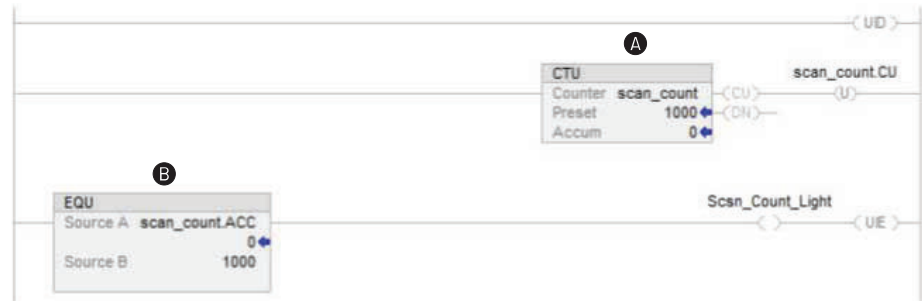


Bind Dependent Instructions with UID and UIE Instructions

If you cannot place scan-dependent instructions in the highest priority task, consider using the User Interrupt Disable (UID) and User Interrupt Enable (UIE) to help prevent a higher priority task from interrupting the scan-dependent logic.

For example, if you bind the scan-dependent logic that is previously shown, a higher priority task would not interrupt the dependent instructions and a switchover would not result in inconsistent data.

Figure 40 - Scan-dependent Instructions Bound with UID and UIE Instructions



Item	Description
A	Use a Counter instruction to count each scan of the program.
B	An Equal To instruction uses the accumulated scan_count value as a reference to turn on an indicator when the thousandth scan is complete.

For more information about UID and UIE instructions, see the Logix 5000 Controllers General Instructions Reference Manual, publication [1756-RM003](#).

(ControlLogix 5570 Only) Align LINT Members on 8-byte Boundaries

The Logix Designer application has requirements for data type use based on the version.

Logix Designer Application Version	Requirement
Version 26 or earlier	Logix 5000 [®] controllers require all data types to be placed on 4-byte address boundaries in RAM.
Version 27 or later	Logix 5000 controllers require 8-byte (64-bit) data types (LINTs) to be placed on 8-byte address boundaries in RAM.

The Logix Designer application manages the requirement automatically, and the change has no effect on individual LINT tags, regardless of application version.

LINTs inside a UDT can be misaligned in these situations:

- You migrate a standard Logix Designer project, version 26 or earlier, to a redundancy project that is version 30.051 or later, and you have LINT tags inside a UDT.
- You migrate a redundancy project, version 24.053 or earlier, to a project that is version 30.051 or later, and you have LINT tags inside a UDT.

Additional pad bytes are added to the data structure to account for the misalignment. The pad bytes can cause an increase in the size of the UDT.

The possible effects of data structure changes, and subsequent actions that you can take as a result, are described in the rest of this section.

IMPORTANT You must also act when your application includes Logix 5000 controllers, version 26 or earlier, that communicate with Logix 5000 controllers, version 30.051 or later.

Possible Impact of Requirement Change

You can adapt your project to accommodate larger structure sizes. You can see the following effects due to the larger size:

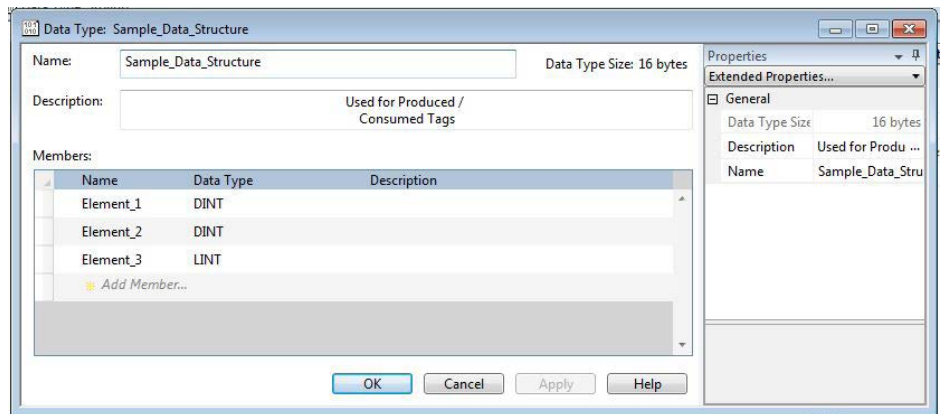
- Message instruction data lengths can require changes to complete successfully.
- Copy lengths of data structures can change.
- Produce/consume connections to other Logix controller types can have data type mismatches and require changes to complete successfully.

To correct produce/consume errors that are caused by UDT alignment changes, modify the tag structures in both projects so that they match:

- Produce/consume with status requires an exact match of the UDT definition including the name of the UDT definition.
- Produce/consume without status requires the Size of the UDT to match.

We recommend that you copy and paste the UDT definition from one project to the other to cover both of these cases. Use the Data Type editor to check the data type size in both projects.

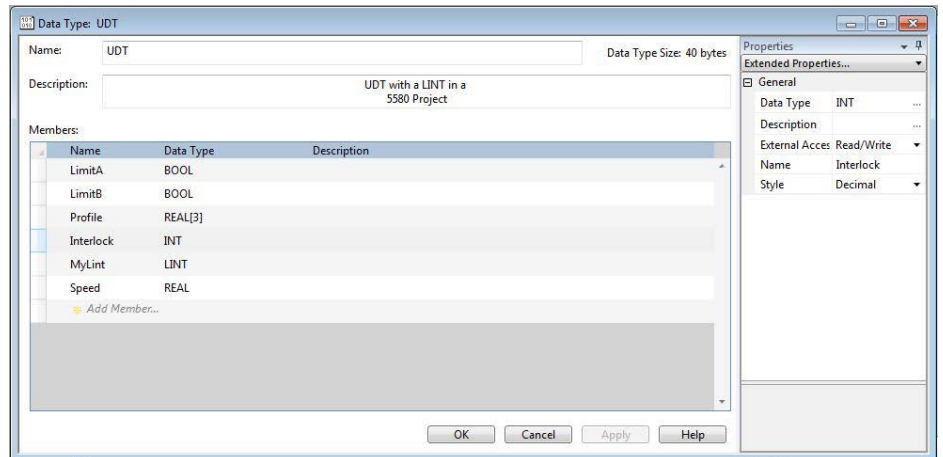
Figure 41 - Data Type Editor



If the data type size is different between the two projects, modify the UDT to produce the same internal data structure.

The following sample UDT illustrates how the 8-byte allocation rule and the 8-byte alignment rule cause a UDT to have another size.

Figure 42 - UDT Sample - Needs Additional Memory Allocation and Alignment



The following table shows how this data structure maps in the Logix Designer application, version 24.053 or earlier. MyLint is split across two 64-bit words, and the total size is 32 bytes.

Table 32 - Data Structure for Logix Designer Projects, Version 26 or Earlier

Word	Elements	Byte Mapping Table				64 Bit Boundaries
0	LimitA and LimitB	Pad	Pad	Pad	Hidden SINT	0
1	Profile (Real [3])	Map	Map	Map	Map	
2		Map	Map	Map	Map	1
3		Map	Map	Map	Map	
4	Interlock (Int)	Pad	Pad	Map	Map	2
5	MyLint (LINT)	Map	Map	Map	Map	
6		Map	Map	Map	Map	3
7	Speed (REAL)	Map	Map	Map	Map	

The next table shows the hidden padding bytes that the Logix Designer application, version 30.051 or later, adds to achieve the 8-byte alignment and allocation rules:

- Padding is added in Word 5 so that MyLint starts at an 8-byte boundary.
- Padding is added in Word 9 so that the entire structure is a multiple of 8 bytes.

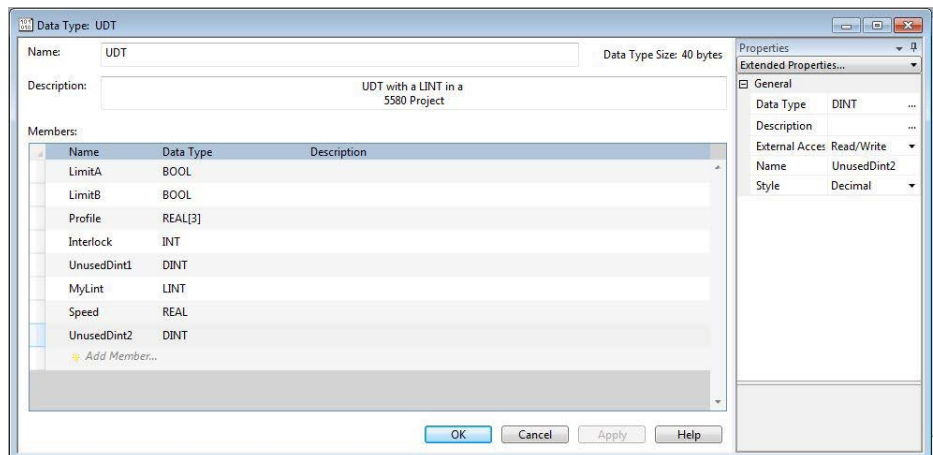
Table 33 - Hidden Padding Added for Logix Designer Projects, Version 27 or Later

Word	Elements	Byte Mapping Table				64 Bit Boundaries
0	LimitA and LimitB	Pad	Pad	Pad	Hidden SINT	0
1	Profile (Real [3])	Map	Map	Map	Map	
2		Map	Map	Map	Map	1
3		Map	Map	Map	Map	
4	Interlock (Int)	Pad	Pad	Map	Map	2
5	Padding for 8-byte alignment	Pad	Pad	Pad	Pad	
6	MyLint (LINT)	Map	Map	Map	Map	3
7		Map	Map	Map	Map	
8	Speed (REAL)	Map	Map	Map	Map	4
9	Padding for 8-byte allocation	Pad	Pad	Pad	Pad	

To create a UDT that is the same size in all types of projects, insert additional data elements so that hidden padding bytes are not necessary.

The following sample UDT illustrates how UnusedDint1 and UnusedDint2 create a UDT with the same size in the Logix Designer application, version 24.053 or earlier, compared to version 30.051 or later.

Figure 43 - UDT Sample - Memory Allocation and Alignment OK



This table shows how this data structure maps in all types of Logix 5000 controller projects.

Table 34 - Memory Map in All Project Types

Word	Elements	Byte Mapping Table				64-Bit Boundaries
0	Bools and 2	Pad	Pad	Pad	Hidden SINT	0
1	Profile (Real [3])	Map	Map	Map	Map	1
2		Map	Map	Map	Map	
3		Map	Map	Map	Map	
4	Interlock (INT)	Pad	Pad	Map	Map	2
5	UnusedDint1	Map	Map	Map	Map	
6	MyLint (LINT)	Map	Map	Map	Map	3
7		Map	Map	Map	Map	
8	Speed (REAL)	Map	Map	Map	Map	4
9	UnusedDint2	Map	Map	Map	Map	

The concept is the same for nested UDTs. If the lower-level UDT is an 8-byte type, which contains at least one 8-byte data element, you must align it to start at an 8-byte boundary.

To correct any mismatched UDTs, complete the following tasks in either project:

1. Start at the deepest nesting level of any multi-level UDT.
2. Work from the beginning of each structure and look for LINT data types.
3. For each LINT data type or 8-byte UDT encountered, map the sizes of the prior UDT elements to determine the byte offset at the start of the element.
If the byte offset for the first 8-byte element is not divisible by 8 bytes (64 bits), insert a DINT tag element just above the 8-byte element. You can use any name. Instructions do not need to reference this element.
4. Repeat the process until all 8-byte elements are aligned on 8-byte (64-bit) boundaries.
5. If needed, add a DINT at the end of the UDT to satisfy the 8-byte allocation rule.
6. Continue up through nested UDTs until the top level is correct.

When the tasks are completed, the UDTs are the same size in the Logix Designer application, version 24.053 or earlier, and in the Logix Designer application, version 30.051 or later.

A useful technique when creating UDTs is to start with the largest data types first, and work down through 8-byte, 4-byte, 2-byte, 1-byte, and finally single-bit data types. The resultant mapping is 64-bit-aligned in all controller types, so no manual padding is required.

Produce/consume with status requires an adjustment to this technique. For these cases, the UDT must start with a 4-byte 'COMMAND_STATUS' element; therefore, one more 4-byte element (DINT or REAL) must be added before placing any 8-byte elements.

Optimize Tasks

To make synchronization, crossloads, and HMI updates as fast as possible, avoid using a continuous task. Instead, the best practice is to use periodic tasks. The fewer the number of periodic tasks used, the better the performance.

IMPORTANT

While a continuous task is fully supported, you can manage performance easier without a continuous task. With a continuous task, the performance of some types of communication can be negatively impacted under certain conditions, such as heavy messaging or HMI data table writes of tags to the controller. For more information about data table writes, see [Communication Performance](#).

If you use multiple periodic tasks, verify the following:

- There are no task overlaps during synchronized steady state. The execution time of each task is smaller than its period.
- The total execution time of all your tasks is less than the period of the task with the largest period.
- The lower priority tasks have longer periods than higher priority tasks to allow time for task interruption by the higher priority tasks.

In the following example, the execution time of the highest priority task (Task 1) is smaller than its period. The total execution time of all tasks is less than the specified period of the lowest priority task.

Table 35 - Example of Periodic Task Configurations

Task	Priority	Execution Time	Period Specified
1	Higher	20 ms	80 ms
2	Lower	30 ms	100 ms
Total execution time: 50 ms			

To tune the period you specify for periodic tasks, do the following:

- To check for overlaps, go online with the controller and access the Task Properties dialog box. On the Monitor tab, note the maximum scan time. Verify that the maximum scan time is smaller than the period for the periodic task.
- To determine how many task overlaps occurred since the last reset, check the Task Overlap Count parameter. Because task overlaps are expected during qualification, check the number of task overlaps while the controller is in a synchronized steady state.

ControlLogix 5570 Considerations

The following table lists some of the different communication types that take place during task execution and service communication periods in ControlLogix 5570 controllers.

Table 36 - Communication Types During Scheduled and Unscheduled Periods

Period	Communication Type
Task execution	Update I/O data (not including block transfers)
	Produced/consumed tags
Service communication	Communication with programming software, such as the Logix Designer application
	Communication with HMI devices
	Execution of MSG instructions, including block transfers
	Responses to messages from other controllers
	Synchronization of the redundancy system
	Reestablishment and monitoring of I/O connections, such as Removal and Insertion Under Power conditions. This process excludes normal I/O updates that occur during the execution of logic.
	Bridging of communication from the serial port of the controller to other ControlLogix devices via the ControlLogix backplane

To make synchronization, crossloads, and HMI updates as fast as possible, you can optimize the configuration of each task. The methods used to increase the time dedicated to servicing communications depends on the type of tasks that are used in a ControlLogix 5570 program.

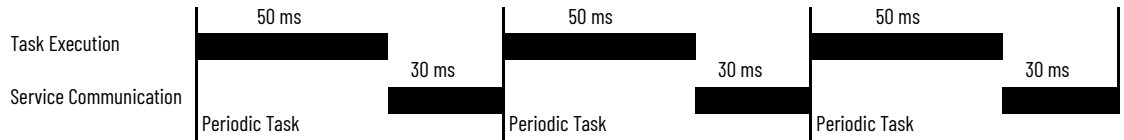
Task Type	See
One or more periodic tasks with no continuous task (recommended)	Periodic Task Configuration Optimization
A continuous task with no other tasks	Continuous Task Configuration Optimization
A continuous task with one or more periodic tasks (not recommended)	See Knowledgebase Technote The System Overhead Time Slice Explained

Periodic Task Configuration Optimization

If you have one or more periodic tasks with no continuous task, you can increase the time that is dedicated to service communication by adjusting the priority and period of each periodic task. If you do not have a continuous task in your project, changing the System Overhead Time Slice has no effect.

If you use periodic tasks, communication is serviced any time that a task is not running. For example, if you configure your task period at 80 ms and the task executes in 50 ms, the controller has 30 ms out of every 80 ms to service communication.

Figure 44 - Periodic Task Execution and Service Communication



Continuous Task Configuration Optimization

If your project contains a continuous task, you can adjust the System Overhead Time Slice setting to change the percentage of time the controller devotes to servicing communication versus executing the continuous task.

IMPORTANT If there is no continuous task, adjusting the System Overhead Time Slice setting has no effect. When there is no continuous task, all controller time that is not used for other tasks is used for servicing communications.

[Table 37](#) shows the ratio between executing the continuous task and servicing communication at various system overhead time slices:

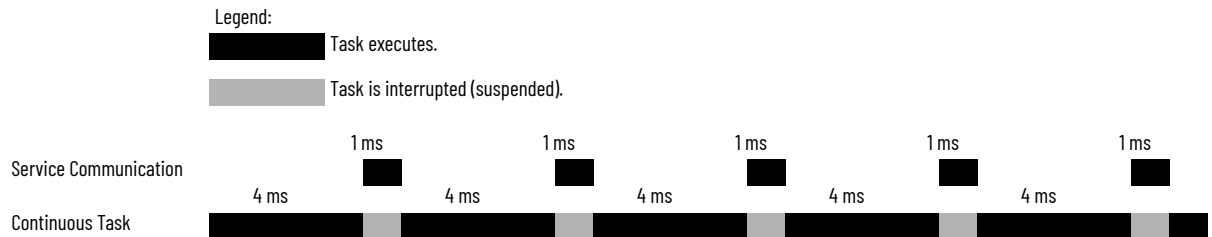
- When the system overhead time slice setting is between 10% and 50%, the time that is allocated for servicing communication is fixed at 1 ms. The continuous task time slice changes to produce the desired ratio.
- When the system overhead time slice is greater than 50...90%, the time that is allocated to the continuous task is fixed at 1 ms. The time that is allocated to servicing communication changes to produce the desired ratio.

Table 37 - System Overhead Time Slice

Time Slice	Continuous Task Run Time	Service Communication Time
10%	9 ms	1 ms
20%	4 ms	1 ms
25%	3 ms	1 ms
33%	2 ms	1 ms
50%	1 ms	1 ms
66%	1 ms	2 ms
75%	1 ms	3 ms
80%	1 ms	4 ms
90%	1 ms	9 ms

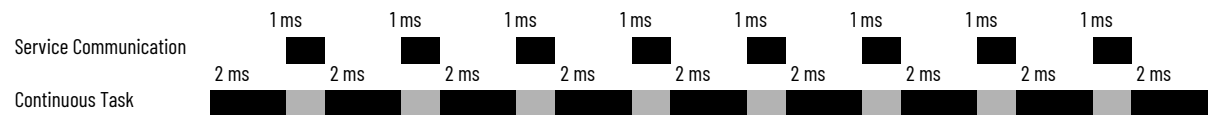
In [Figure 45](#), the system overhead time slice is set to 20% (default). With this percentage, communication is serviced after every 4 ms of continuous task execution. Communication is serviced for up to 1 ms before the continuous task is restarted.

Figure 45 - System Overhead Time Slice Set to 20%

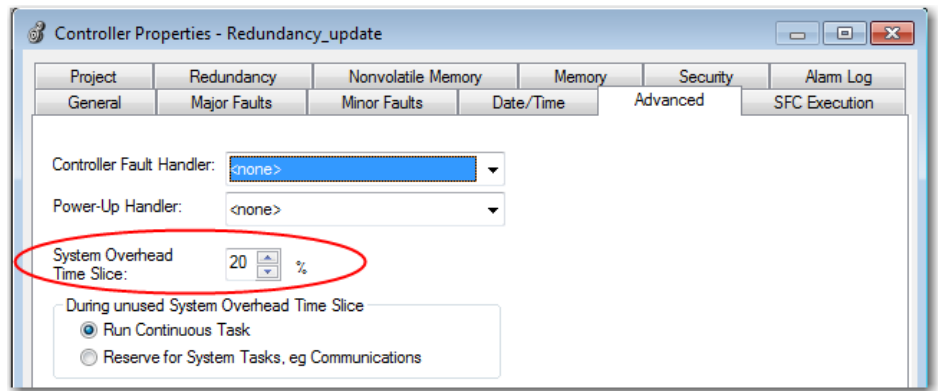


In [Figure 46](#), the system overhead time slice is set to 33%. With this percentage, communication is serviced after every 2 ms of continuous task execution. Communication is serviced for up to 1 ms before the continuous task is restarted.

Figure 46 - System Overhead Time Slice Set to 33%



You can change the System Overhead Time Slice value on the Advanced tab of the controller properties.



In the During Unused System Overhead Time Slice area, select one of these options:

- If you want the controller to revert to running the continuous task as soon as the communication servicing task has no pending activity, select the Run Continuous Task option (default setting).

This option results in using only the allocated communication servicing time if there is a need for it.

IMPORTANT

We do not recommend that you use the Reserve for System Task option for production. The option was developed to simulate systems with high communication requirements.

- To allocate the entire 1 ms of the system overhead time slice to service communication, even if no service communication or background tasks must be executed, select the Reserve for System Task option.

You can choose this option without service communication or background tasks to simulate a communication load on the controller during design and programming. Use this setting for testing only.

Programming Considerations

Apply these guidelines when programming the primary controller for redundancy or Logix SIS.

Data Transfer

IMPORTANT When you write to a tag, regardless if the data is the same or different, the system crossloads it, along with the used memory that is in the same package, during the next configured crossload time. For optimal performance, write to tags only when necessary. For example, do not write to tags for HMI reads faster than 2x the update rate.

- For data that is known to change frequently, we recommend grouping it all into a structure. You can then reference each member of this structure by using the alias functionality with only minor changes to the application programming. This can minimize the amount of data that is required to be transferred.
- Program sync points can be selectively turned off to reduce the frequency of transferred data. For optimal performance have as few sync points as the application allows.

For more information, see [Configure Crossload and Synchronization Settings](#).

SSV Instruction Operation

Modifications that are made by SSVs are not crossloaded to the secondary while qualifying, locking, or locked.

Check the module redundancy state, and do not execute SSVs when in these states if it is important that the operation is reflected on the secondary.

Communication Performance

- Controller applications can experience higher communication utilization when large portions of the I/O tree are not physically present, such as multiple I/O chassis. The increased communication utilization can result in an increase in the total time that is needed to qualify the redundant system.

The communication utilization can be partially reduced by inhibiting the missing I/O in the configuration tree, but it will still be higher than if the I/O were physically present and operational.

- Frequent and sustained incoming data table writes (>10/s for minutes) to controller tag values of a redundant controller can impact the communications performance of the redundant controller.

Examples of incoming data table writes include:

- Executing a message (MSG) instruction with CIP Data Table Write message type from another controller targeted to the redundant controller
- Writing a tag value from an HMI
- Modifying a tag value while online with the Studio 5000 Logix Designer® Application

Impacts on communications performance can include the following:

- Reduced responsiveness while online with Studio 5000 Logix Designer® application
- Error (16#000c) reported when a controller with many consuming tags (>15) attempts to establish connections to the redundant controller's produced tags

IMPORTANT FactoryTalk® Linx and FactoryTalk Linx Gateway are optimized to reduce the communications burden on the controller.

Program-scoped Tags

- Program-scoped tags remove the need for UID/UIE instructions around instructions like bit shifts, and can also improve the performance of the highest priority task.
- Program-scoped tags only help with the performance of higher priority tasks, so they have no impact on performance for applications with only one task.
- The controller isolates program-scoped data from controller-scoped data. At each sync point, the controller transfers the controller-scoped data that is flagged for crossloading, along with the program-scoped data that is flagged for crossloading for the programs that have executed since the last sync point. We recommend making more use of program-scoped data, especially when using multiple tasks.

IMPORTANT We recommend not using InOut parameters between programs in different tasks. This data may not remain bumpless during switchover.

Instruction Operation

- Make the size of the following as small as needed for the application:
 - Data arrays/structures/UDTs
 - Add-On Instructions
 - FBD routines in ControlLogix 5580 redundancy
- For FBD routines, use Function Block functions when possible. Function Block functions do not have backing tag structures and reduce the amount of data that requires crossloading.
- BSR, BSL, FAL, FBC, DDT, SRT, and FFU instructions

When referencing controller-scoped tags in a lower or same priority task, partial updates can be crossloaded to the secondary as part of the other task's sync point. If a switchover occurs, the instruction could have incorrect data. Use UID/UIE pairs around the instruction or use program-scoped tags instead.
- When performing MSG reads, the MSG backing tag and the data tag should be at the same scope so that they are tracked together.

Alarms

- If a substantial number of alarms change state often, such as with every scan cycle, synchronization can be interrupted and the system can be stuck in a qualifying state until the alarms become stable. For more information, see the Knowledgebase Technote [Studio 5000 & ControlLogix: ALMA/ALMD instruction limits](#).
- The alarm burst of many Logix tag-based alarms can lead to a significant increase of a task scan time on a synchronized redundant chassis pair. The scan time increase depends on the number of alarm conditions that change state during the alarm burst and their level of nesting.

IMPORTANT Each 1 - 25 tag-based alarm conditions established within one particular scope (each scope is determined by a separate identifier within the alarm fully qualified name) adds roughly 0.4 ms to the program scan time, while each level of nesting can add 0.4 ms in the worst case scenario.

We recommend the following:

- Minimize the number of the alarm conditions that can change state during a potential alarm burst.
- Avoid excessive nesting of the conditions.
- Measure potential alarm bursts during system commissioning and change the commissioned project if measured scan times are not acceptable.

Diagnostics

You can use these programming features to assist with diagnostics:

- To track and display redundancy status on an HMI or other user consumable interface, use GSV instructions.
- For Logix SIS redundancy, you can determine if the system is qualified and synchronized by using the Redundancy System Status bit (S:R) in your logic.

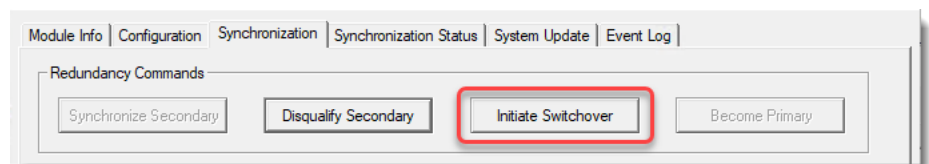
For more information about these programming features, see [Use Logic to Monitor Status](#).

Conduct a Test Switchover

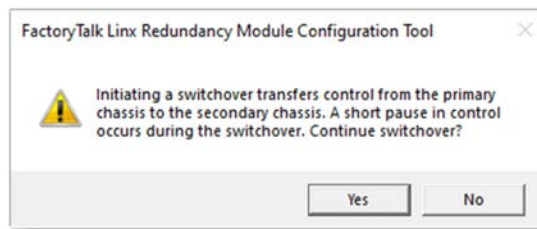
Complete these steps to verify that your redundant system switches over as expected. Your system must be fully qualified before you begin.

IMPORTANT To confirm that configured settings behave as expected, we recommend that you test a switchover before placing the redundant chassis pair in operation.

1. Access the RMCT for the primary redundancy module.
2. On the Synchronization tab, select Initiate Switchover.



3. When the following message appears, select Yes to begin the switchover.



4. Verify that the switchover was successful.

Synchronization After a Switchover

If your Auto-synchronization setting is Always, your system begins synchronizing immediately after the switchover. To monitor the synchronization of your system after you initiate the test switchover, you can use these methods:

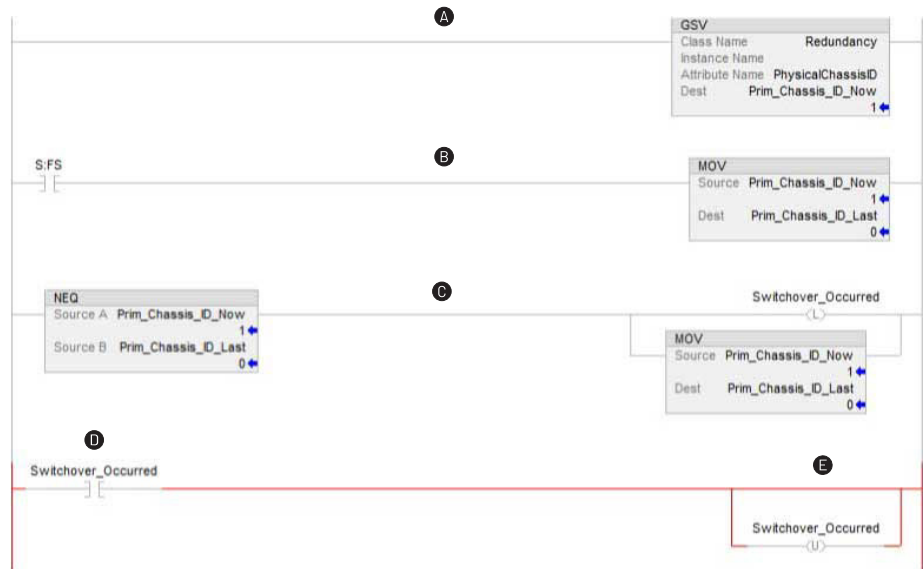
- On the Synchronization Status tab in the RMCT, refer to the Secondary Readiness column. The states No Partner, Disqualified, Synchronizing, and Synchronized indicate the stages of synchronization.
- On the front panel of the redundancy modules, refer to the status messages.
- Run a second test switchover where you power off the primary chassis to initiate the switchover.

IMPORTANT We recommend that you perform a power cycle switchover once per year to proof test the redundancy system. This test can also help improve availability calculations.

Program Logic to Run After a Switchover

If your application requires certain logic or instructions to be executed after a switchover, then use programming and tags similar to the values shown in this ladder logic example.

Figure 47 - Precondition Used to Run Logic After Switchover



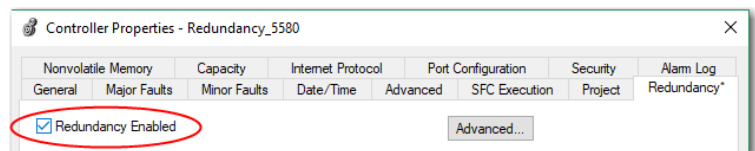
Item	Description
A	The GSV instruction obtains the chassis ID of the primary chassis in control.
B	If this is the first program scan, then use the current primary chassis ID as the chassis ID for the last scan.
C	If a switchover occurs, the chassis ID changes. The NEQ instruction compares the current and last primary chassis ID values. If the values are different, the Switchover_Occurred bit is turned on. Also, the current primary chassis ID is moved into the last chassis ID.
D	If the Switchover_Occurred bit is on, then the instructions added to this rung are executed and the Switchover_Occurred bit is reset.
E	Add your switchover-dependent instructions here.

Download the Project

Download the project only to the primary controller. When the secondary controller is synchronized, the system automatically crossloads the project to the secondary controller.

IMPORTANT If the secondary chassis was qualified and becomes disqualified after you download the project, verify that you have enabled the controller for redundancy.

In Logix SIS, a secondary chassis can be disqualified if the safety signature cannot be validated.



Store a Redundancy Project to Nonvolatile Memory

Use this procedure to store an updated project and firmware to the nonvolatile memory card of the controller. You can store a project to nonvolatile memory in either of these conditions:

- Store a project with the controller in Program or Remote Program mode
- Store a project while a system is running

IMPORTANT

We recommend that you store the same project on the nonvolatile memory cards of both controllers. Then, if a primary or secondary controller loses the project from its internal memory, you can load the most recent project back onto that controller.

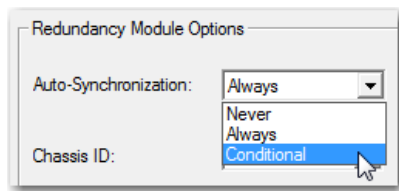
If you store the same project on the nonvolatile memory cards of both controllers, while the process is running, you must save the project on the controllers while they are in the secondary controller state. To do so, you save the project on the secondary controller, conduct a switchover, and save the project on the new secondary controller. Even if you do not plan to use the SD card, leave the card installed in the controller to collect diagnostic information that you can provide to Rockwell Automation Technical Support.

For more information, see the steps in [Store a Project with Controller in Program or Remote Program Mode](#) or [Store a Project While a System is Running](#).

Store a Project with Controller in Program or Remote Program Mode

To store the controller project in nonvolatile memory while the system is not running, complete these steps. Before you begin, verify that a controller communication path has been specified and that you are able to go online with the primary controller.

1. Verify that the redundant chassis are synchronized.
2. Put the primary controller into Program or Remote Program mode.
3. Access the RMCT.
4. On the Configuration tab, set Auto-synchronization to Conditional.

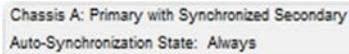


5. On the Synchronization tab, select Disqualify Secondary.
6. In the Logix Designer application, access the Controller Properties dialog box and select the Nonvolatile Memory tab.
7. Select Load/Store.
8. Select <-- Store and then select Yes.
9. When the store is complete, go online with the secondary controller.
10. Complete [steps 6...8](#) to store the project in nonvolatile memory of the secondary controller.
11. Access the RMCT.
12. On the Synchronization tab, select Synchronize Secondary.
13. On the Configuration tab, set Auto-synchronization to your preferred setting.

Store a Project While a System is Running

To store your controller project in nonvolatile memory while your redundant system is running, complete these steps.

1. Access the RMCT.
2. Verify that the redundant chassis are synchronized.



Chassis A: Primary with Synchronized Secondary
Auto-Synchronization State: Always

3. On the Configuration tab, set Auto-synchronization to Never.
4. On the Synchronization tab, select Disqualify Secondary.
5. Go online with the secondary controller.

IMPORTANT Do not go online with the primary controller until you have completed this procedure.

6. In the Logix Designer application, access the Controller Properties dialog box and select the Nonvolatile Memory tab.
7. To store the project in nonvolatile memory, select Load/Store then <--Store.
8. Access the RMCT.
9. On the Synchronization tab, select Synchronize Secondary and wait for the system to synchronize.
10. Select Initiate Switchover.
11. Go online with the new secondary controller.
12. To store the project, complete [step 6](#) and [step 7](#).
13. On the Configuration tab of the RMCT, set Auto-synchronization to your preferred setting.
14. On the Synchronization tab, select Synchronize Secondary.

Load a Project

If you must load a project from nonvolatile memory, you must first disqualify your redundancy system. You then load the project from the nonvolatile memory card to the primary controller and resynchronize the redundant chassis once the load is complete.

For details about loading a project from nonvolatile memory, see the Logix 5000 Controllers Nonvolatile Memory Card Programming Manual, publication [1756-PM017](#).

Online Edits

You can edit the redundant controller program while the system is online and running. However, considerations for redundancy must be made alongside the guidelines in the Logix 5000 Controllers Quick Start, publication [1756-QS001](#).

Partial Import Online (PIO)

Consider these points when using PIO with redundancy systems:

- If you select Import Logix Edits as Pending or Accept Program Edits when executing a PIO, the primary controller treats the PIO feature as a set of multiple test edits where, after the import is complete, you can switch between testing the edits or not.
- We recommend that you do not use Finalize All Edits in Program when you import edits. If you use this option, any failure due to the import causes a failure on the new primary controller after a switchover. If the new edits cause the controller to have a major fault, both controllers experience the major fault, resulting in loss of control.
- If edits exist in the primary controller due to a PIO, they are treated the same as normal test edits regarding the 'Retain Test Edits at Switchover' selection and Redundancy System Update.
- If a PIO is in progress, the primary controller rejects any attempt to qualify.
- If you attempt to initiate a PIO on a primary controller in the process of qualifying the system, that PIO is rejected.
- If a switchover occurs while the PIO is still in process, a PIO to the new primary controller can either fully end or fully complete, depending on how far the PIO had proceeded at the time of switchover.

If the PIO does not complete due to the switchover, reattempt the PIO after the system has synchronized.

To perform online edits, consider the following:

- Plan for test edits
- Assemble edits with caution
- Reserve memory for tags and logic in ControlLogix 5570 redundancy

Plan for Test Edits

Before you edit your redundant program while your system is running, verify that the Retain Test Edits on Switchover setting meets your application requirements for standard tasks.

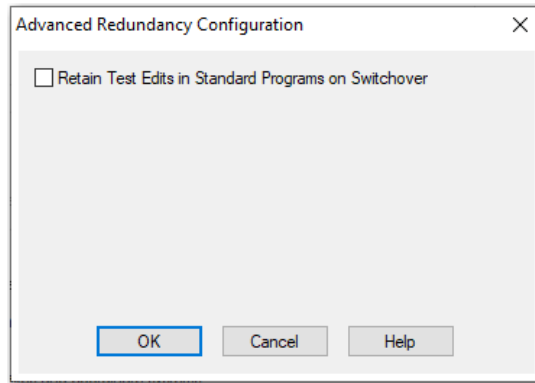
IMPORTANT	<p>In Logix SIS redundancy, test edits that apply to the safety task are not canceled, regardless of the configuration of the Retain Test Edits on Switchover setting. If an online test edit results in a fault to the primary safety controller, then the edit causes the same fault on the secondary safety controller.</p> <p>For test edits that apply to standard tasks in any type of redundancy system, we recommend that you leave the Retain Test Edits on Switchover checkbox cleared to avoid faulting both controllers when testing your edits.</p>
------------------	--

Use this table to determine the Retain Test Edits on Switchover setting that suits your application requirements for standard tasks.

Standard Task Application Requirement	Retain Test Edits on Switchover Setting
Help prevent a test edit from faulting the primary and secondary controllers if there is a switchover	Clear the Retain Test Edits on Switchover checkbox. The controller discards the test edits on switchover.
Keep test edits active, even if there is a switchover and at the risk of faulting both controllers	Select the Retain Test Edits on Switchover checkbox. The controller keeps the test edits active on switchover.

To access the Retain Test Edits on Switchover checkbox, select the Redundancy tab in the controller properties and then select Advanced.

Figure 48 - Retain Test Edits on Switchover



Assemble Edits with Caution

When you assemble edits to your program while online, the original program that existed before the changes were made is deleted. As a result, if the edits you assemble cause a fault on the primary controller, the new primary controller also faults after the switchover. Also, when you assemble edits in the primary controller, the edits are also assembled in the secondary controller.

Before you assemble any edits to your program, test the edits to verify that faults do not occur.

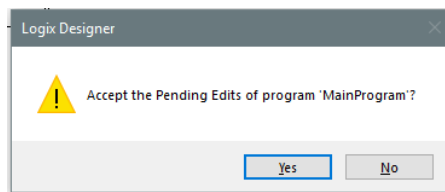
1. In the Controller Organizer, open the routine to edit.
2. Modify your routine.
3. Select Verify Routine.
4. Select Accept Pending Program Edits.



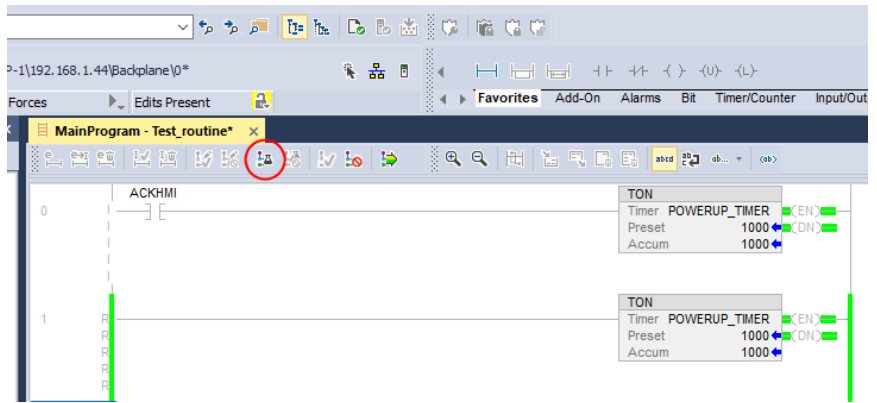
Even if you have not enabled the Retain Test Edits on Switchover property, faults can still occur on the primary and secondary controllers if the edits are assembled.

The Retain Test Edits on Switchover property affects only edits that are being tested. The Retain Test Edits on Switchover does not affect the redundant controllers that are running assembled edits.

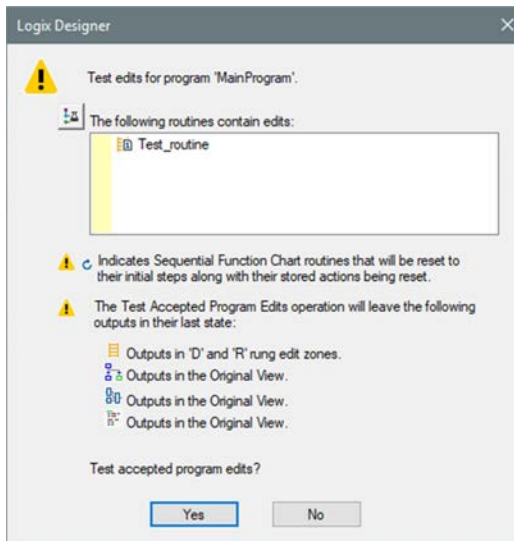
5. When the following message appears, select Yes to accept the pending edits.



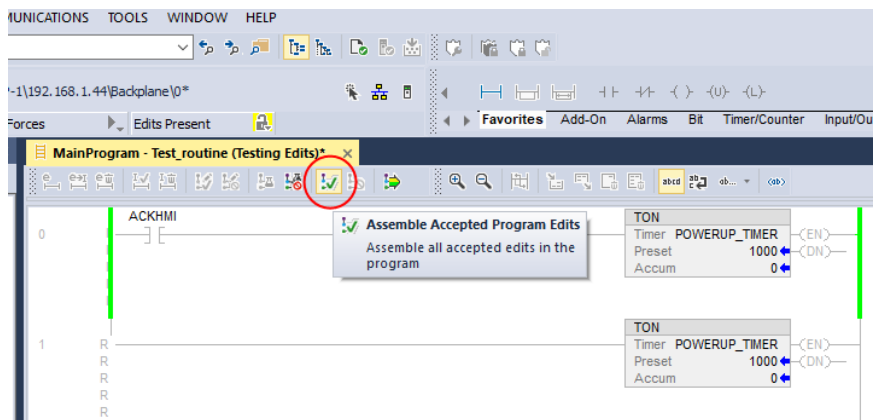
6. Select Test Accepted Program Edits.



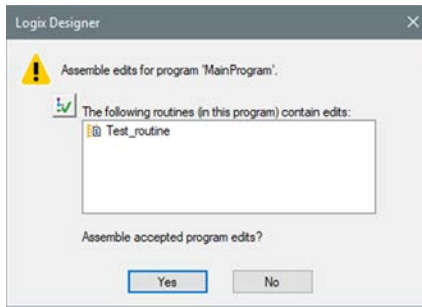
7. When the following warning appears, review the information, and then select Yes.



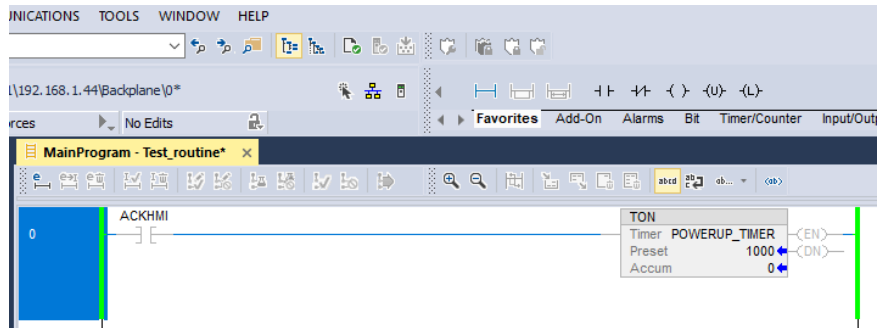
8. Select Assemble Accepted Program Edits.



9. When the following warning appears, review the information, and then select Yes.



Your edits are now assembled.



(ControlLogix 5570 Only) Reserve Memory for Tags and Logic

IMPORTANT Do not change the memory usage settings for tags and logic unless Rockwell Automation Technical Support instructs you to change the settings.

Depending on your redundant application, you may need to change the memory usage property for a ControlLogix 5570 redundant controller. The setting that you specify impacts how the controller divides memory for tags and logic to be stored to the buffer during a crossload to the secondary controller. [Table 38](#) indicates when you can consider changing the memory usage setting.

Table 38 - Possible Memory Usage Setting Change

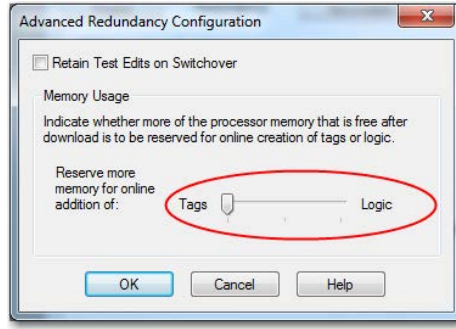
If your online edits are primarily changes to	Then move the Memory Usage slider towards
Tags with little or no changes to logic	Tags
Logic with little or no new tags created	Logic

IMPORTANT Do not set the Memory Usage slider to only tags or logic:

- If you move the slider to only tags, you cannot perform edits while online and OPC communication can fail.
- If you move the slider to only logic, you cannot create or edit any tags while online.

IMPORTANT For ControlLogix 5570 controllers with firmware revision 19, the Memory Usage slider is set to the far left for tags and the first synchronization attempt is successful. However, after switchover or disqualification, the next qualification attempt fails, and one or more entries appear in the secondary redundancy module event log with the following description: '(14) Error Setting Up Data Tracking.'

To recover from this issue, move the slider slightly to the right. This change must be made offline or in Program mode. Additionally, you must download the updated application to the disqualified secondary to update its configuration. The next qualification attempt is successful.



Calculate RPI Timeout for Standard I/O

Assuming best practices are followed, switchover time can be as slow as 50 ms.

Use the following formula to calculate an RPI timeout for standard I/O:

$$RPI * 2^X = Y \text{ where for the lowest } X, Y \text{ is } \geq (4 * RPI) + 100 \text{ ms}$$

EXAMPLE RPI = 4 ms for X = 5, Y = 128
 Timeout = 128 ms because 128 > 116 ((4*4) + 100)

Table 39 - RPI Timeout Examples

RPI (ms)	Timeout (ms)
5	160
10	160
15	240
24	384
25	200

Initiate Redundancy and System Update Commands

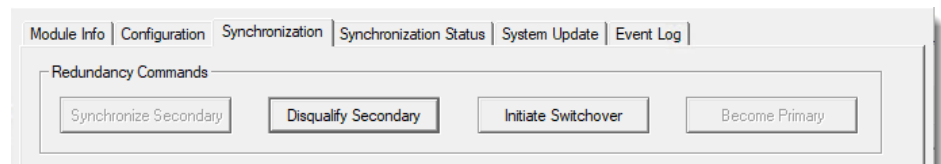
The redundancy module provides ways to control the redundancy state of the redundant chassis pair and to perform firmware updates without interrupting redundant operation.

Initiate Redundancy Commands in the RMCT

On the Synchronization tab in the RMCT, you can initiate these redundancy commands:

- Synchronize Secondary
- Disqualify Secondary
- Initiate Switchover
- Become Primary

Figure 49 - Redundancy Commands



Synchronization events are logged on the Synchronization tab of the RMCT and can help you troubleshoot redundancy issues:

- For 1756-RM3 modules, see [View the Synchronization Log](#).
- For 1756-RM2 modules, see [View Recent Synchronization Attempts](#).

Synchronize Secondary

The Synchronize Secondary command forces the primary redundancy module to attempt synchronization with its partner.

This command is available only when the chassis redundancy state is one of the following:

- Primary with Disqualified Secondary
- Disqualified Secondary

Synchronization is asynchronous with the execution of this command. Successful execution of this command begins with synchronization, which can take several minutes. Monitor the chassis status at the bottom of the RMCT to determine when synchronization is complete.

Disqualify Secondary

The Disqualify Secondary command forces the primary redundancy module to disqualify its partner.



ATTENTION: Disqualifying the secondary chassis makes it unable to assume control functions and redundancy is lost. If you disqualify the secondary and a major fault occurs on the remaining primary, a switchover does not occur.

This command is available only when the chassis redundancy state is one of the following:

- Primary with Synchronized Secondary
- Synchronized Secondary

If you use the Disqualify Secondary command when the Auto-synchronization setting is Always, a synchronization attempt occurs immediately after the secondary chassis becomes disqualified. To keep the secondary disqualified after initiating the Disqualify Secondary command, set Auto-synchronization to Conditional or Never before disqualifying the secondary.

Initiate Switchover

The Initiate Switchover command forces the system to initiate an immediate switchover from the primary chassis to the secondary chassis.

Reasons to initiate a switchover manually include these scenarios:

- During a redundancy firmware update
- After you complete maintenance on one chassis in the redundant chassis pair
- To perform a test of your redundant system behavior by simulating a failure that is detected in the primary chassis

This command is available only when the chassis redundancy state is one of the following:

- Primary with Synchronized Secondary
- Synchronized Secondary

Become Primary

The Become Primary command forces a disqualified secondary chassis to become a primary chassis. This command is available only when the chassis redundancy state is Secondary with No Primary.

IMPORTANT

When you initiate the Become Primary command, the controller restarts with the controller project erased. During the power-up process, the controller is unavailable. Once the controller is powered-up, download your current project to the controller.

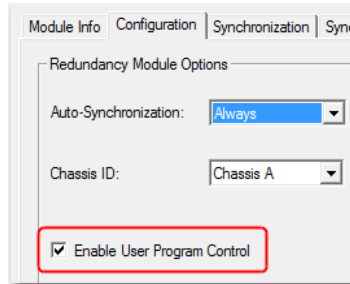
Initiate Redundancy Commands with MSG Instructions

For some applications, consider programming the controller to initiate redundancy system commands via the redundancy modules. You can configure an MSG instruction to issue the following redundancy commands:

- Initiate a switchover
- Disqualify the secondary chassis
- Synchronize the secondary chassis

To initiate redundancy commands via an MSG instruction, follow these steps.

1. On the Configuration tab of the RMCT, verify that Enable User Program Control is selected for the redundancy module.



2. In the program for the redundant controller, create an MSG instruction.
3. On the Communication tab of the Message Configuration dialog box, configure the path to the redundancy module and verify that the Connected checkbox is cleared.

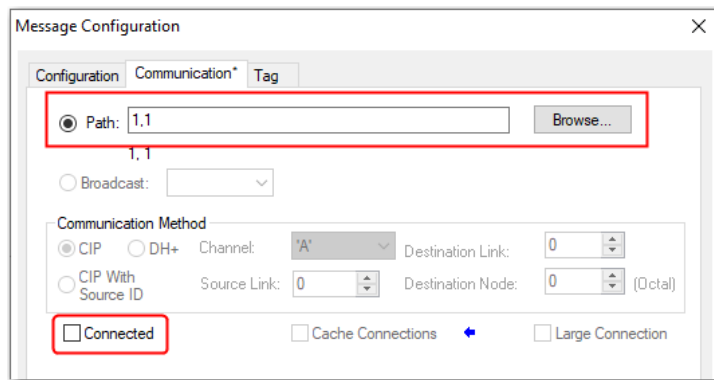


Table 40 - Redundancy Command Communication Parameters

Parameter	Value
Path	1,[slot number of the redundancy module] For example, enter 1,1 for a redundancy module in slot 1 of the chassis.
Connected	Leave the Connected checkbox cleared.

- On the Configuration tab of the Message Configuration dialog box, configure the MSG instructions with the following parameters depending on the redundancy command.

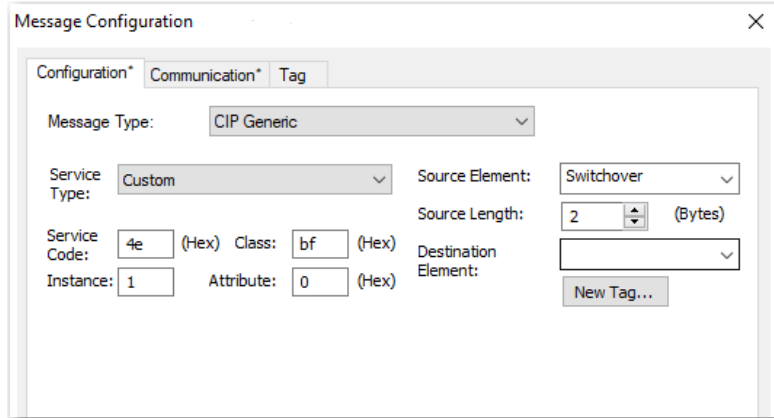


Table 41 - Initiate a Switchover

Parameter	Value
Message Type	CIP Generic
Service Type	Custom
Service Code	4e
Class	bf
Instance	1
Attribute	None - no value needed
Source Element	INT tag with a value of 1
Source Length	2
Destination Element	None - no value needed

Table 42 - Disqualify the Secondary Chassis

Parameter	Value
Message Type	CIP Generic
Service Type	Custom
Service Code	4d
Class	bf
Instance	1
Attribute	None - no value needed
Source Element	INT tag with a value of 1
Source Length	2
Destination Element	None - no value needed.

Table 43 - Synchronize the Secondary Chassis

Parameter	Value
Message Type	CIP Generic
Service Type	Custom
Service Code	4c
Class	bf
Instance	1
Attribute	None - no value needed
Source Element	INT tag with a value of 1
Source Length	2
Destination Element	None - no value needed.

MSG Instruction Behavior During Qualification and Switchover

To understand how MSG instructions operate during qualification and switchover, refer to the following sections.

During Qualification

MSG instructions operate as follows during qualification of the redundant chassis pair:

- The status message on the front of the redundancy module displays QFNG for qualifying.
- If a configured message is cached, the primary controller automatically establishes a connection with the secondary controller with no errors.
- If a configured message is uncached or unconnected, the message experiences the following error: Error 1 Extended Error 301, No Buffer Memory.

During a Switchover

MSG instructions operate as follows during a switchover:

- In the primary controller, the message instruction status bits update asynchronously to the program scan. Consequently, you cannot crossload your message instructions status bits to a secondary controller.
- Any active message instructions in the old primary controller become inactive. When the switchover occurs, you must reinitialize the execution of your message instructions in the new primary controller.
- Cached and connected messages cause the message instruction to pause for 7.5 seconds because the primary controller has not received a response from the secondary controller:
 - For cached messages, the message instruction tries to execute three more times, each attempt followed by a pause of 7.5 seconds. If 30 seconds pass and the targeted controller does not respond to the initiating controller, then the switchover errors out with connected timeout Error 1 Extended Error 203. An example of a connected message is CIP™ data table read-and-write messages after a connection has been established.
 - Uncached messages error out after 30 seconds if you have initiated them because the initiating controller never received a reply to the forward-open request. The error is Error 1F Extended Error 204, an unconnected timeout. Examples of uncached messages include CIP generic messages and messages that are captured during the connection process.

Initiate System Update Commands in the RMCT

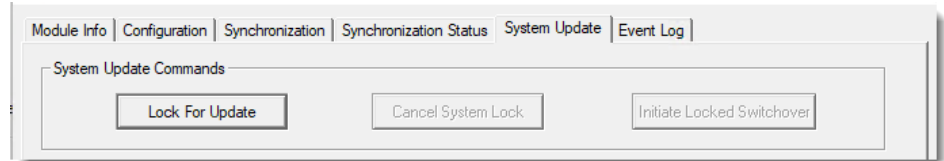
To perform firmware updates for the secondary chassis while the primary chassis remains in control, use the system update commands on the System Update tab of the RMCT. The system update commands are available only when connected to the primary redundancy module.

To perform an online system update, follow the procedures in [Chapter 14](#).



ATTENTION: When performing firmware updates, redundancy is lost. If there is a fault on the operating primary chassis, the system cannot switch control to the secondary chassis.

Figure 50 - System Update Commands on Primary Redundancy Module



When system update commands are in progress, you cannot access these tabs:

- Configuration
- Synchronization
- Synchronization Status

If you attempt to access any of these tabs while the system is locked or is completing a locked switchover, an error message appears.

System update events are logged on the System Update tab of the RMCT and can help you troubleshoot system update issues:

- For 1756-RM3 modules, see [View the Lock for Update Logs](#).
- For 1756-RM2 modules, see [View System Update Logs](#).

Lock for Update

The Lock for Update command enables you to synchronize a redundant chassis pair under these conditions:

- The secondary redundancy module uses a firmware revision and programming software version that is later than the primary redundancy module.
- The active primary redundancy module uses a firmware revision and programming software version that is earlier than the secondary redundancy module.

IMPORTANT During a lock for update in Logix SIS redundancy, the safety function is temporarily muted for up to 2 seconds + 1 safety task period.

The Lock for Update command is available only when all modules in the primary chassis have no compatibility discrepancies. Before issuing the lock command, complete these tasks:

- On the Configuration tab, set Auto-synchronization to Never.
- Disqualify the secondary chassis by using the Disqualify Secondary command on the Synchronization tab of the secondary redundancy module.
- Update the primary and secondary redundancy modules to compatible firmware revisions.
- Update all other modules in the secondary chassis to their intended firmware revisions.
- Configure the controller project as required to accommodate the update and replacement of modules if needed.

The lock can take several minutes to complete. To determine when the lock is complete, check the following:

- System Update Lock Attempts log on the System Update tab. The status changes from In Progress to Locked.
- Chassis status in the status bar at the bottom of the dialog box. The status changes from Primary with Disqualified Secondary to Primary Locked for Update.

Abort System Lock

To stop a system lock already initiated with the Lock for Update command, use the Abort System Lock command. The command is available as soon as you initiate a lock.

When you select Abort System Lock, the following occurs:

- The redundant chassis status returns to Primary with Disqualified Secondary.
- The system update stops and the program in the secondary controller clears.

If you select Abort System Lock, you must download the program to the secondary controller before you can attempt a Lock for Update again.

Initiate a Locked Switchover

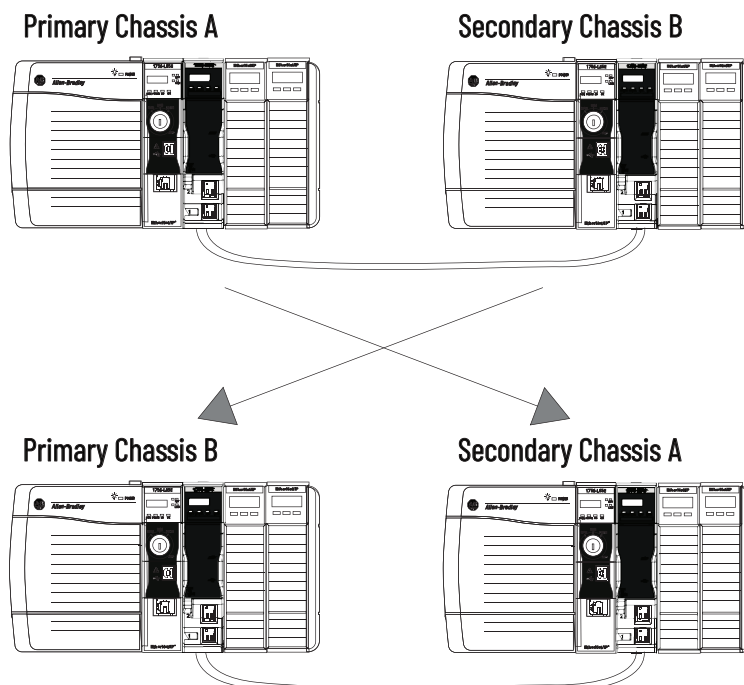
The difference between a locked switchover and a normal switchover is that you must always initiate a locked switchover. You or a fault in the primary chassis can initiate a normal switchover.

The Initiate Locked Switchover command is available under these conditions:

- The chassis state is Primary with Locked Secondary.
- The Lock for Update process is complete.

If you select Initiate Locked Switchover, your secondary chassis assumes control and becomes the new primary. The old primary is now the new secondary chassis and you can update the firmware of the modules in the new secondary chassis.

Figure 51 - Illustration of Switchover



Notes:

Monitor and Maintain a Redundancy System

To monitor and maintain a redundancy system, you can do the following:

- Reference the controller log
- Track changes to components, such as routines and Add-On Instructions
- Use logic to monitor status
- Monitor communication module statistics
- Understand temperature monitoring and fault behavior

Reference the Controller Log

A controller log is a record of changes, including changes made in programming software, controller keyswitch interactions, and events. The log is stored on the NVS memory of the controller automatically. You can move the log to an SD card as needed or automatically at predefined times. The NVS memory of the controller and each external memory card type has a maximum number of entries that they can store.

For more information about controller logging, see the Logix 5000 Controllers Information and Status Programming Manual, publication [1756-PM015](#).

Redundancy System Considerations

Because redundancy systems operate with partnered controllers, there are considerations that you must consider regarding controller logging:

- The primary and secondary controllers maintain separate logs.
- You do not need to synchronize the logs.
- On the primary controller, controller logging occurs exactly as it does on a controller in a non-redundant system, regardless of whether the system is qualified and synchronized or disqualified.
- A secondary controller logs the removal or insertion of an SD card, in any operating state. Otherwise, the secondary controller only logs events that occur when the controller is in a disqualified state.

Track Changes to Components

In the Logix Designer application, you track whether routines, Add-On Instructions, and constant tags have been changed. The Logix Designer application creates a tracked state value to indicate the current state of all components.

Tracked components appear in the Tracked Components dialog box, which is accessible from the Security tab of the controller properties.

For more information, see the Logix 5000 Controllers Information and Status Programming Manual, publication [1756-PM015](#).

Use Logic to Monitor Status

IMPORTANT

When programming your redundancy system, program so that your redundancy system status is continually monitored and displayed on your HMI device.

If your redundancy system becomes disqualified or a switchover occurs, the change in status is not automatically annunciated. You must program the system to communicate the change in status via your HMI or other status-monitoring device.

For most redundant applications, you must program to obtain the status of the system. Program to obtain system status when you do the following:

- Program HMI to display the system status
- Precondition logic to execute based on the system status
- Use the diagnostic information to troubleshoot the system

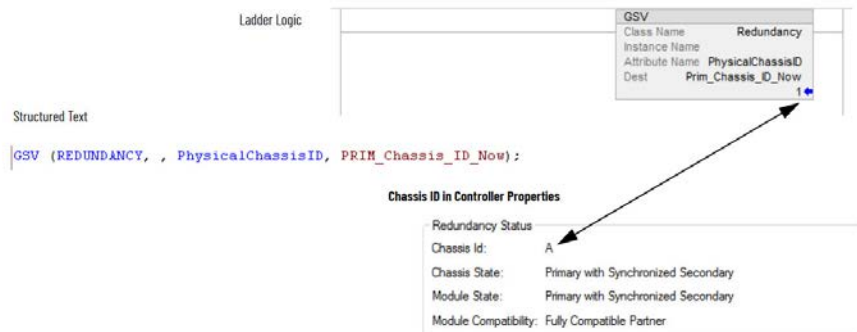
Get System Value Instruction

To obtain the status of your redundant system, use a Get System Value (GSV) instruction in your program and plan for the tags you are writing the values to.

In this example, the GSV instruction is used to obtain the chassis ID of the chassis that is functioning as the primary. The **PhysicalChassisID** value is stored in the **PRIM_Chassis_ID_Now** tag. The **PhysicalChassisID** value that is retrieved matches the Chassis ID indicated in the Controller Properties dialog box.

Physical Chassis ID	Chassis ID
0	Unknown
1	Chassis A
2	Chassis B

Figure 52 - GSV Instruction to Get Chassis ID



For more information about the REDUNDANCY object attributes, see [Appendix B](#).

Redundancy Status Bit

In Logix SIS and ControlLogix® 5580 systems, you can determine if your system is operating with redundancy by using the Redundancy Status bit (S:R). You can use the bit in standard or safety task logic. The bit can monitor the system while the controller is in Run or Test mode.

S:R Bit Status	Redundancy Status
On (1)	The system is operating with redundancy.
Off (0)	The system operating without redundancy.

IMPORTANT

When the S:R bit turns Off in a safety task that supports a SIL 3 safety function, you must repair the system within your specified mean repair time (MRT). If the system is not repaired within the MRT, you must take a specified action to maintain or achieve a safe state.

For MRT requirements, see the Logix SIS Safety Reference Manual, publication [1756-RM015](#).

Figure 53 - Redundancy Status Bit



(1756-RM2 and 1756-RM Modules Only). Get Attribute Message for Fiber Channel Status

For 1756-RM2 or 1756-RM modules, you can use a CIP Generic Get Attribute message to retrieve the status of the fiber channels of the redundancy module.

CIP Generic Message - Get Attribute Single

- Class: 305
- Instance: 1
- Attribute: 4E (Channel 1) or 4F (Channel 2)

Return Value is a signed DINT, Value Equals:

- 1 = ACTIVE
- 2 = REDUNDANT
- 3 = LINK_DOWN
- 4 = TRANSCEIVER_NOT_INSTALLED
- 5 = TRANSCEIVER_FAILED
- 7 = UNKNOWN

For more information, see Knowledgebase Technote [Viewing the 1756-RM2 Fiber Channel Status From a Logix Application](#).

Monitor Communication Module Statistics

Use the diagnostic webpages for communication modules to monitor the following statistics:

- CPU usage
- Connections used

For information about how to access the diagnostic webpages, see the ControlLogix EtherNet/IP Network Devices, publication [1756-UM004](#).

CPU Usage

The CPU usage of the EtherNet/IP modules must be at 80% or less. CPU usage below 80% reserves enough CPU functionality for the EtherNet/IP module to facilitate a switchover.

If the CPU usage is above 80%, the secondary chassis can fail to synchronize with the primary chassis after a switchover occurs. Unscheduled communication can be slowed.

If you must reduce the CPU usage of your EtherNet/IP modules, consider making the following changes:

- Review the Requested Packet Interval (RPI) of your connections.
 - The RPI rate of a connection affects the loading on the associated communications modules.
 - Before changing RPI rates, see the guidelines for I/O modules in the Logix 5000 Controllers Design Considerations Reference Manual, publication [1756-RM094](#).
- Reduce the number of devices that are connected to your module.
- Distribute the load by adding more communications modules, seven maximum, to the redundant chassis pair.
- Configure digital I/O with rack-optimized connections instead of direct connections.
- Take steps to reduce your CPU utilization. See the EtherNet/IP Network Devices User Manual, publication [ENET-UM006](#).

Connections Used

If you go online with a controller through an EtherNet/IP module that is near its connection limit, you can experience difficulty. The process of going online consumes another connection from the EtherNet/IP module. You can also experience difficulty when you add modules to the system.

Understand Temperature Monitoring and Fault Behavior

1756-RM3 redundancy modules monitor temperatures and act as the temperature reaches critical thresholds.

Refer to the following table to understand temperature monitoring and fault behavior.

IMPORTANT If you follow the recommended limits for ambient temperature and apply the required clearances around the chassis, redundancy modules should not reach temperature limits.
For temperature specifications, see the ControlLogix and GuardLogix Controllers Technical Data, publication [1756-TD001](#).

Table 44 - 1756-RM3 Temperature Monitoring

Status Message on Front Display	Fault	Result/Action
Over Temperature	Minor recoverable Fault code 0x6	The fault does not impact the redundancy state. Once the temperature cools to normal, clear the minor recoverable fault.
Critical Temperature	Major recoverable Fault code 0x5	The fault causes a disqualification and switchover. Once the temperature cools to normal, clear the major recoverable fault.
CPU Internal Thermal Fault	Major non-recoverable Fault code 0x2	The module shuts down and causes a disqualification and switchover. To recover from the fault, reset the module. If the module restarts sooner than it cools to normal temperature, the module logs additional faults according to its current temperature.

For information about how to view faults, see [Redundancy Module Faults](#).

Notes:

Troubleshoot Systems with 1756-RM3 Modules

When a fault or other event occurs on a redundancy system with 1756-RM3 modules, use these methods to determine the cause:

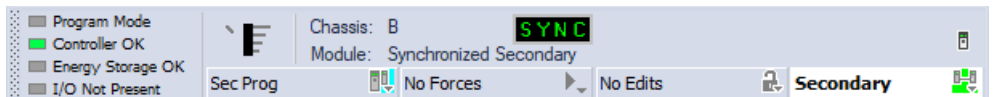
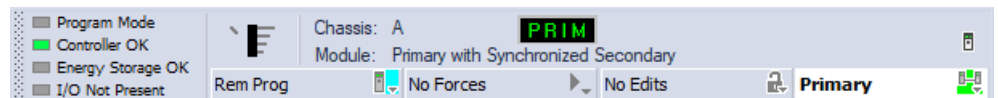
- View diagnostic information in the Logix Designer application.
- View redundancy module events and status by accessing logs in the Redundancy Module Configuration Tool (RMCT). Each partner redundancy module keeps its own events in separate logs.
- View and clear redundancy module faults.
- Check the status messages and status indicators on the front panel of the redundancy modules. See [Appendix A](#).

View Diagnostic Information in the Logix Designer Application

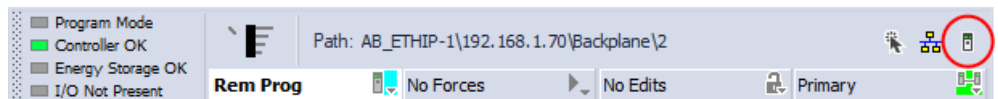
To view diagnostic information in the Logix Designer application, complete these steps.

1. Go online with the redundant controller.
2. Select Primary or Secondary, depending on which controller is online.

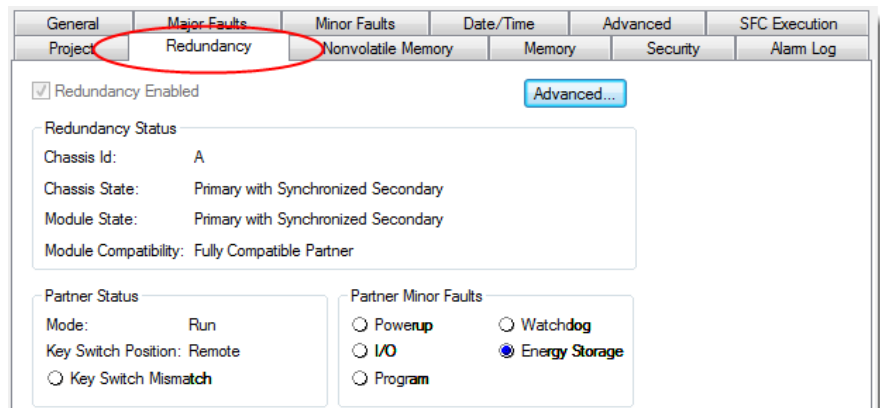
The redundant controller ID and status are displayed.



3. For more information, select the Controller Properties icon.

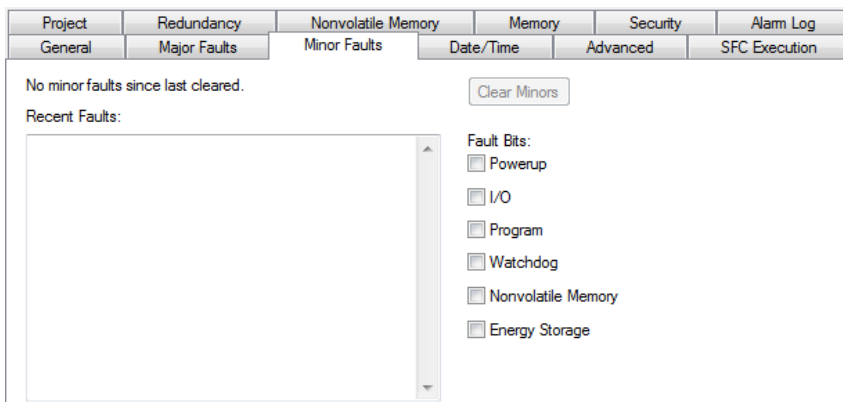


4. To view redundancy status, select the Redundancy tab.



- To view faults, select the Major Faults and Minor Faults tabs.

The fault bits are status bits that the controller sets. You can set fault bits for testing, but that is not the main purpose of these bits.



View the Synchronization Log

On the Synchronization tab of the RMCT, you can view a log of synchronization events. If qualification of the redundant chassis pair fails, use the synchronization log to help identify and resolve the cause.

Figure 54 - Synchronization Log

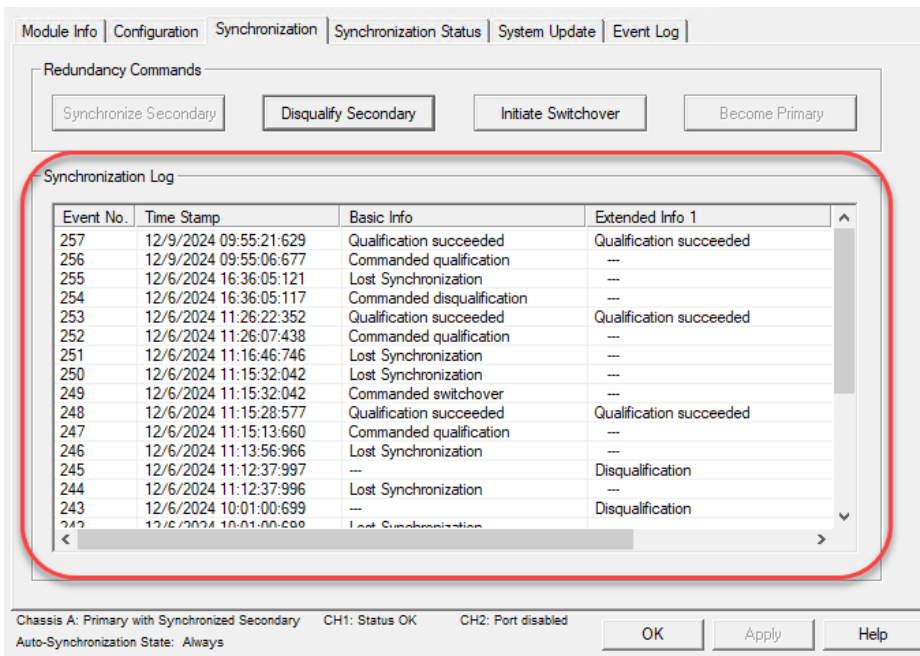


Table 45 - Synchronization Log Parameters

Parameter	Description
Event No.	A unique, sequential number to identify the event.
Time Stamp	The date and time that the event was logged.
Basic Info	A basic description of the synchronization event. If qualification did not succeed or a fault is indicated, refer to the Extended Info columns to diagnose the cause.
Extended Info 1	Additional information that is related to the basic description of the event.
Extended Info 2	Extended information is not available for every event.

View Module-level Synchronization Status

On the Synchronization Status tab of the RMCT, you can view information about all modules in the same chassis as the connected redundancy module. Use this information to identify which module pair is causing a synchronization failure. Depending on the type of synchronization failure, it can be helpful to compare the Synchronization Status tabs for the primary and secondary redundancy modules. If there is a difference between major or minor revisions of the modules, the Compatibility column shows Incompatible.

Figure 55 - Module-level Synchronization Status

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	100	1756-L85E/B	37.11	Synchronized	Primary	Full
1	100	1756-EN4TR/A	7.1	Synchronized	Primary	Full
2	100	CLX Redundancy Premium Mod...	21.11	Synchronized	Primary	Full
3	---	<empty>	---	---	---	---
4	---	<empty>	---	---	---	---
5	---	<empty>	---	---	---	---
6	---	<empty>	---	---	---	---

Chassis A: Primary with Synchronized Secondary CH1: Status OK CH2: Port disabled
Auto-Synchronization State: Always

Table 46 - Synchronization Status Parameters

Parameter	Description
Slot	The slot number of the module.
% Complete	The percentage of the synchronization status that is complete.
Module Name	The name of the module.
Module Revision	The firmware revision of the module.
Secondary Readiness	The redundancy state of the module: <ul style="list-style-type: none"> • Undefined • Synchronized • Synchronizing • No Partner • Disqualified • Locked
State	The state of the module's chassis: Primary or Secondary
Compatibility	The compatibility of the partner module in the partner chassis: <ul style="list-style-type: none"> • Undetermined • Full • Incompatible

View the Lock for Update Logs

On the System Update tab of the RMCT, you can view logs for the following events:

- System update lock attempts
- Locked switchover attempts

Figure 56 - Lock for Update Logs

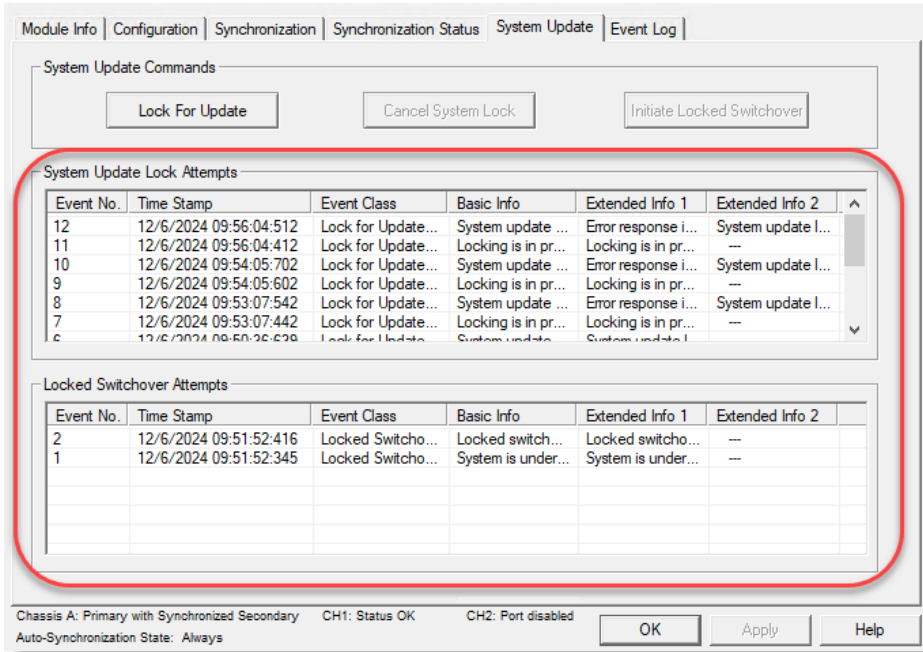


Table 47 - System Update Lock Attempts

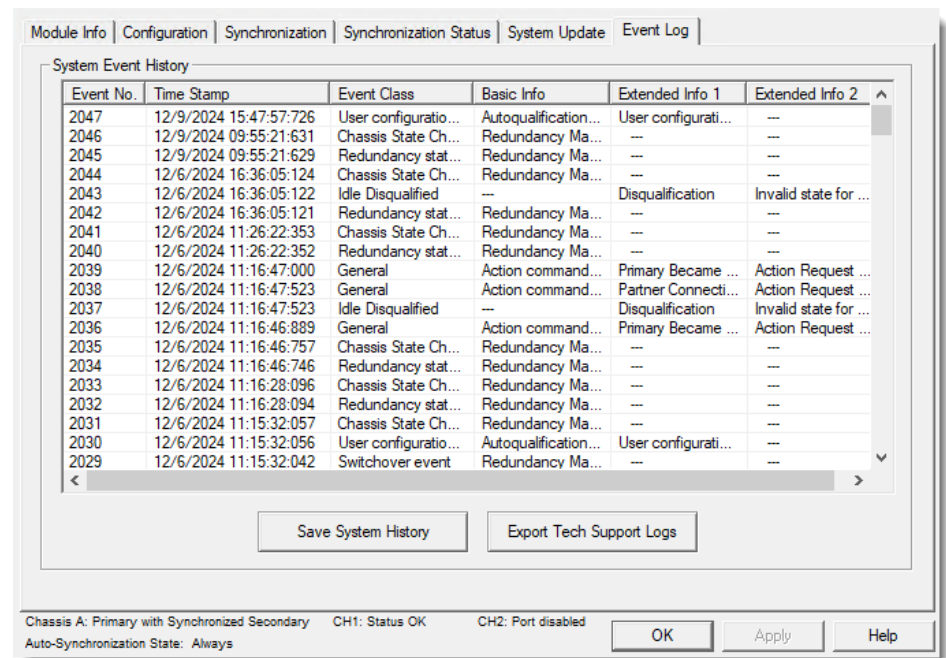
Parameter	Description
Event No.	A unique, sequential number to identify the event.
Time Stamp	The date and time that the event was logged.
Event Class	All events related to system update lock attempts have the same event class: Lock for Update log
Basic Info	One of the following basic descriptions of the event: <ul style="list-style-type: none"> • System update lock is not attempted • Locking is in progress • System update lock is successfully completed • System update lock attempt failed If a system update lock attempt failed, refer to the Extended Info parameters to identify the cause.
Extended Info 1	Additional information that is related to the basic description of the event. Use this information to troubleshoot failed lock attempts. Possible causes include the following:
Extended Info 2	<ul style="list-style-type: none"> • Wrong chassis redundancy state • Wrong autoqualification option • Major fault in redundancy module • Modules in primary chassis and secondary chassis do not match Extended information is not available for every event.

Table 48 - Locked Switchover Attempts

Parameter	Description
Event No.	A unique, sequential number to identify the event.
Time Stamp	The date and time that the event was logged.
Event Class	All events related to locked switchover attempts have the same event class: Locked Switchover log
Basic Info	One of the following basic descriptions of the event: <ul style="list-style-type: none"> • Locked switchover is not attempted • System is undergoing locked switchover process • Locked switchover is successfully completed • Locked switchover attempt failed If a locked switchover attempt failed, refer to the Extended Info parameters to identify the cause.
Extended Info 1	Additional information that is related to the basic description of the event. Use this information to troubleshoot failed locked switchover attempts. Possible causes include the following:
Extended Info 2	<ul style="list-style-type: none"> • Wrong chassis redundancy state • Major fault in redundancy module • Disconnected partner module • Synchronization connection timeout Extended information is not available for every event.

View, Save, and Export the Event Log

On the Event Log tab of the RMCT, you can view a history of events for both partner redundancy modules. You can save the system event history to nonvolatile memory and export Tech Support logs to send to Technical Support.

Figure 57 - Event Log**Table 49 - Event Log Parameters**

Parameter	Description
Event No.	A unique, sequential number to identify the event.
Time Stamp	The date and time that the event was logged.
Event Class	A broad category to classify the event. For event class descriptions and corrective actions, see Event Classes .
Basic Info	A basic description of the event.
Extended Info 1	Additional information that is related to the basic description of the event.
Extended Info 2	Extended information is not available for every event.

Event Classes

The following event classes can appear in the Event Class column in the event log.

Table 50 - Event Classes

Event Class	Description
Qualification Event	An event that is related to chassis qualification. For example, the qualification process succeeded.
Disqualification Event	An event that is related to chassis disqualification. For example, the Disqualify Secondary command was issued.
Switchover Event	An event that is related to a chassis switchover. For example, the Initiate Switchover command was issued.
RM Fault Event	One of the redundancy modules had a major or minor fault. For recovery information, see the Code field in the fault log on the Module Info tab. See Redundancy Module Faults .
User configuration change event	A redundancy module configuration parameter has been changed. For example, if you change the Auto-synchronization parameter from Always to Never, an event that is classified as Configuration is logged.
Redundancy state has changed	The state of a redundancy module changed. For example, the redundancy module lost its partner.
Chassis State Changed	The state of the redundant chassis pair changed. For example, the redundancy status changed from disqualified secondary to qualified secondary.
Idle Qualified	An event occurred while the chassis was in an idle qualified state. The event caused the chassis to leave the idle qualified state.
Idle Disqualified	An event occurred while the chassis was in an idle disqualified state. The event caused the chassis to leave the idle disqualified state.
General	An event unrelated to the redundancy state or a redundancy action.

Event Log Examples

This section contains example event log entries for typical system events.

Manual Switchover

Event Class	Basic Info	Extended Info 1	Extended Info 2
Switchover Event	Commanded switchover	–	–

Manual Disqualification

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Commanded disqualification	–	–

Qualification Successful

Event Class	Basic Info	Extended Info 1	Extended Info 2
Qualification Event	Qualification succeeded	Qualification succeeded	–

Qualification Failed Due to Incompatible Module

Event Class	Basic Info	Extended Info 1	Extended Info 2
Qualification Event	Qualification Abort	Qualification aborted due to some modules not having fully compatible partners	Bitmap of compatibility assessment for modules in chassis

Switchover Due to Module Removal from Primary

Event Class	Basic Info	Extended Info 1	Extended Info 2
Switchover Event	Redundancy Manager State: Disqualified Secondary With Primary	–	–

Switchover Due to Network Cable Removal in Primary

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Communication on switchover was lost, switchover processed with uncoordinated manner.	Switchover	—

Switchover Due to Chassis Power Fault in Primary Chassis

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Qualification Abort - Primary Module Screamed on Partner	—

Disqualification Due to Network Connection Lost between Primary and Secondary Chassis

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Qualification Abort - Disqualify command	—

Disqualification Due to Partner Chassis Power Fault

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Partner Redundancy Module has major nonrecoverable fault	—

Disqualification Due to Partner Chassis Module Removal

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Qualification Abort - Module Removal	—

Disqualification Due to Partner Chassis Redundancy Module Fault

Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Qualification Abort - Disqualify command	—

Disqualification Due to Redundancy Module Fiber Cable Disconnected or Faulted

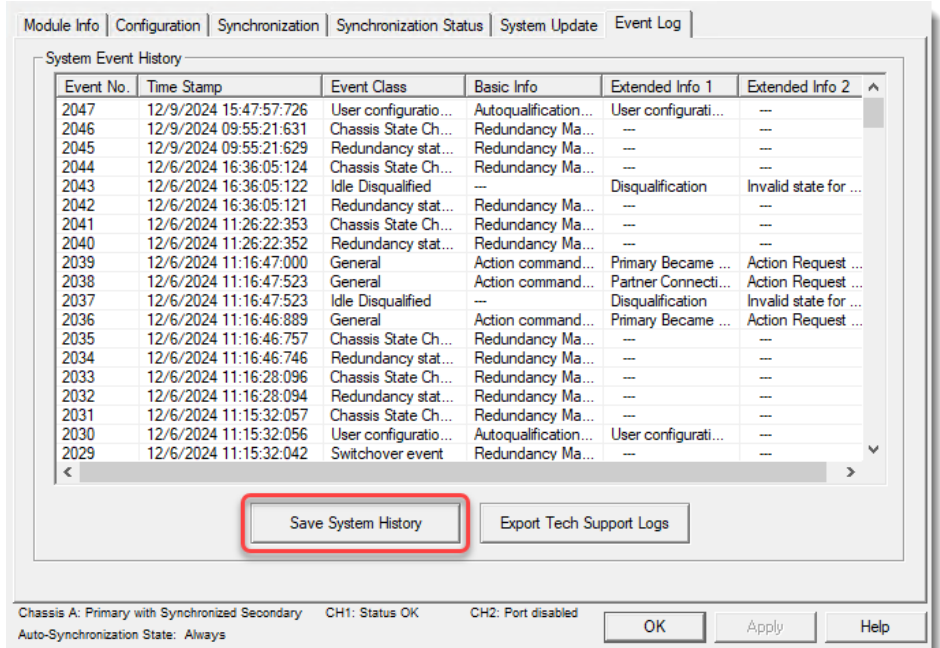
Event Class	Basic Info	Extended Info 1	Extended Info 2
Disqualification Event	Qualification Abort	Qualification aborted due to lack of partner RM.	—

Save System History

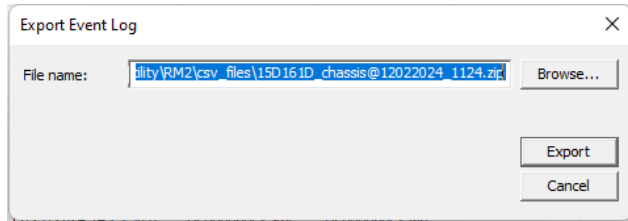
When you save system history, the RMCT saves all event log entries to a ZIP file with two CSV files: one for the connected redundancy module and one for the partner redundancy module.

To save system history, follow these steps.

1. On the Event Log tab, select Save System History.



2. Browse to the location where you want to save the ZIP file and select Export.



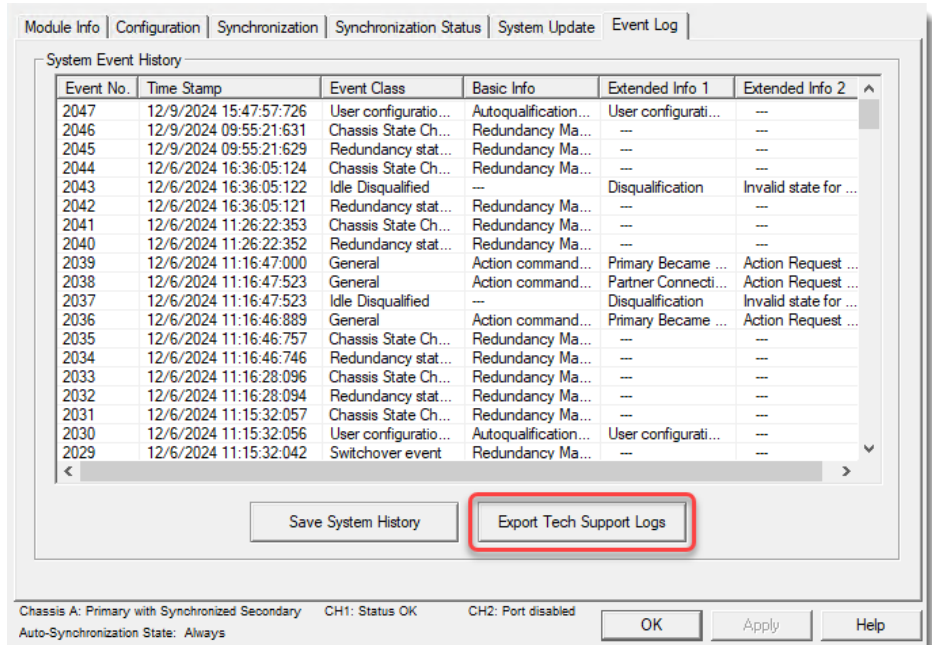
Export Tech Support Logs

To help Rockwell Automation Technical Support troubleshoot your redundancy system, you can export Tech Support logs from the Event Log tab.

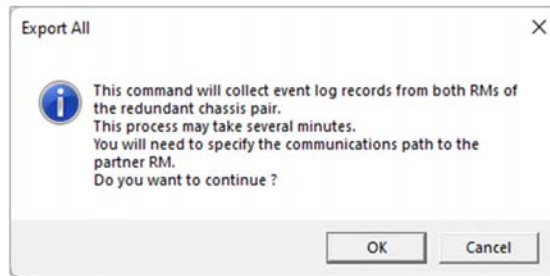
When you export Tech Support logs, the RMCT exports all log entries for both partner redundancy modules to a BIN file.

To export Tech Support logs, follow these steps.

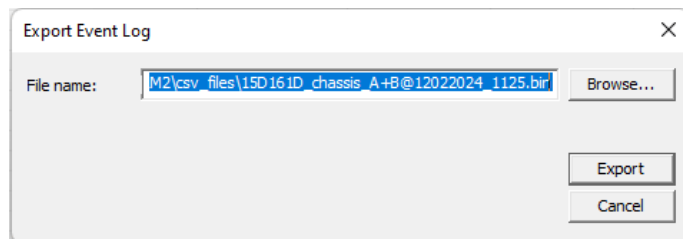
1. On the Event Log tab, select Export Tech Support Logs.



2. When the following message appears, select OK.



3. Browse to the directory in which to save the exported file and select Export.



Redundancy Module Faults

Redundancy module faults appear in the following locations:

- On the module status display. For fault messages that appear on the module status display, see [Table 63](#).
- In the Status area on the Module Info tab of the RMCT.

Figure 58 - Fault Log

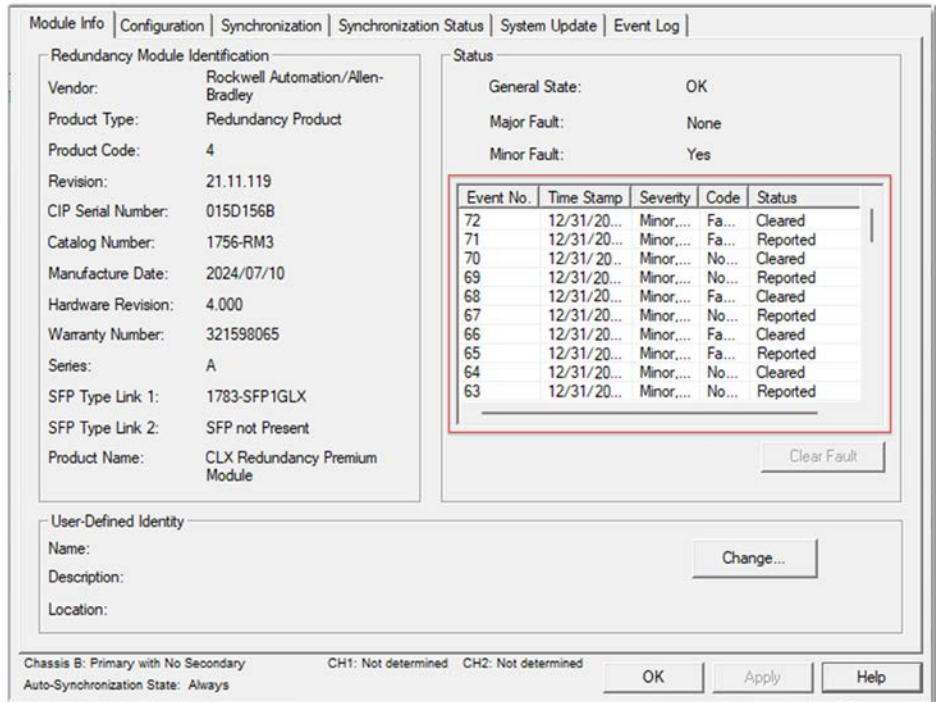


Table 51 - Fault Log Parameters

Parameter	Description
Event No.	A unique, sequential number to identify the fault.
Time Stamp	The date and time that the fault was logged.
Severity	One of the following fault severity types: <ul style="list-style-type: none"> • Minor recoverable—The fault does not stop redundancy operation and provides you with a recovery mechanism. • Minor nonrecoverable—The fault does not stop redundancy operation. No recovery mechanism is available. • Major recoverable—The fault impacts redundancy operations, although the effect is not always immediate. For example, if the fault occurred in the secondary redundancy module, the secondary chassis is disqualified and is not able to take control if the primary redundancy module fails. • Major nonrecoverable—The fault is critical and redundancy operations stop: <ul style="list-style-type: none"> - A switchover can occur. - No recovery mechanism is available. - The module can require replacement.
Code	The cause of the fault. Depending on the fault, the resolution may also be identified. Example causes of a fault include the following: <ul style="list-style-type: none"> • CPU temperature is too high • SD card failure • No SFP transceiver is installed on Link 1 or 2 • Module in chassis failed; replace module
Status	One of the following fault statuses: <ul style="list-style-type: none"> • Reported • Cleared

Clear a Fault

IMPORTANT Before you clear major faults, export the system history.

Faults can be cleared automatically or manually, depending on the severity:

- A major or minor recoverable fault is automatically cleared when the cause of the fault is resolved. If the fault is raised and immediately resolved by firmware, the fault persists for at least 1 minute.
- A major nonrecoverable fault is cleared manually by one of these methods:
 - Restart the module.
 - Remove and insert the module in the chassis while power is applied.
 - Select the Clear Fault button below the fault log in the RMCT. With this feature, you can remotely restart a redundancy module without physically removing and reinserting it in the chassis. The Clear Fault button is active only when the redundancy module is in a major fault state.

Figure 59 - Clear a Major Nonrecoverable Fault

The screenshot displays the 'Redundancy Module Identification' and 'Status' sections of the RMCT interface. The 'Redundancy Module Identification' section includes fields for Vendor (Rockwell Automation/Allen-Bradley), Product Type (Redundancy Product), Product Code (4), Revision (21.11.119), CIP Serial Number (015D156B), Catalog Number (1756-RM3), Manufacture Date (2024/07/10), Hardware Revision (4.000), Warranty Number (321598065), Series (A), SFP Type Link 1 (1783-SFP1GLX), SFP Type Link 2 (SFP not Present), and Product Name (CLX Redundancy Premium Module). The 'Status' section shows General State: OK, Major Fault: None, and Minor Fault: Yes. Below this is a table of event logs with columns for Event No., Time Stamp, Severity, Code, and Status. A 'Clear Fault' button is highlighted with a red box at the bottom right of the status section.

Event No.	Time Stamp	Severity	Code	Status
72	12/31/20...	Minor...	Fa...	Cleared
71	12/31/20...	Minor...	Fa...	Reported
70	12/31/20...	Minor...	No...	Cleared
69	12/31/20...	Minor...	No...	Reported
68	12/31/20...	Minor...	Fa...	Cleared
67	12/31/20...	Minor...	No...	Reported
66	12/31/20...	Minor...	Fa...	Cleared
65	12/31/20...	Minor...	Fa...	Reported
64	12/31/20...	Minor...	No...	Cleared
63	12/31/20...	Minor...	No...	Reported

Redundant Controller Major Fault Messages

The Major Fault TXX:CXX message on the controller scrolling display indicates major faults.



This manual links to Logix 5000 Controller and I/O Fault Codes and Syslog Messages, [1756-RD001](#); the file automatically downloads when you click the link.

Notes:

Troubleshoot Systems with 1756-RM2 Modules

When a fault or other event occurs on the redundancy system, use these methods to determine the cause:

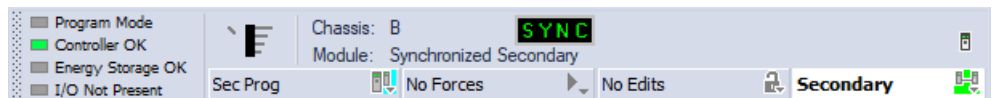
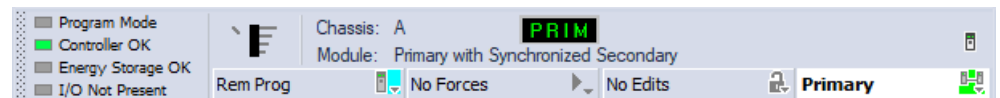
- View diagnostic information in the Logix Designer application.
- View synchronization, event, and fault information in the Redundancy Module Configuration tool (RMCT).
- Identify a lost partner network connection in the RMCT.
- Identify a lost redundancy module connection or missing redundancy module in the RMCT.
- Identify a non-redundant controller in the RMCT.
- Understand redundancy module and controller fault codes.
- Check the redundancy module status messages and status indicators. See [Appendix A](#).
- (ControlLogix® 5570 only). View ControlNet® network status with RSNetWorx™ for ControlNet software. See [Appendix G](#).

View Diagnostic Information in the Logix Designer Application

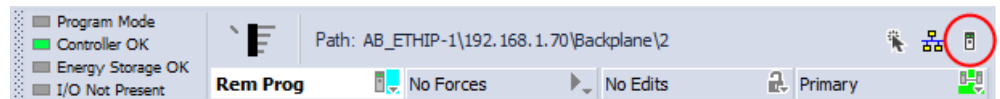
To view diagnostic information in the Logix Designer application, complete these steps.

1. Go online with the redundant controller.
2. Select Primary or Secondary, depending on which controller is online.

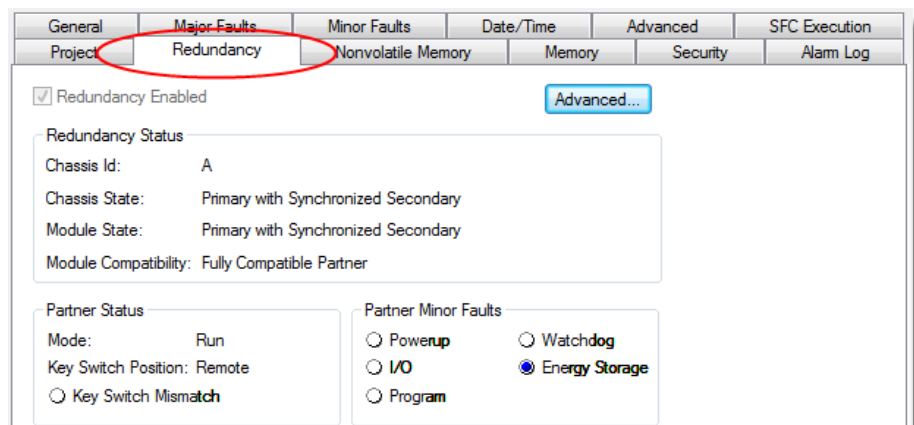
The redundant controller ID and status are displayed.



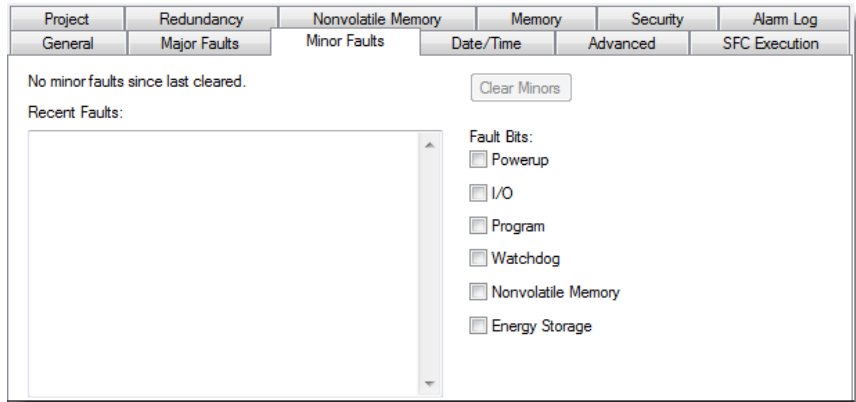
3. For more information, select the Controller Properties icon.



4. To view redundancy status, select the Redundancy tab.



- To view fault types and codes, select the Major Faults and Minor Faults tabs. The fault bits are status bits that the controller sets. You can set fault bits for testing, but that is not the main purpose of these bits.



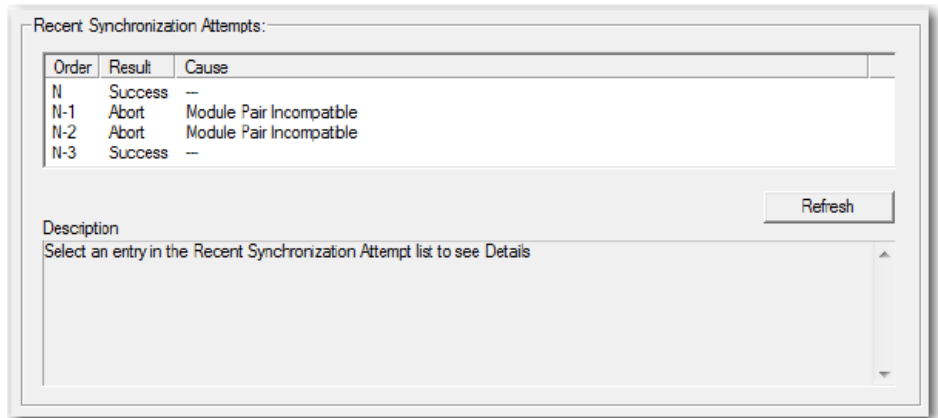
- If necessary, see these resources:
 - [Recovery Messages](#)
 - Major, Minor, and I/O Faults Programming Manual, publication [1756-PM014](#)

View Recent Synchronization Attempts

In the RMCT, the Synchronization tab provides a log of the last four synchronization attempts. If a synchronization command was unsuccessful, the Recent Synchronization Attempts log indicates a cause.

For more information about how to resolve the synchronization conflict, select the attempt and view the Description in the lower box.

Figure 60 - Example of an Unsuccessful Synchronization Attempt



You can view a log of the last four synchronization attempts in the log on the Synchronization tab. N or N-X identify synchronization attempts in the log. If the redundant chassis fail to synchronize, a cause is identified.

This table describes the possible result of synchronization attempts.

Table 52 - Results of Recent Synchronization Attempts

Result	Description
Undefined	The result of the synchronization is unknown.
No attempt since last powerup	Synchronization has not been attempted since power was applied to the module.
Success	Full synchronization was successfully completed.
Abort	The synchronization attempt failed. See Table 53 for further information.

If the result of a synchronization attempt is Abort, refer to the following table to diagnose the cause. For help with troubleshooting these causes, contact Rockwell Automation technical support.

Table 53 - Causes of Aborted Synchronization Attempts

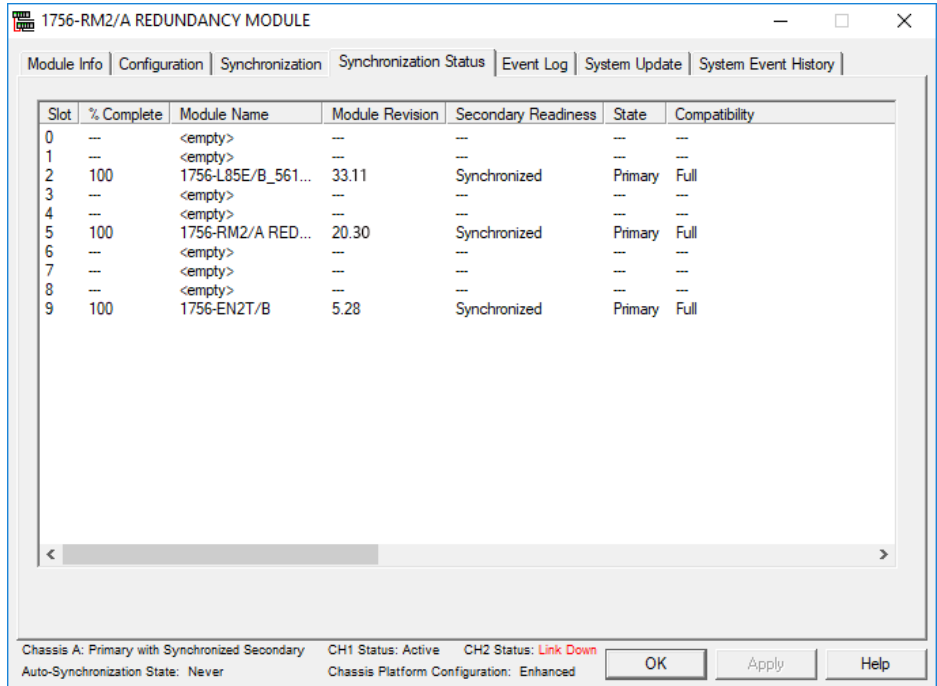
Cause	Description
Undefined	The cause of synchronization failure is unknown.
Module Pair Incompatible	Synchronization was aborted because one or more module pairs are incompatible.
Module Configuration Error	Synchronization was aborted because one of the modules is improperly configured.
Edit Session In Progress	Synchronization was aborted because an edit or session is in progress.
Crossloading Failure	An undetermined failure occurred during synchronization between redundancy modules.
Comm Disconnected	The cable between the redundancy modules was disconnected.
Module Insertion	Synchronization was aborted because a module was inserted into a chassis.
Module Removal	Synchronization was aborted because a module was removed from a chassis.
Secondary Module Failed	Synchronization was aborted because of a failure in the secondary module.
Incorrect Chassis State	Synchronization was aborted due to an incorrect chassis state.
Comm Does Not Exist	Synchronization could not be performed because the communication link between redundancy modules does not exist.
Non-redundant Compliant Module Exists	Synchronization could not be performed because one or more non-redundancy modules are present in one of the chassis.
Sec Failed Module Exists	A module in the secondary chassis has asserted the SYS_FAIL line, which indicates that it has faulted or failed.
Local Major Nonrecoverable Fault	Synchronization was aborted because of a local major non-recoverable fault.
Partner Has Major Fault	Synchronization was aborted because the partner module has a major fault.
Sec SYS_FAIL_L Subsystem Failed	The test of the SYS_FAIL line in the secondary chassis failed.
Sec RM Device Status = Comm Error	Synchronization was aborted because the status of the secondary redundancy module indicates a communication error.
Sec RM Device Status = Major Recoverable Fault	Synchronization was aborted because the status of the secondary redundancy module indicates a major recoverable fault.
Sec RM Device Status = Major Non-recoverable Fault	Synchronization was aborted because the status of the secondary redundancy module indicates a major nonrecoverable fault.
Incorrect Device State	Synchronization was aborted because the device is in the wrong state.
Primary Module Failed	Synchronization was aborted because of a failure in the primary module.
Primary Failed Module Exists	A module in the primary chassis has asserted the SYS_FAIL line, which indicates that it has faulted or failed.
Auto-Sync Option	Synchronization was aborted because the Auto-synchronization setting of one of the redundancy modules was changed during synchronization.
Module Qual Request	Synchronization was aborted because another synchronization request was received. The current synchronization has stopped so that the new synchronization request can be serviced.
SYS_FAIL_L Deasserted	Synchronization was aborted because one of the modules came out of a faulted or failed state.
Disqualify Command	Synchronization was aborted because the redundancy module received a disqualify command from another device. The originating device sends this command when it can no longer perform in the qualified state.
Disqualify Request	Synchronization was aborted because the redundancy module received a disqualify command from another device. The originating device sends this command when it can no longer perform in the qualified state.
Platform Configuration Identity Mismatch Detected	There are modules in the primary or secondary chassis that do not belong to the platform.
Application Requires Enhanced Platform	A redundant controller is running an application that contains a feature that is qualified to run only on an enhanced redundant platform, for example, Alarms.
ICPT Asserted	A test line on the backplane is asserted.
Unicast Not Supported	A unicast connection is configured in the redundant controller, and redundancy systems do not support unicast except for concurrent communication.
PTP Configuration Error	The PTP clock of a redundant controller is not synchronized or the partner controller pair is synchronized to another Grandmaster.
Secured Module Mismatch	A mismatch was detected between a primary and secondary secured module.

View Module-level Synchronization Status

On the Synchronization Status tab, you can view the following status information for each module in the chassis:

- Synchronization state, such as synchronized or disqualified
- Chassis designation, such as primary or secondary
- Module compatibility with its partner, such as full or undefined

Figure 61 - Synchronization Status Tab



You can use the module-level status information to identify which module pair is causing a synchronization failure. Depending on the type of synchronization failure, you must open the Synchronization Status tabs for the primary and secondary redundancy modules:

- If there is a difference between major revisions of the controllers or modules, the Compatibility column shows **Incompatible**.

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	0	1756-L85E	33.11	No Partner	Primary	Incompatible
1	0	1756-RM2/A REDUNDAN...	20.30	Disqualified	Primary	Full
2	0	1756-EN2TR/C 217021900	11.02	Disqualified	Primary	Full

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	0	1756-L85E	32.11	No Partner	Secondary	Incompatible
1	0	1756-RM2/A REDUNDAN...	20.30	Disqualified	Secondary	Full
2	0	1756-EN2TR/C 217021900	11.02	Disqualified	Secondary	Full

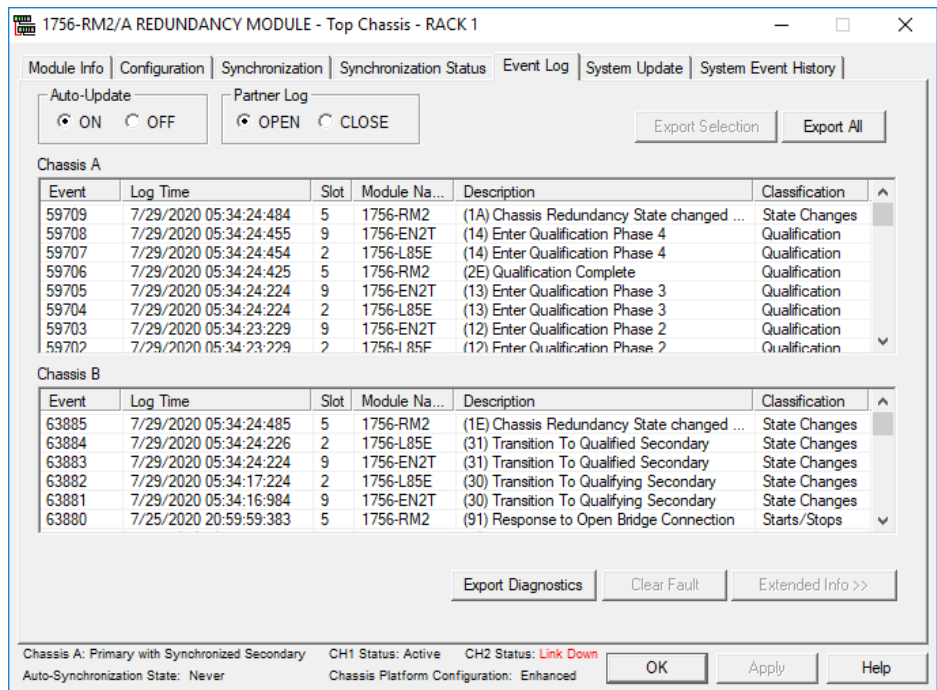
- If there is a difference between minor revisions of the controllers or modules, the Compatibility column also shows **Incompatible**.

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	0	1756-L85E	33.11	Disqualified	Primary	Full
1	0	1756-RM2/A REDUNDAN...	20.30	No Partner	Primary	Incompatible
2	0	1756-EN2TR/C 217021900	11.02	Disqualified	Primary	Full

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	0	1756-L85E	33.11	Disqualified	Secondary	Full
1	0	1756-RM2/A REDUNDAN...	20.5	No Partner	Secondary	Incompatible
2	0	1756-EN2TR/C 217021900	11.02	Disqualified	Secondary	Full

View the Event Log

To determine the cause of an event, error, switchover, or major fault, access the RMCT event log. Messages in the event log are for Rockwell Automation development engineering to debug redundancy system events after the fact. Anyone who is not part of the development engineering team can have difficulty interpreting the meaning of many of the events in the Event Log. For user-facing messages, see [View System Event History](#). These messages are designed for the user.



The Event Log tab provides a history of events that have occurred on the redundant chassis.

These system events are indicated in the event logs:

- Qualification stages that are entered and completed
- Module insertion/removal
- Firmware errors
- Communication events and errors
- Configuration changes
- Other system events that affect qualification and synchronization

The events that are logged in this tab are not always indicative of an error. Many of the events that are logged are informational only. To determine if additional action or troubleshooting is required in response to an event, see [Table 55](#).

You can set parameters on the Event Log tab to view the log for one chassis or the event logs of both chassis.

Figure 62 - Event Log Tab

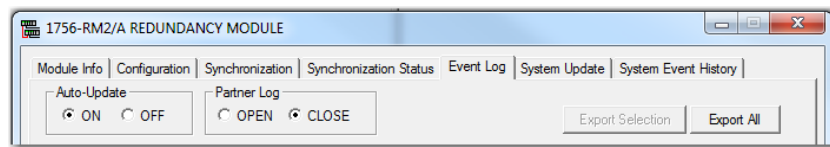


Table 54 - Event Log Parameters

Parameter	Description
Auto-Update	Select ON to keep the log updating automatically.
Partner Log	Select CLOSE to view only the log of one redundancy module.

Controller Events

Occasionally, controller-related events can be logged in the RMCT event log. In some cases, the events are status updates rather than an anomaly that requires troubleshooting.

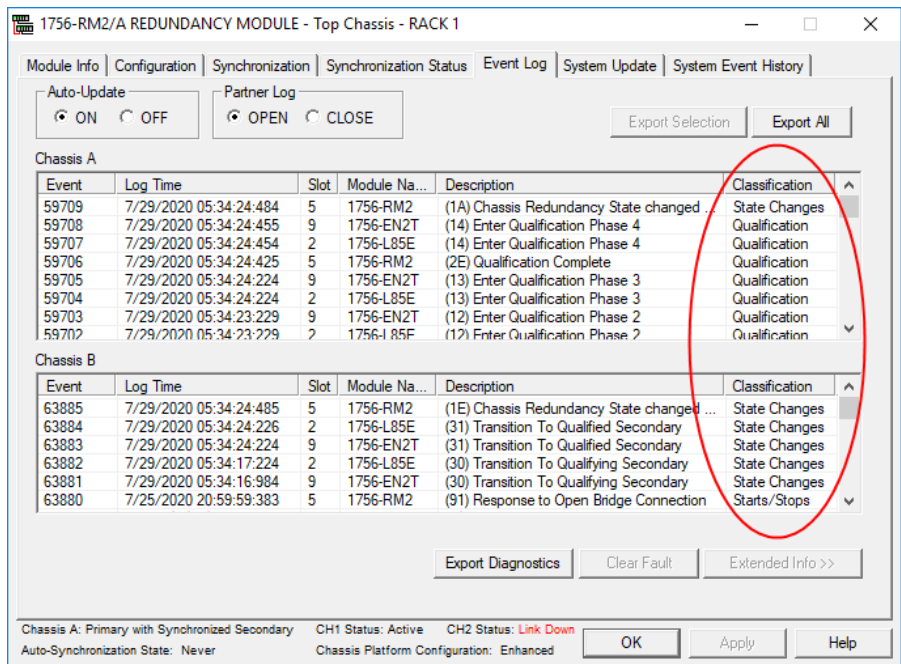
In other cases, the event description can indicate Program Fault Cleared or a similar description of a resolved anomaly. If state changes or switchovers do not follow these types of events, then they are not indicative of an anomaly that requires troubleshooting.

If a state change or switchover follows an event that is logged for a controller in the redundant system, use the Logix Designer application to go online with the controller and determine the cause of the fault. For more information about how to use the Logix Designer application to troubleshoot a fault, see [View Diagnostic Information in the Logix Designer Application](#).

Event Classifications

Each event that is identified and logged is classified. You can use these classifications to identify the severity of the event and determine if additional action is required.

Figure 63 - Event Classifications



Use the following table to determine what an event classification indicates and if corrective action is required.

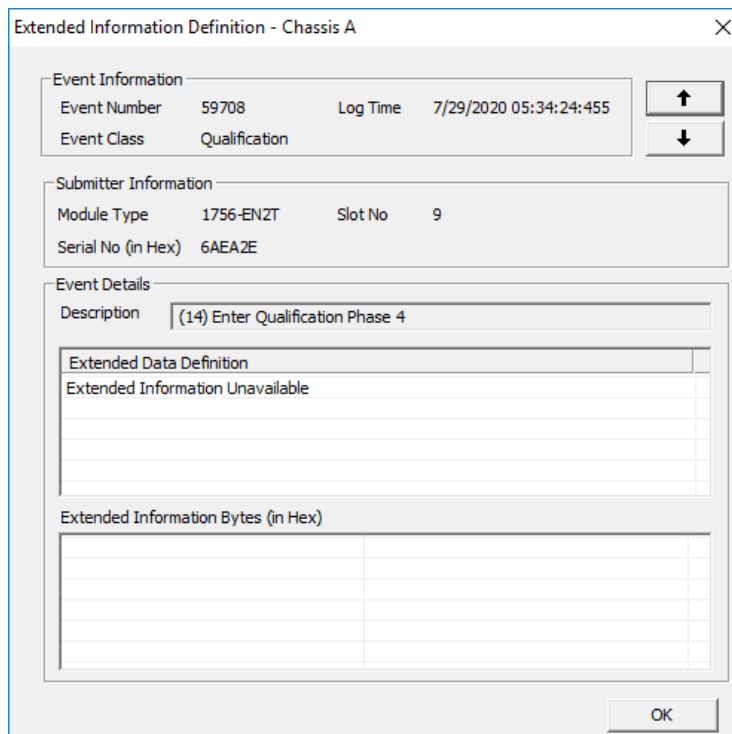
Table 55 - Classification Types

Classification Type	Description	Action Required
Configuration	A redundancy module configuration parameter has been changed. For example, if you change the Auto-synchronization parameter from Always to Never, an event that is classified as Configuration is logged.	No corrective action is required. This event is provided for informational purposes and does not indicate a serious anomaly with the redundancy system.
Command	An event that is related to commands that are issued to the redundant system has occurred. For example, if you change the Redundancy Module Date and Time parameters, a WCT time change event of the Command classification is logged.	No corrective action is required. This event is provided for informational purposes and does not indicate a serious anomaly with the redundancy system.
Failure	A failure on the redundancy module has occurred. For example, an internal Firmware error event that is classified as a Failure can be indicated in the event log.	Action can be required to determine the cause of the failure. If a Switchover or Major Fault event does not precede a failure, then the module could have corrected the error internally and additional action is not required. To determine if corrective action is required, double-click the event to see Extended Event Information and the suggested recovery method, if applicable.
Major Fault	A major fault has occurred on a redundancy module.	Action can be required to determine the action that is necessary to correct the fault. Double-click the event to see Extended Event Information and the suggested recovery method, if applicable.
Minor Fault	A minor fault has occurred on a redundancy module.	No corrective action is required. This event is provided for informational purposes and does not indicate a serious anomaly with the redundancy system.
Starts/Stops	Various internal chassis and module processes have started or stopped.	No corrective action is required. However, if an event that is classified as a Failure, State Change, or Major Fault occurs after the Starts/Stops event, view the Extended Event Information of both events to determine if the events are related.
State Changes	A chassis or module state change has occurred. For example, if the chassis designation changes from being a disqualified secondary to a qualified secondary, a State Change event is logged.	No corrective action is required. However, if an event that is classified as a Failure, or Major Fault occurs after the State Changes event, view the Extended Event Information of both events to determine if the events are related.
Switchover	An event that is related to a chassis switchover has occurred. For example, if an Initiate Switchover command is issued, an event that is classified as Switchover is logged.	Action can be required to determine the cause of the switchover and potential correction methods. Double-click the event to see Extended Event Information and the suggested recovery method, if applicable.
Synchronization	An event that is related to chassis synchronization has occurred. For example, if the Synchronization command has been issued, a Network Transitioned to Attached event is logged and classified as Synchronization.	No corrective action is required. This event is provided for informational purposes and does not indicate a serious anomaly with the redundancy system.

Access Extended Information about an Event

Events that are logged on the Event Log tab can have more information available. To access more information about an event, double-click an event in the log.

Figure 64 - Extended Information Definition Dialog Box



Interpret Extended Information for an Event

The information that is listed in this table can be provided (depending on the type of event) after you have accessed the Extended Information Definition dialog box.

Information Type	Description
Event Information	The redundancy system assigns this event information: <ul style="list-style-type: none"> • Event number • Date and time the event occurred • Event classification
Submitter Information	This information reflects information for the module that reported the event. Information that is provided in this section includes the: <ul style="list-style-type: none"> • Name of the module that originated the event • Slot number of the module that originated the event • Serial number of the module that originated the event
Event Details	This section provides these additional details about the event: <ul style="list-style-type: none"> • Description of the event • Examine the Extended Data Definition, which provides an explanation of the event and bytes, for errors • Extended Data Bytes in hexadecimal that provides further details of the event

Interpret Event Log Information

Table 56 - Qualification Codes

Status Code	Description
PwQS	Primary with qualified (synchronized) secondary partner
PwQgS	Primary with qualifying secondary
QSwP	Qualified (synchronized) secondary with primary partner
DSwP	Disqualified secondary with primary partner
DSwNP	Disqualified secondary with no partner
PLgU	Primary locking for update
PLU	Primary locked for update
PwDS	Primary with disqualified secondary partner
PwNS	Primary with no secondary partner
SLgU	Secondary locking for update
SLU	Secondary locked for update

To view and interpret Event Log information, follow these steps.

1. Open the RMCT and select the Event Log tab.
2. If an event occurred, open the event log for both chassis A and B.
3. In the event log for chassis A, locate the event line that shows the qualification code, start date, and time of the event.

This entry is the last time that the redundancy module was working properly.

For information about qualification codes, see [Table 56](#).

Event	Log Time	Slot	Module Na...	Description	Classifi
27026	12/17/2019 10:56:03:530	1	1756-RM2	(1A) Chassis Redundancy State changed to PwQS	State C
27025	12/17/2019 10:56:03:400	2	1756-EN2TR	(14) Enter Qualification Phase 4	Qualific
27024	12/17/2019 10:56:03:400	3	1756-EN2TR	(21) Equally Able To Control	State C
27023	12/17/2019 10:56:03:399	3	1756-EN2TR	(14) Enter Qualification Phase 4	Qualific
27022	12/17/2019 10:56:03:377	1	1756-RM2	(2E) Qualification Complete	Qualific
27021	12/17/2019 10:56:03:375	3	1756-EN2TR	(13) Enter Qualification Phase 3	Qualific

4. In the event log for chassis B, locate the matching time entry. This entry displays the disqualification code on the Event line.

Event	Log Time	Slot	Module Na...	Description	Classific
11811	12/17/2019 10:56:03:530	1	1756-RM2	(1E) Chassis Redundancy State changed to QSwP	State C
11810	12/17/2019 10:56:03:375	3	1756-EN2TR	(31) Transition To Qualified Secondary	State C
11809	12/17/2019 10:56:03:374	2	1756-EN2TR	(31) Transition To Qualified Secondary	State C
11808	12/17/2019 10:56:01:350	3	1756-EN2TR	(30) Transition To Qualifying Secondary	State C
11807	12/17/2019 10:56:01:350	2	1756-EN2TR	(30) Transition To Qualifying Secondary	State C

5. In the list of preceding events, locate the point that a switchover or disqualifying event occurred.

In the event log for chassis A, the event line shows the end date and time of the event.

Event	Log Time	Slot	Module Na...	Description	Classifi
26984	12/17/2019 10:55:37:657	1	1756-RM2	(C) Port2 Communication error	Minor
26983	12/17/2019 10:55:35:616	1	1756-RM2	(19) Chassis Redundancy State changed to PwDS	State C
26982	12/17/2019 10:55:35:530	3	1756-EN2TR	(1) Network Transition to Not Attached	Synchi
26981	12/17/2019 10:55:35:496	1	1756-RM2	(31) Switchover Complete	Switch
26980	12/17/2019 10:55:35:495	3	1756-EN2TR	(2) Network Not Attached Warning	Synchi

In the event log for chassis B, there is a disqualification code that the secondary has been disqualified. For information about qualification codes, see [Table 56](#).

Event	Log Time	Slot	Module Na...	Description	Classific
11787	12/17/2019 10:55:37:795	1	1756-RM2	(C) Port2 Communication error	Minor Fe
11786	12/17/2019 10:55:35:616	1	1756-RM2	(1D) Chassis Redundancy State changed to DSwP	State Ch
11785	12/17/2019 10:55:35:614	1	1756-RM2	(31) Switchover Complete	Switcho
11784	12/17/2019 10:55:35:593	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/S
11783	12/17/2019 10:55:35:593	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/S

- To find the error that caused the disqualification, examine the range of time in between the start of the event and the end of the event.

This range of time can be large depending on how much time has passed since the last disqualifying event.

Event	Log Time	Slot	Module Na...	Description	Classific
11846	12/17/2019 11:13:21:002	1	1756-RM2	(90) Request to Open Bridge Connection	Starts/S
11845	12/17/2019 11:13:01:370	1	1756-RM2	(4D) WCT time change (> 1 second)	Commarr
11844	12/17/2019 11:12:17:274	1	1756-RM2	(1D) Chassis Redundancy State changed to DSwP	State Ch
11843	12/17/2019 11:12:17:274	1	1756-RM2	(BC) Chassis Platform Identity Updated	Configur
11819	12/17/2019 10:39:31:893	1	1756-RM2	(7) Firmware error	Minor Fe
11818	12/17/2019 10:39:11:387	1	1756-RM2	(7) Firmware error	Minor Fe
11817	12/17/2019 10:39:10:888	1	1756-RM2	(7) Firmware error	Minor Fe
11816	12/17/2019 10:39:08:388	1	1756-RM2	(FF) Firmware Diagnostic Entry	Minor Fe
11815	12/17/2019 10:39:08:388	1	1756-RM2	(FF) Firmware Diagnostic Entry	Minor Fe
11814	12/17/2019 10:38:37:291	1	1756-RM2	(D2) CH2 Link Up	Minor Fe
11813	12/17/2019 10:38:37:195	1	1756-RM2	(C) Port2 Communication error	Minor Fe
11812	12/17/2019 10:38:37:195	1	1756-RM2	(C) Port2 Communication error	Minor Fe
11811	12/17/2019 10:56:03:530	1	1756-RM2	(1E) Chassis Redundancy State changed to QSwP	State Ch

Event	Log Time	Slot	Module Na...	Description	Classifica
11967	12/17/2019 13:48:00:839	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11966	12/17/2019 13:48:00:819	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11965	12/17/2019 13:48:00:804	1	1756-RM2	(1D) Chassis Redundancy State changed to DSwP	State Chi
11964	12/17/2019 13:48:00:799	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11963	12/17/2019 13:48:00:783	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11962	12/17/2019 13:48:00:781	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11961	12/17/2019 13:48:00:780	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11960	12/17/2019 13:48:00:780	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Sh
11959	12/17/2019 13:48:00:779	3	1756-EN2TR	(F) Partner Connection Closed	Synchron
11958	12/17/2019 13:48:00:779	2	1756-EN2TR	(F) Partner Connection Closed	Synchron
11957	12/17/2019 13:48:00:778	1	1756-RM2	(45) SYS_FAIL_L Active	Failure
11956	12/17/2019 13:48:00:777	2	1756-EN2TR	(1) Network Transition to Not Attached	Synchron
11955	12/17/2019 11:44:12:697	1	1756-RM2	(1E) Chassis Redundancy State changed to QSwP	State Chi

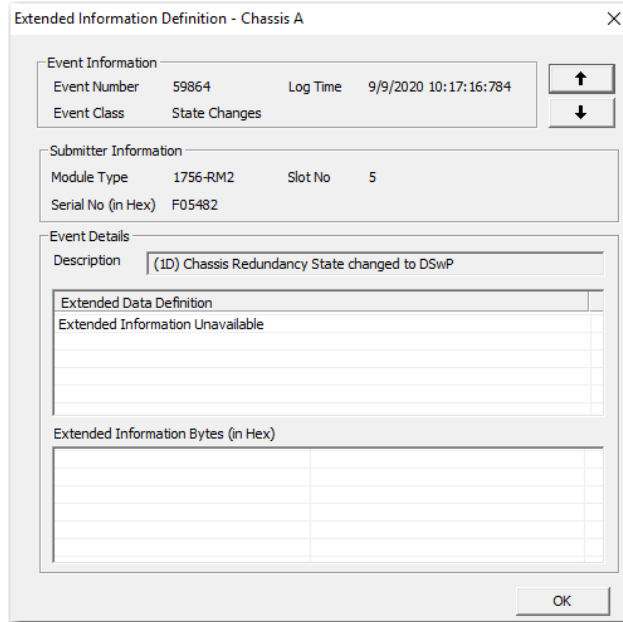


To identify a significant event, you can also do the following:

- In the Log Time column, scan within a time range that corresponds to the time an event was reported or annunciated.
- Identify differences between times logged. Gaps in time often identify events that require troubleshooting. Gaps in months, days, or minutes can indicate a significant change to the system.

Not all events that are logged are indicative of an anomaly that must be corrected. For example, events that are classified as Minor Faults do not warrant corrective behavior unless they occur just before a switchover, major fault, or state change **and** can be identified as contributing to successive events.

7. After you locate an event entry that is related to the anomaly you are troubleshooting, double-click the event to open the Extended Event Information dialog box. If no recovery method is described, action is not required in response to the event.



8. View the description and extended data definitions to obtain further event information and a possible recovery method.

Export Event Log Data

After you view extended information about an event, you can export event data by using either of these options:

- **Export Selection**—Exports event log data for single or multiple events that occur on a primary or secondary redundancy module.
- **Export All**—Exports all event log data for events in both of the redundancy modules in the redundant chassis pair. We recommend that you use this feature when troubleshooting system-related anomalies where the location of a fault could have occurred a lengthy period before the current event.

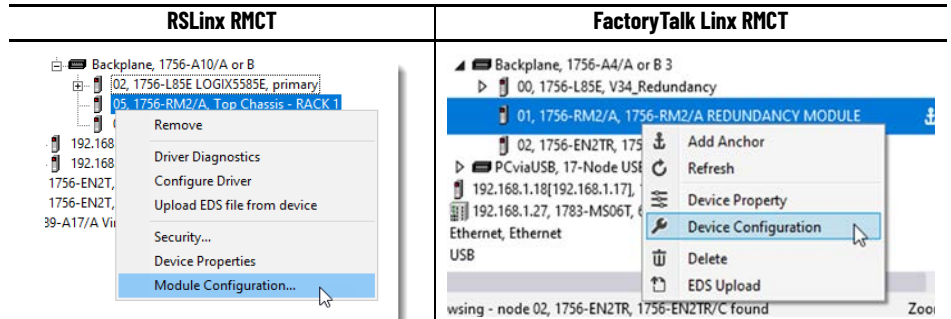
IMPORTANT To export event data so that Rockwell Automation Technical Support can troubleshoot an anomaly, you must obtain the event logs for the primary and secondary redundancy modules. We recommend that you get the logs by choosing Export All with the CSV file type.

If you cannot access the event log for the secondary redundancy module, export it from the partner event log via the primary redundancy module.

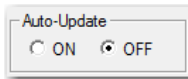
Keep in mind that the view the primary redundancy module has of the event log of the secondary redundancy module is typically limited. To troubleshoot an anomaly with Rockwell Automation Technical Support, you must obtain the event log of the secondary redundancy module from the view of the module itself.

To export event data, complete these steps.

1. Launch the communication software and browse to the redundancy modules.
If the redundancy modules are not available in the communication software after a fault, apply the recovery method that the module indicates before you export the data.
2. Right-click the **primary** redundancy module and choose the Configuration option.
If you cannot see the Configuration option in the list, then the compatible version of the RMCT is not installed.

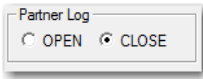


3. In the Auto-Update area, select Off to keep the log from updating.



4. In the Partner Log area, select Close.

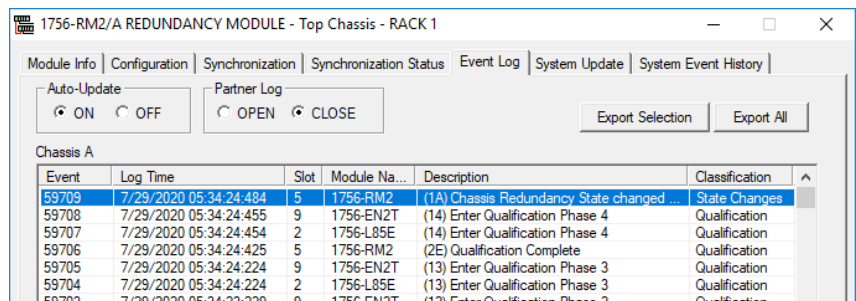
This action closes the event log of the partner module.



5. To export one or a few events, select the events, and then select Export Selection.
or

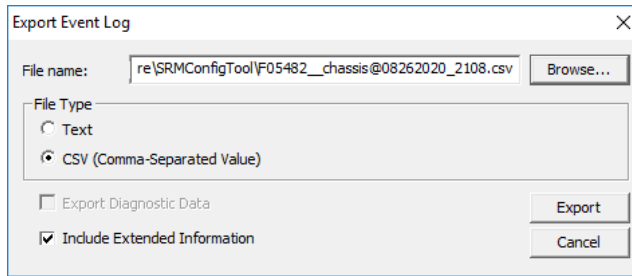
To export all events, select Export All and then do the following:

- a. On the Export All dialog box, select OK.
- b. On the communication software dialog box, select the partner redundancy module and select OK.

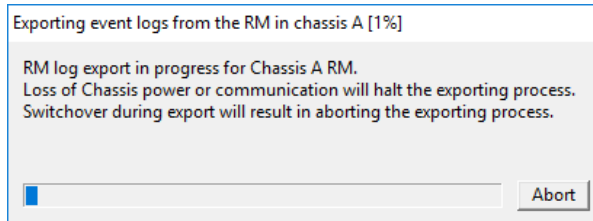


6. On the Export Event Log dialog box, specify the following:
 - Enter a file name and location or use the default name and location.
 - Select CSV (Comma-Separated Value).
 - Select Include Extended Information.

7. Select Export.



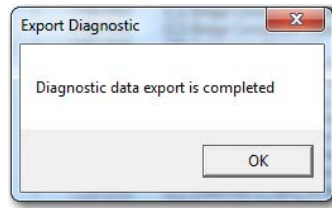
The log can take a few minutes to export.



8. If you exported data from a selection of events and want to export the secondary redundancy module log for a complete system view, repeat this procedure for the secondary module.

or

If you exported all event data, wait for the following dialog box to appear, and then select OK. A .csv and a .dbg file are in the folder location specified. Provide the .csv file to Rockwell Automation Technical Support.



Export Diagnostics

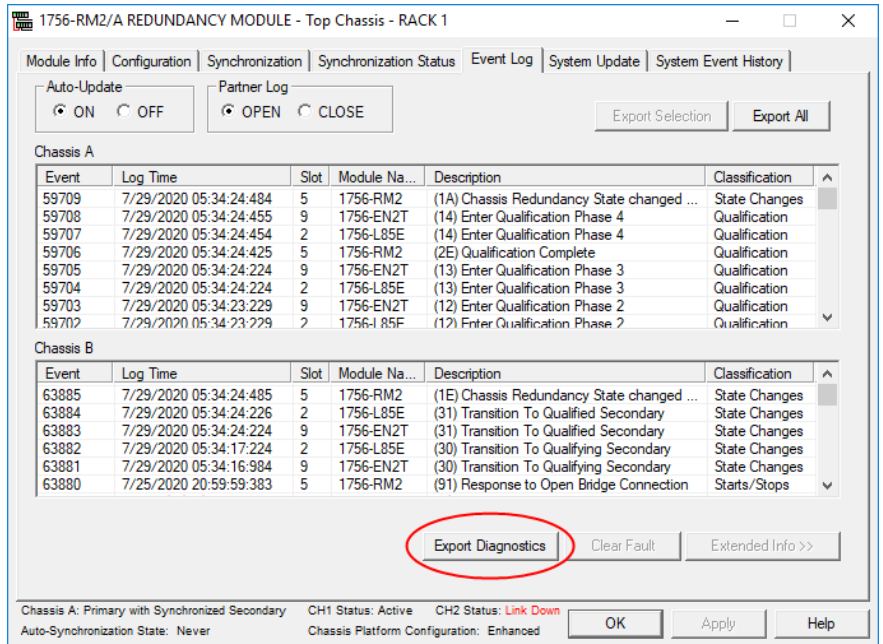
IMPORTANT Only export diagnostics when requested to do so by Rockwell Automation Technical Support.

If a nonrecoverable firmware fault occurs, select Export Diagnostics to collect and save diagnostic data from the redundancy module and its partner. A red 'OK' light on the front of the redundancy module indicates a nonrecoverable fault, and a fault message scrolls across the status display. When you select Export Diagnostics, information is recorded that Rockwell Automation engineering can use to determine the cause of the fault.

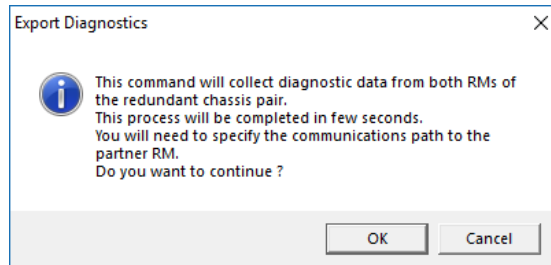
Because diagnostic information is recorded for the redundancy module and its redundancy partner, a communication path to the partner redundancy module is also part of the process to obtain the diagnostics.

To export diagnostics, complete these steps.

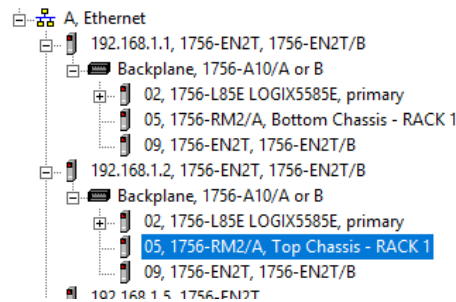
1. Select Clear Fault to clear any faults.
2. Select Export Diagnostics.



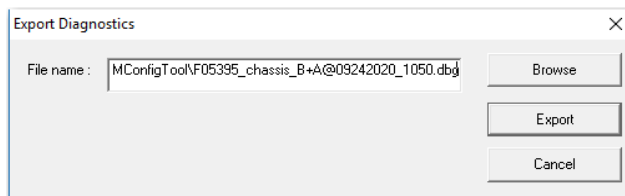
When the Export Diagnostics dialog box appears, select OK to continue.



3. Select the communication path to the partner or secondary module and select OK.



4. On the Export Diagnostics dialog box, enter a name and location to save the export file.



5. Select Export.

It can take several minutes to export the data. The Export Diagnostic Complete dialog box appears once the export has completed.

Contact Rockwell Automation Technical Support

If you cannot successfully troubleshoot your system with the event logs, prepare to contact Rockwell Automation Technical Support by exporting the event logs of the primary and secondary redundancy modules. The technical support representative who assists you uses those files to help determine the cause of a switchover or other anomaly.

For more information about how to export the event logs, see [Export Event Log Data](#).

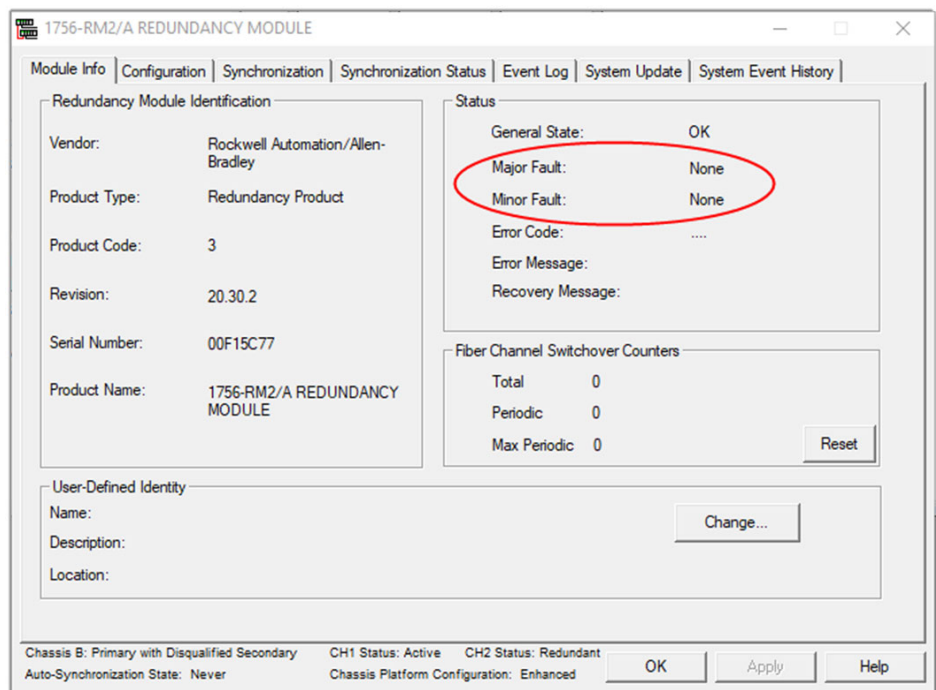
Clear a Fault

IMPORTANT Before you clear major faults from the module, export all event and diagnostic data. The Clear Fault button is active only when the redundancy module is in a major fault state.

You can use the Clear Fault button on the Event Log tab to clear major faults that occur on a redundancy module. With this feature, you can remotely restart the redundancy module without physically removing and reinserting it from the chassis. The module restart clears the fault.

Module faults appear on the Module Info tab.

Figure 65 - Faults on Module Info Tab



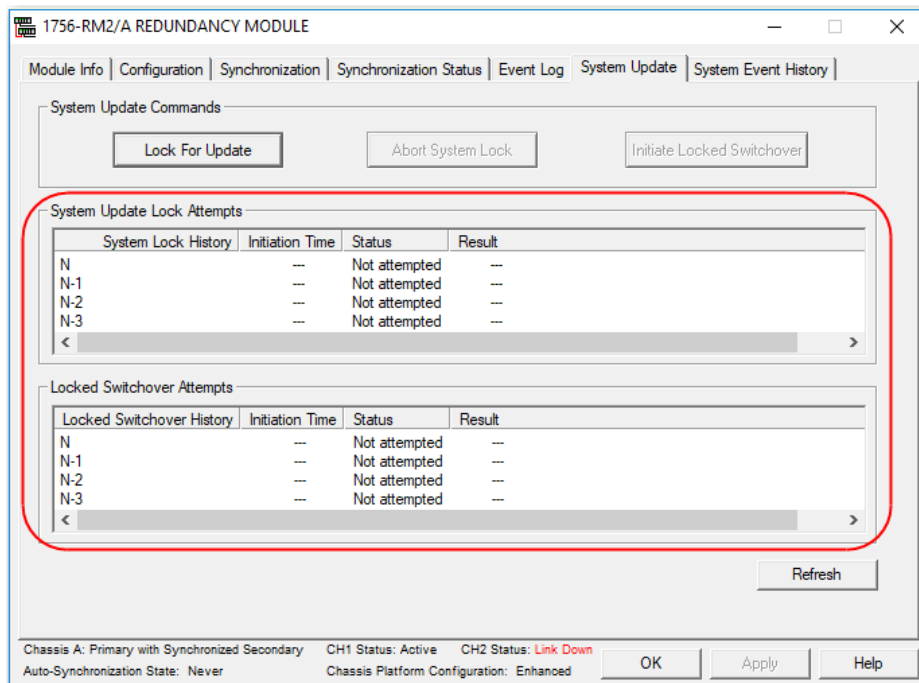
View System Update Logs

The System Update tab of the RMCT shows logs for the following:

- System update lock attempts
- Locked switchover attempts

You can access these logs in the RMCT for both partner redundancy modules.

Figure 66 - System Update Logs



System Update Lock Attempts

Attempts to lock the system for an update appear in the System Update Lock Attempts log. This log displays information about the last four lock attempts:

- Time and date
- Status
- Result

See the following table for status definitions.

Table 57 - System Update Lock Attempts

Status	Description
Not Attempted	A system lock has not been attempted since the last powerup.
In Progress	A lock is in progress.
Locked	The lock was successfully completed.
Abort	The lock attempt failed. The reason for the failure is indicated in the Result field.

If the status is Abort, one of these conditions can exist:

- An error occurred while communicating with the partner redundancy module.
- A module in the secondary chassis does not have a partner in the primary chassis.
- A module pair is incompatible.
- The SysFail test was unsuccessful in the primary redundancy module.
- A major recoverable fault occurred in the primary redundancy module.
- A major nonrecoverable fault occurred in the primary redundancy module.
- A module was inserted into the chassis.
- A module was removed from the chassis.

- A failed module exists in the secondary chassis.
- A failed module exists in the primary chassis.
- An Abort System Update command was received.
- An invalid response was received from a module.
- A module rejected the state change.
- A platform mismatch was detected.
- For more information on Lock for Update failures, see Knowledgebase Technote [Lock for Update Fails](#).

Locked Switchover Attempts

The Locked Switchover Attempts log provides information about the last four locked switchover attempts:

- Time and date
- Status
- Result

See the following table for status definitions.

Table 58 - Locked Switchover Attempts

Status	Description
Not Attempted	A locked switchover has not been attempted since the last powerup.
In Progress	A locked switchover is in progress.
Success	A locked switchover was successfully completed.
Abort	The locked switchover attempt failed. The cause of the failure is indicated in the Result field.

If the status is Abort, one of these conditions can exist:

- A module declined a locked switchover readiness request.
- An invalid response was received from the locked switchover readiness request.
- After an initiate switchover prompt, a module rejected the command.
- After an initiate switchover prompt, a module replied with an invalid response.

View System Event History

The System Event History tab shows the last 20 events. There are 10 events from each redundancy module. The type of events are described in the following table.

Table 59 - Event Types

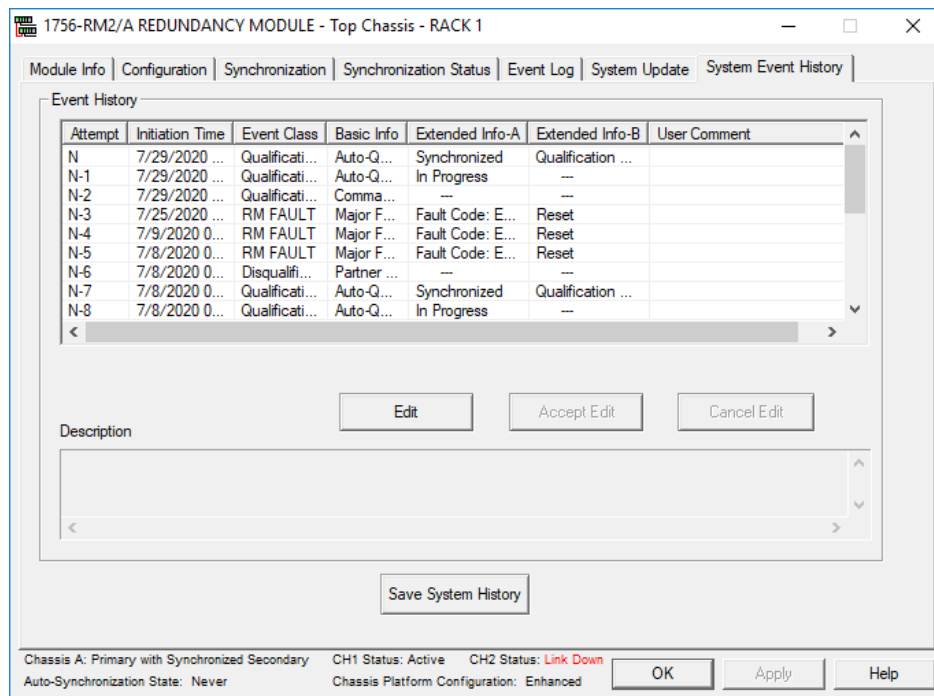
Event Type	Description
Qualification	The redundancy system can now complete a switchover to the secondary redundancy chassis.
Disqualification	The secondary redundancy chassis is not ready to accept control of the system. The redundancy system cannot complete a switchover.
Switchovers	The secondary chassis has now become the primary chassis and is now controlling the system.
Faults	A module has faulted in the redundancy system.

For each event logged, the Event History table shows the following information.

Figure 67 - Event Descriptions

Column	Description
Attempt	Event count from N to N-19 for a maximum of 20 events.
Initiation Time	The time and date of the event from the redundancy module clock.
Event Class	Qualification, Disqualification, or RM FAULT (Redundancy Module fault)
Basic Info	Information about the origin of the event (for example, Commanded or Auto Qualification).
Extended Info-A	A short text description of the event.
Extended Info-B	Additional details on the event.
User Comment	An editable user comment for the event.

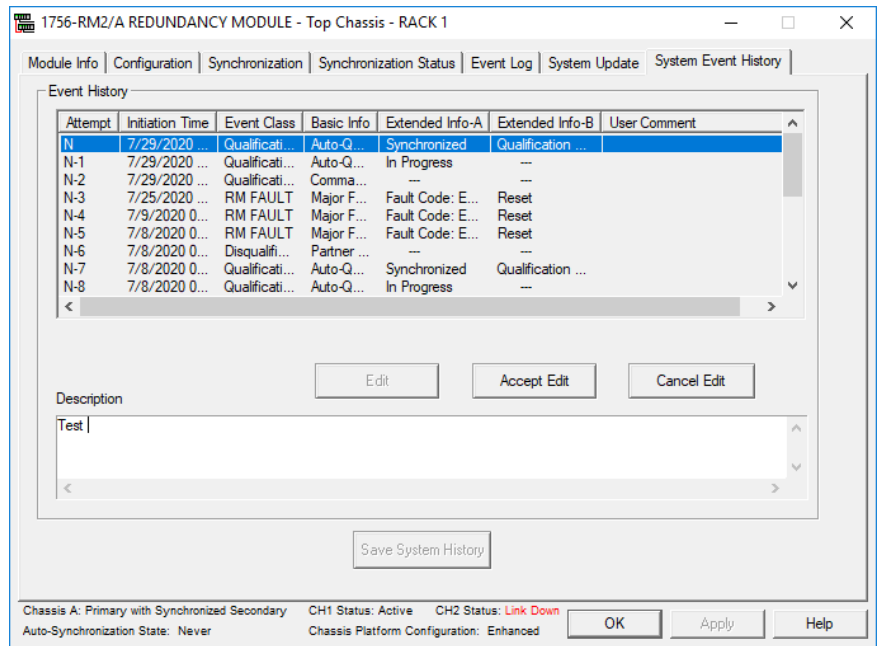
Figure 68 - System Event History



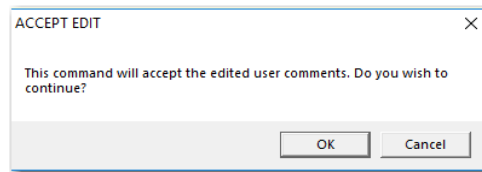
Edit a User Comment for a System Event

To edit the User Comment that is associated with a system event, complete these steps.

1. Select the event.
2. Select Edit.
3. In the Description field, type your event description.



4. Select Accept Edit.
5. On the Accept Edit dialog box, select OK.



Save System Event History

To save the system event log to the nonvolatile memory of the redundancy module, select Save System History at the bottom of the System Event tab. Saved event history can assist with troubleshooting the system later.

Event Examples

This section contains example event history records for typical system events.

Manual Switchover

Event Class	Basic Info	Extended Info-A	Extended Info-B
Switchover	Commanded	–	–

Disqualify Secondary

Event Class	Basic Info	Extended Info-A	Extended Info-B
Disqualification	Commanded	–	–

Qualification Successful

Event Class	Basic Info	Extended Info-A	Extended Info-B
Qualification	Auto-Qualification	Synchronized	Qualification Complete
Qualification	Auto-Qualification	In Progress	–

Qualification Failed Due to Incompatible Module

Event Class	Basic Info	Extended Info-A	Extended Info-B
Qualification	Auto-Qualification	In Progress	–
Qualification	–	Qual Abort	Cause: module pairs are incompatible

Switchover Due to Module Removal from Primary

Event Class	Basic Info	Extended Info-A	Extended Info-B
Disqualification	Module Fault	Chassis B	SYS_FAIL_L Asserted in Secondary Chassis
Switchover	Module Removal	Chassis B - Slot No:	–

Switchover Due to Network Cable Removal in Primary

Event Class	Basic Info	Extended Info-A	Extended Info-B
Switchover	Module Fault	Chassis B - Slot No:	Possible Causes: 1. Network cable removal 2. Controller program fault

Switchover Due to Chassis Power Fault in Primary Chassis

Event Class	Basic Info	Extended Info-A	Extended Info-B
Switchover	Partner RM Power Failure	–	–

Disqualification Due to Network Connection Lost between Primary and Secondary Chassis

Event Class	Basic Info	Extended Info-A	Extended Info-B
Switchover	Module Fault	Chassis B - Slot No:	Possible Causes: 1. Network Cable Removal ⁽¹⁾ 2. Controller Program Fault

(1) This lost connection is not a network cable removal issue. The communication modules not being able to see each other over the network has caused the lost connection.

Disqualification Due to Partner Chassis Power Fault

Event Class	Basic Info	Extended Info-A	Extended Info-B
Disqualification	Partner RM Power Failure	–	–

Disqualification Due to Partner Chassis Module Removal

Event Class	Basic Info	Extended Info-A	Extended Info-B
Disqualification	Module Removal	Chassis A - Slot No:	–

Disqualification Due to Partner Chassis Redundancy Module Fault

Event Class	Basic Info	Extended Info-A	Extended Info-B
RM FAULT	Major Fault	Fault Code: EE05	Reset
Disqualification	Partner RM Power Failure	–	–

Disqualification Due to Redundancy Module Fiber Cable Disconnected or Faulted

Event Class	Basic Info	Extended Info-A	Extended Info-B
Disqualification	RM Fiber Cable Disconnect	–	–

Identify a Lost Partner Network Connection

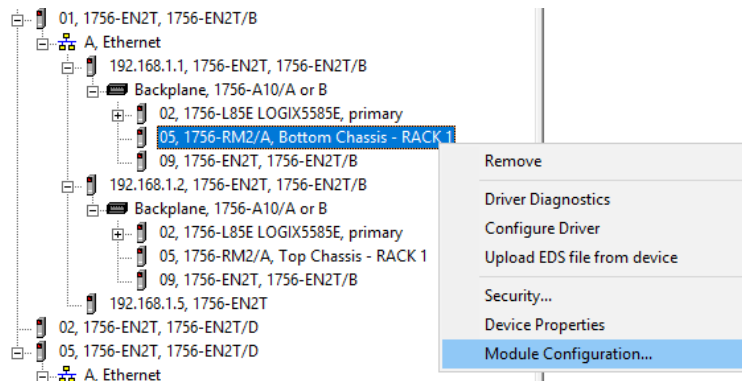
If a partner network connection between a redundant chassis pair is lost, a state change or switchover can occur. State changes include the following:

- Primary with qualified secondary > Primary with disqualified secondary
- Qualified secondary with primary > Disqualified secondary with primary

To use the event log to determine if a lost partner network connection caused a state change, complete these steps.

1. Open the communication software and access the RMCT of the primary redundancy module.

This chassis is the chassis that was previously the secondary but is now the primary.



2. Locate the last event that indicates successful qualification and status.

Event	Log Time	Slot	Module Na...	Description	Classification
23357	12/17/2019 04:37:22:407	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Stops
23356	12/17/2019 04:37:22:407	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Stops
23355	12/17/2019 04:37:22:407	1	1756-RM2	(C2) Bridge Connection Deleted	Starts/Stops
23354	12/17/2019 04:37:22:403	1	1756-RM2	(BD) SYS_FAIL_L Active in Partner RM	Failure
A 23353	12/17/2019 04:37:22:402	1	1756-RM2	(30) Switchover Attempted	Switchover
B 23352	12/17/2019 04:35:59:220	1	1756-RM2	(1E) Chassis Redundancy State changed ...	State Changes

Item	Description
A	A switchover is initiated.
B	The event indicates that the chassis state changed to qualified secondary.

3. Open the event log for the secondary chassis because the cause of the switchover is not apparent.
4. Use the time of the switchover event that is found in the primary chassis to identify the corresponding event in the secondary chassis.

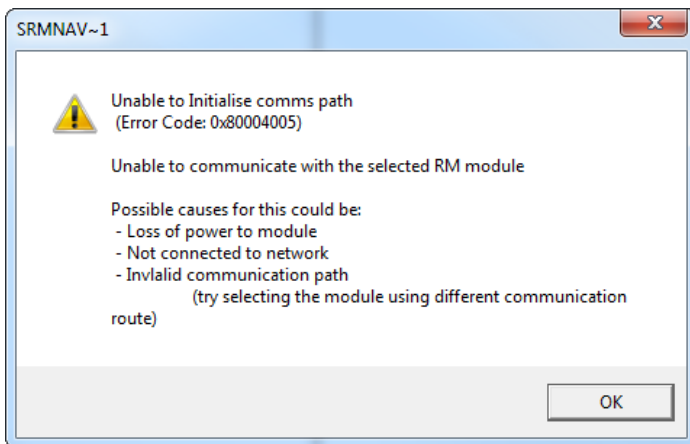
The switchover indicated in the primary chassis log occurred at 04:37:22.

Chassis B					
Event	Log Time	Slot	Module Na...	Description	Classification
9326	12/17/2019 04:37:22:515	1	1756-RM2	(46) SYS_FAIL_L Inactive	Failure
9325	12/17/2019 04:37:22:404	3	1756-EN2TR	(1) Network Transition to Not Attached	Synchronizati...
9324	12/17/2019 04:37:22:402	1	1756-RM2	(45) SYS_FAIL_L Active	Failure
9323	12/17/2019 04:37:22:401	1	1756-RM2	(30) Switchover Attempted	Switchover
9322	12/17/2019 04:37:22:401	2	1756-EN2TR	(1) Network Transition to Not Attached	Synchronizati...
9321	12/17/2019 04:35:59:219	1	1756-RM2	(1A) Chassis Redundancy State changed ...	State Changes

The corresponding events in the secondary chassis log indicate that the network is not attached and that the SYS_FAIL_LActive backplane signal is active. Both these events indicate an error in the connection of the Ethernet module to the network.

5. Confirm the Ethernet connection error by browsing the network in the communication software.

If the node is no longer connected, an attempt to access the secondary RMCT fails and results in the following message.



To recover from a EtherNet/IP™ network disconnection, perform the following:

- Check all EtherNet/IP network and switch connections.
- If the Auto-synchronization parameter is not set to Always, use the commands in the Synchronization tab of the RMCT to synchronize your chassis.

For more information about troubleshooting EtherNet/IP network anomalies, see the EtherNet/IP Network Devices User Manual, publication [ENET-UM006](#).

Identify a Lost Redundancy Module Connection

To determine if a lost connection between the redundancy modules caused a switchover or state change, open the event log of the primary redundancy module.

Figure 69 - Lost Connection in Event Log

Chassis A						
Event	Log Time	Slot	Module Na...	Description	Classificati	
24076	12/17/2019 05:30:46:8...	3	1756-EN2TR	(4) Partner Connection Timeout	Synchroniz	
24075	12/17/2019 05:30:46:7...	2	1756-EN2TR	(4) Partner Connection Timeout	Synchroniz	
24074	12/17/2019 05:30:46:1...	1	1756-RM2	(1C) Chassis Redundancy State changed to DSw...	State Char	
24073	12/17/2019 05:30:46:1...	1	1756-RM2	(56) The partner RM has been disconnected	State Char	
24072	12/17/2019 05:30:46:1...	1	1756-RM2	(C) Port2 Communication error	Minor Fault	
24071	12/17/2019 05:30:46:1...	1	1756-RM2	(D0) CH2 Link Down	Minor Fault	
24070	12/17/2019 05:30:46:1...	1	1756-RM2	(C) Port2 Communication error	Minor Fault	

Chassis B						
Event	Log Time	Slot	Module Na...	Description	Classi	
9940	12/17/2019 05:31:43:901	1	1756-RM2	(1A) Chassis Redundancy State changed to PwQS	State	
9939	12/17/2019 05:31:43:771	2	1756-EN2TR	(14) Enter Qualification Phase 4	Qualif	
9938	12/17/2019 05:31:43:770	3	1756-EN2TR	(21) Equally Able To Control	State	
9937	12/17/2019 05:31:43:770	3	1756-EN2TR	(14) Enter Qualification Phase 4	Qualif	
9936	12/17/2019 05:31:43:742	1	1756-RM2	(2E) Qualification Complete	Qualif	

In the example above, the primary chassis event log clearly indicates that a redundancy module has been disconnected. The dimmed secondary chassis log also indicates that the module is not connected.

To resolve this anomaly, check the intermodule cable that connects the redundancy modules. Verify that it is properly connected and is not severed.

Once the anomaly is resolved, synchronize the chassis by using the synchronization commands in the Synchronization tab if your Auto-synchronization parameter is not set to Always.

Redundancy Module Missing

To determine if a missing redundancy module caused a state change and switchover, access the event log of the primary chassis.

Figure 70 - Partner Module Screamed Event

Chassis B						
Event	Log Time	Slot	Module Na...	Description	C	
5419	12/17/2019 01:59:06:876	1	1756-RM2	(D3) Switchover from CH1 to CH2	M	
5418	12/17/2019 01:59:06:876	1	1756-RM2	(CF) CH1 Link Down	M	
5417	12/17/2019 01:59:06:873	1	1756-RM2	(30) Switchover Attempted	S	
5416	12/17/2019 01:59:06:873	1	1756-RM2	(57) Partner RM Screamed.	S	
5415	12/17/2019 01:59:06:873	1	1756-RM2	(6) Hardware failure	M	
5414	12/17/2019 01:58:24:764	1	1756-RM2	(1E) Chassis Redundancy State changed to QSwP	S	
5413	12/17/2019 01:58:24:482	2	1756-EN2TR	(21) Transition To Qualified Secondary	C	

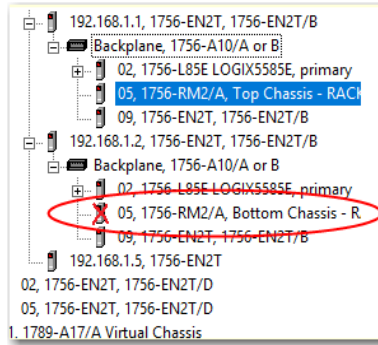
Chassis A						
Event	Log Time	Slot	Module Na...	Description	C	
6797	12/17/2019 01:58:24:764	1	1756-RM2	(1A) Chassis Redundancy State changed to PwQS	S	
6796	12/17/2019 01:58:24:533	3	1756-EN2TR	(21) Equally Able To Control	C	
6795	12/17/2019 01:58:24:533	2	1756-EN2TR	(14) Enter Qualification Phase 4	C	
6794	12/17/2019 01:58:24:532	3	1756-EN2TR	(14) Enter Qualification Phase 4	C	
6793	12/17/2019 01:58:24:503	1	1756-RM2	(2E) Qualification Complete	C	

Item	Description
A	Redundancy module screamed event indicates module removal.
B	Last normal event logged.
C	Dimmed secondary chassis log indicates issue with redundancy module.

The redundancy module logs the Partner RM Screamed event just before it is disconnected. Depending on the cause of the missing module, the Partner RM Screamed event can fail to be logged before the module is lost.

You can also browse to the redundancy module in the communication software to determine if it is connected to the network. A red X over the redundancy module indicates that the module is not reachable.

Figure 71 - Missing Redundancy Module



To correct the missing module anomaly, first verify that the redundancy module is correctly installed and powered. Then check the intermodule cable that connects the redundancy modules.

After you verify that the module is installed and powered, synchronize the chassis by using the synchronization commands in the Synchronization tab if your Auto-synchronization parameter is not set to Always.

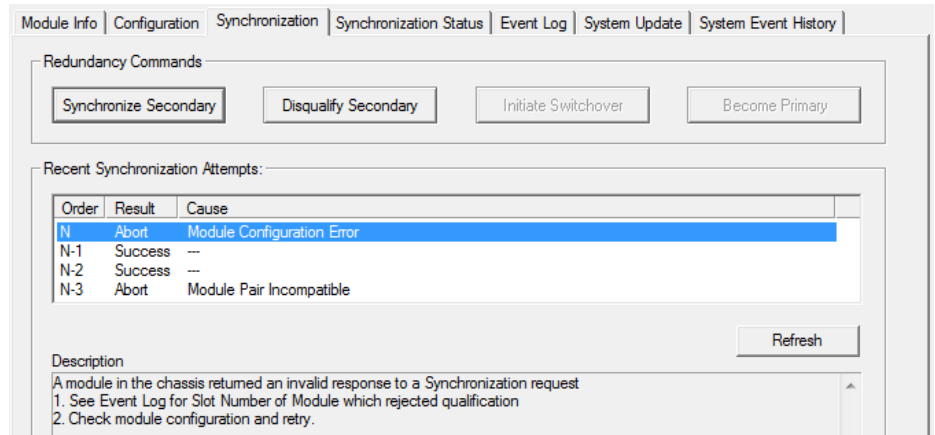
Qualification Failure Caused by Non-redundant Controller

If you place a controller that is not enabled for redundancy into the redundant chassis, the qualification and synchronization fail. To determine if your synchronization failure is due to a non-redundant controller, complete these steps.

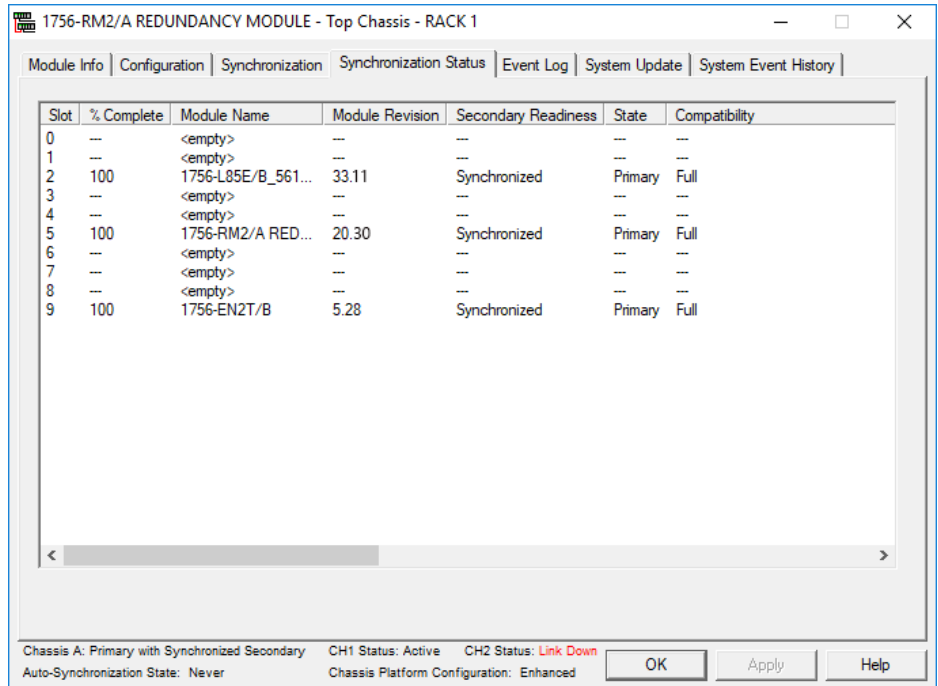
1. Open the RMCT for the primary module.
2. Select the Synchronization tab and view the Recent Synchronization Status Attempts log.

The log indicates that there is a module configuration error.

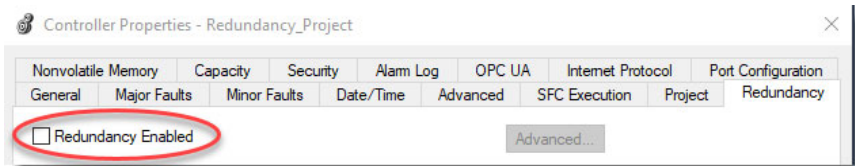
3. To view the description, select the failed attempt.



4. To check the compatibility between modules, select the Synchronization Status tab. In the example below, the Compatibility column shows all modules as fully compatible.



5. Open the Logix Designer application and go online with the primary controller in your system.
6. Open the controller properties and verify that Redundancy Enabled is selected. In the example below, the controller is not enabled for redundancy.



If Redundancy Enabled is **not** selected, then do the following:

- Remove the controllers that are not redundancy enabled.
- Enable the controller for redundancy and make other program changes to accommodate redundancy.
- After you remove or correct the Redundancy Enabled setting, attempt to synchronize your redundant system again.

Redundancy Module Faults

Redundancy modules can experience any of the following faults. You can view these faults in the event log or on the module status display.

Table 60 - Redundancy Module Fault Types

Fault Type	Description
Minor Recoverable	The fault does not stop redundancy operation and provides you with a recovery mechanism.
Minor Nonrecoverable	<ul style="list-style-type: none"> The fault does not stop redundancy operation. No recovery mechanism is available.
Major Recoverable	The fault impacts redundancy operations, although the effect is not always immediate. For example, if the fault occurred in the secondary redundancy module, the secondary chassis is disqualified and is not able to take control if the primary redundancy module fails.
Major Nonrecoverable	<ul style="list-style-type: none"> The fault is critical and redundancy operations stop. A switchover can occur. No recovery mechanism is available. The module can require replacement.

Faults can be cleared automatically or manually, depending on the type of fault:

- A major or minor recoverable fault is automatically cleared when the cause of the fault is resolved. If the fault is raised and immediately resolved by firmware, the fault persists for at least 1 minute. An example of this scenario is the detection of a corrupted log that is immediately fixed by resetting the log file.
- A major nonrecoverable fault can be cleared only by restarting the module or by removing and inserting the module in the chassis while power is applied.

IMPORTANT This section describes a subset of module fault codes that you can view in the event log or module status display.
If you see a fault code that is not included in this chapter, contact Rockwell Automation for assistance in troubleshooting that fault.

Event Log

The redundancy module logs the fault type in its event log in NVS memory. You can access the event log through the RMCT to troubleshoot the fault yourself or with assistance from Rockwell Automation Technical Support for troubleshooting the fault.

Module Status Display

A character string scrolls across the module status display to indicate the fault type. The character string displays the fault type in either of these ways:

- Two to four-character word abbreviations
- Alphanumeric codes

The following table describes the two- to four-character word abbreviations.

Table 61 - Major Fault Code Messages

1st Word	2nd Word	3rd Word	4th Word	Error Description
CFG	LOG	ERR		Configuration log error. No action is required.
COMM	RSRC	ERR		Communication resource error. Reset the redundancy module.
COMM	RSRC	ERR	PRT1	Port1 Communication resource error on Backplane. Reset the redundancy module and check the chassis.
COMM	RSRC	ERR	PRT2	Port2 Communication resource error on redundancy link. Complete these tasks: 1. Reset the module. 2. Check the cable.
COMM	ERR	PRT1		Port1 Communication error, Backplane communication. Check or replace the chassis.
COMM	ERR	PRT2		Port2 Communication error on the redundancy link. Check or replace the single-mode cable.
COMM	ERR			General Communication Error. No action is required.
DUPL	RM			Duplicate redundancy module. This module is not in control. Remove this redundancy module.
EVNT	LOG	ERR		Event Log Error. No action is required.
FRMW	ERR			Firmware error. Update the firmware.
HDW	ERR			Hardware failure. Replace the module.
OS	ERR			Operating system error. Replace the module.
RM	PWR	DOWN		The redundancy module power is down. The module detected a DC_Fail condition. Check the other modules in the chassis.
WDOG	ERR			Watchdog time out. Reset the module.
WDOG	FAIL			The watchdog task failed its status check. Replace the module.

The fault code is a four-character alphanumeric string. Valid characters are 0...9 and A through Z, except S and O. The first character is always E. Each firmware subsystem within the redundancy module is assigned a range of fault codes. Each subsystem assigns fault codes within its range. If you encounter one of these error codes, record the Exxx code and contact Rockwell Automation Technical Support.

Recovery Messages

For certain faults, the module status display provides recovery instructions. Up to four, four-character words are displayed.

Table 62 - Recovery Messages

Recovery Instruction Code	Description
RPLC MOD	Replace the redundancy module only.
RSET RM2	Reset the redundancy module only.
REMV MOD	Remove the redundancy module only.
SEAT MOD	Reinsert only the redundancy module into the chassis.

Redundant Controller Major Fault Messages

The Major Fault TXX:CXX message on the controller scrolling display indicates major faults.



This manual links to Logix 5000 Controller and I/O Fault Codes and Syslog Messages, [1756-RD001](#); the file automatically downloads when you click the link.

Online Firmware Updates

You can update redundancy system firmware while a redundancy system is online by using the Redundancy System Update (RSU) feature. The RSU feature is not required to update firmware when a redundancy system is offline.

To access release notes for each redundancy firmware revision, see the Product Compatibility and Download Center at rok.auto/pcdc.

The RSU feature has these restrictions:

- RSU is not supported if you are updating firmware revision 36 to firmware revision 37 and the redundancy system has FLEXHA 5000™ I/O modules in it.
- RSU can only update redundancy bundles to other redundancy bundles.
- RSU cannot jump major revisions. You can use RSU to update the system to only the next major revision. If the target revision is multiple major revisions later than the current revision, you must repeat the RSU process multiple times.
- RSU can only update a redundancy system to a later firmware bundle.
- RSU cannot move a redundancy system to an earlier firmware bundle.
- RSU cannot upgrade a redundancy system to a new controller family. For example, you cannot use RSU to upgrade from a ControlLogix® 5570 controller to a ControlLogix 5580 controller.
- The firmware of every module in the system must be at the same revision or higher in the bundle being updated to. See the Knowledgebase Technote [ControlLogix: Redundancy Firmware Bundle Revision History](#).
- A replacement controller must have memory equal to or greater than the memory in the original controller.
- Do not exceed 520 class 3 messages or HMI connections when you attempt to do an update with RSU or the lock for update could fail.

If the lock for update fails when you attempt to use RSU, see the Knowledgebase Technote [Lock for Update Fails](#).

Application constraints can limit the migration capability of some controllers. For example, some features are supported only with ControlLogix 5580 Process controllers.

Logix SIS Considerations

Consider the following when you update Logix SIS firmware:

- You can use the RSU feature to update Logix SIS firmware with or without a signed or locked application in either redundant controller. For example, you can have a signed application in the primary controller and still update firmware in the secondary controller without a signature and vice versa. Safety-locking is also optional.
- Because the controller firmware revision changes during the RSU process, there is a safety signature mismatch between the primary and secondary controllers. The system does not cross-check the safety signature between the controllers during the RSU process.

IMPORTANT After an online firmware update, it is your responsibility to validate the new safety application before you switch control to the secondary controller.

- The redundant safety controllers synchronize during the RSU process. For important information about synchronization and concurrent communication to I/O, see [Concurrent Communication to I/O](#).

Before You Begin

Before you update firmware in a redundancy system, complete these tasks:

- Download and install the compatible versions of the Studio 5000 Logix Designer® application, communication software, and ControlFLASH Plus™ software.

ControlFLASH Plus software updates the module firmware. For information on how to use ControlFLASH Plus software, see the ControlFLASH Plus Quick Start Guide, publication [CFP-QS001](#).

- Understand the migration paths for redundancy system updates.

Redundancy System	Resource
Logix SIS	Logix SIS Redundancy System Update Migration Paths
ControlLogix 5580	ControlLogix 5580 Redundancy System Update Migration Paths
ControlLogix 5570	ControlLogix 5570 Redundancy System Update Migration Paths

- Understand the redundant chassis requirements as described in [Chapter 2](#).
- Download and install the redundancy firmware bundle as described in [Chapter 5](#).
- Install the RMCT as described in [Chapter 5](#).

IMPORTANT Before you install RMCT version 8.06.03 or later, uninstall existing versions of the RMCT. If you do not uninstall previous versions, you can have difficulty uninstalling version 8.06.03 or later at another time.

- If your application includes ControlLogix 5570 controllers, version 26 or earlier, that communicate with ControlLogix 5570 controllers, version 30.051 or later, see [\(ControlLogix 5570 Only\) Align LINT Members on 8-byte Boundaries](#).

Verify the RMCT Version

The Redundancy Module Configuration Tool (RMCT) launches at the version that is compatible with the redundancy module firmware that is installed. You must update your RMCT version and the redundancy module firmware revision so it is compatible with the new RMCT version. If you do not perform this update, the About dialog box will not reflect the new RMCT version.

To verify the installed version of the RMCT, complete these steps.

- Access the RMCT.
- Right-click the title bar and choose About.

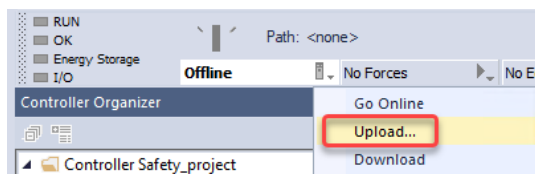
The version that appears on the About dialog box is the earliest RMCT version that you need based on your bundle

Prepare the Controller Project for the Update

Use the following procedure to upgrade to a major controller firmware revision, upgrade to a controller with more memory, or upgrade a communication module.

To prepare the controller project and controllers for the update, complete these steps.

- Start the Logix Designer application and select your redundancy project.
- Go online with the primary controller.
- To make sure that your offline project has the latest updates, or in case you do not have an offline file, upload the project from the primary controller.



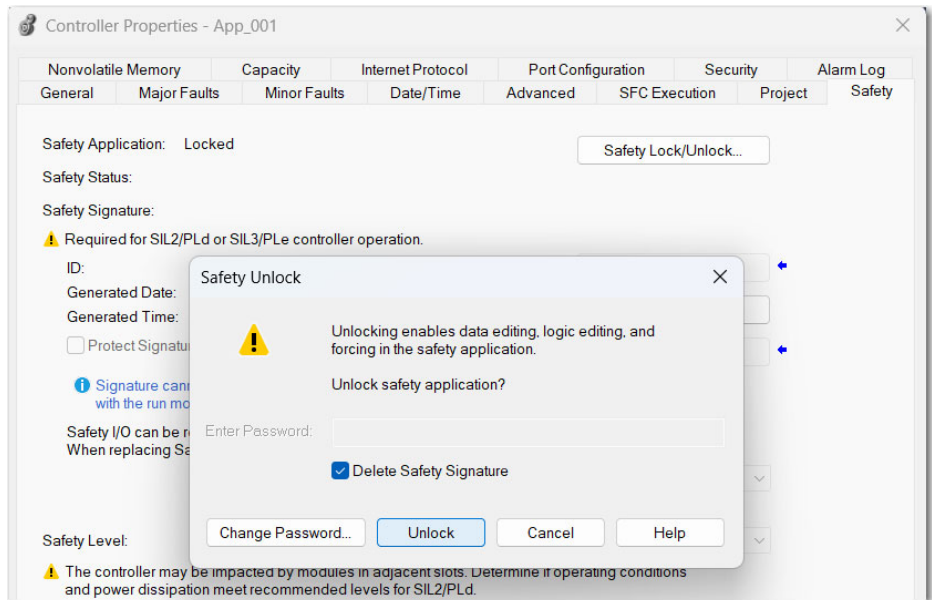
- If safety-locked, safety-unlock the controller.
- Cancel or assemble any pending test edits.
- Remove all sequential function chart (SFC) forces from the project.
- Verify that no changes are required for the following:
 - I/O forces

- I/O configuration

IMPORTANT After this step, changes to I/O cannot be made until after the redundancy system revision update is complete and both chassis are synchronized.

8. Save the project.
9. Go offline.
10. If the project is a Logix SIS project and the project has a safety signature, delete the safety signature.

IMPORTANT To move to another firmware revision, the project must be unlocked with no safety signature. If needed, keep a copy of the original signed project for your records.

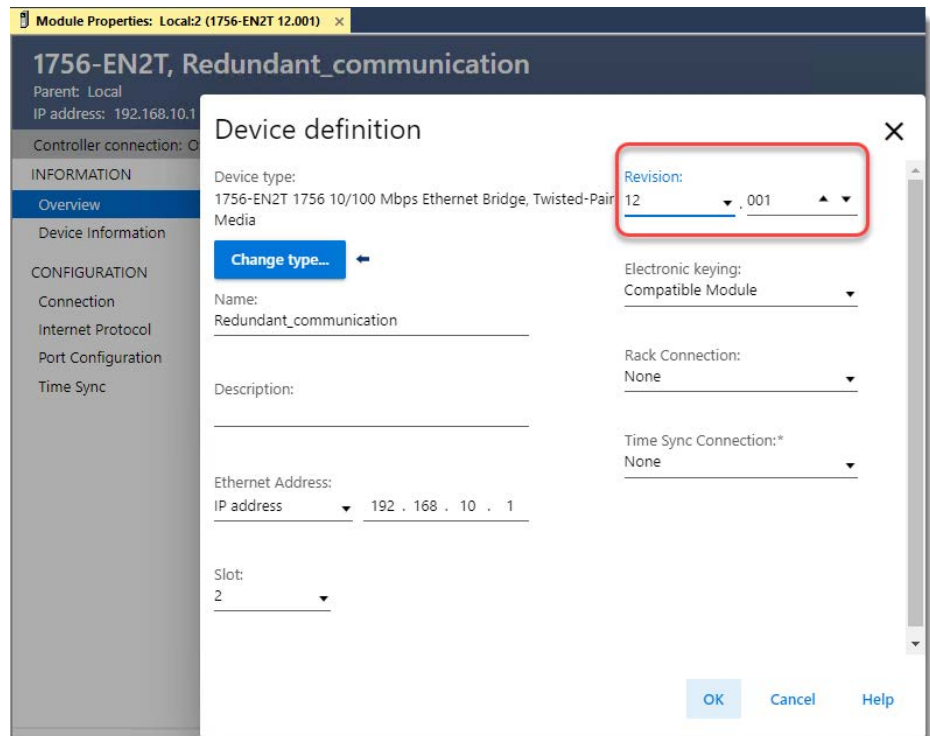


11. Open the controller properties.
12. On the General tab, select Change Controller.
13. Specify the controller catalog number and controller revision that you are upgrading to.
14. If you install a new controller while updating the secondary chassis firmware, specify the new controller catalog number.
15. Select OK.

The Logix Designer application converts the project to the later revision.

- For each communication module in the chassis, access the module properties and select the target firmware revision.

If you are unable to select the new revision, change the Electronic Keying parameter to Compatible Module. You must also select the highest available firmware revision.



- Save the project.
- Proceed to update the redundancy system firmware.

Update the Redundancy System Firmware

You can update redundancy firmware to another revision while your process continues to run. Before you update your redundancy system to a new revision, consider the following:

- During the update procedures, you cannot use the Logix Designer application to change the mode of the controller. Instead, use the keyswitch on the front of the controller.
- Remember the following when completing the tasks described in the rest of this section:
 - Do not change the project other than with changes that are identified in these tasks.
 - Verify that no one else is also changing the project.
 - Do not use a FactoryTalk® Batch Server to change equipment phase-states when upgrading your redundancy system.

To update your running redundancy system, complete this process.

- Prepare the redundant chassis for the firmware update.
- Update the redundancy module firmware in the secondary chassis.
- Update the redundancy module firmware in the primary chassis.
- Update other module firmware in the secondary chassis.
- Lock the system for update and initiate a locked switchover.
- Update other module firmware in the new secondary chassis.
- Synchronize the redundant chassis.



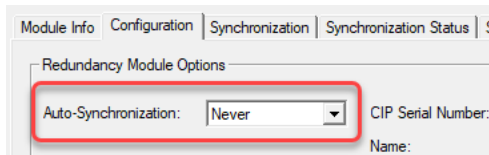
WARNING: While you complete the process to update the redundancy system firmware, there is a loss of redundancy. The controller runs the machinery without a backup until the update is complete.

Prepare the Redundant Chassis for the Firmware Update

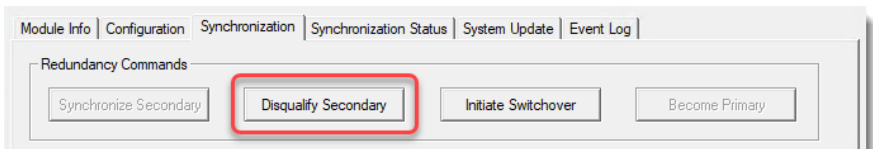
Before you can update firmware, you must set the Auto-qualification parameter to Never and manually disqualify the secondary chassis.

To prepare the primary and secondary chassis for the firmware update, complete these steps.

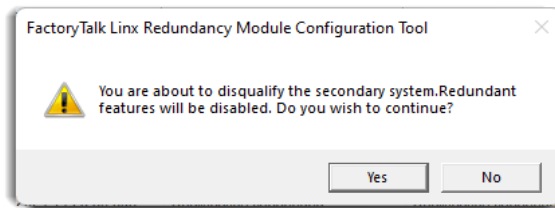
1. Set the keyswitch on the primary and secondary controllers to REM.
If both controllers in the redundant chassis pair are not in Remote Run (REM) mode, the firmware update cannot be completed.
2. Access the RMCT for the redundancy module primary chassis.
3. On the Configuration tab of the RMCT, set Auto-synchronization to Never.



4. Select Apply, and then select Yes.
5. On the Synchronization tab, select Disqualify Secondary



6. When the following message appears, select Yes to proceed.



The secondary chassis is disqualified as shown in bottom left of the RMCT and on the status display of the redundancy module.

7. Close the RMCT to help prevent a timeout from occurring when the firmware of the redundancy module is updated.
8. Proceed to update the redundancy module firmware in the secondary chassis.

Update the Redundancy Module Firmware in the Secondary Chassis

IMPORTANT

To maintain the crossload communication path between redundant modules during the update process, you must update the redundancy module firmware in the secondary chassis before the primary chassis. If you only have physical access to the primary chassis, then the secondary chassis must be updated first to ensure a valid communication path.

To update the redundancy module firmware in the secondary chassis, complete these steps.

1. Launch ControlFLASH Plus software.
2. Update the redundancy module firmware.
3. Close the ControlFLASH Plus software.
4. Proceed to update the redundancy module firmware in the primary chassis.

Update the Redundancy Module Firmware in the Primary Chassis

To update the redundancy module firmware in the primary chassis, complete these steps.

1. Launch ControlFLASH Plus software.
2. Update the redundancy module firmware.
3. Once the firmware update is complete, verify that the redundancy module status displays PRIM, which indicates a successful upgrade.
4. Close the ControlFLASH Plus software.
5. Proceed to update the other module firmware in the secondary chassis.

Update Other Module Firmware in the Secondary Chassis

To update firmware for other modules in the secondary chassis, complete these steps.

1. Optional: To replace module hardware, remove the module from the secondary chassis and replace it with the new module.

Before you replace communication modules as part of this firmware update process, make sure that you first read [Module Replacement](#). When replacing communication modules, the rotary switches and port configuration for the new modules must match the existing modules.

2. Launch ControlFLASH Plus software.
3. Update the firmware for modules other than the redundancy module.
4. Close the ControlFLASH Plus software.
5. Proceed to download the project to the secondary controller.

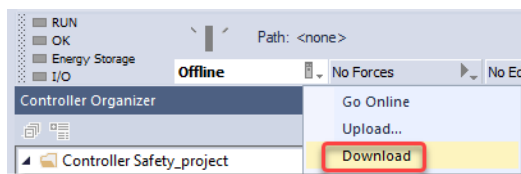
Download the Project to the Secondary Controller

When you download a project that has I/O forces enabled, the application prompts you to enable or disable forces after the download completes. After the locked switchover, the forces are whatever you selected (enabled or disabled).

IMPORTANT For Logix SIS, the generation of a safety signature on the secondary controller is prohibited. If you require a signed application, the project must be signed before you download it to the secondary controller. You can safety-lock the project after you download the signed application.

1. Download the project to the secondary controller.

IMPORTANT Be sure that the project is ready to download according to the instructions in [Prepare the Controller Project for the Update](#).



2. Go offline.
3. Proceed to lock the system for update and initiate a locked switchover.

Lock the System for Update and Initiate a Locked Switchover

For details about the Lock for Update and Initiate Locked Switchover commands that are used in this procedure, see [Initiate System Update Commands in the RMCT](#).



ATTENTION: Before you switch control to a secondary Logix SIS safety controller, verify that the safety project on the secondary controller is the one you intend to execute. You can use the safety signature to verify that the correct safety project is on the controller.

IMPORTANT

During a lock for update in Logix SIS redundancy, the safety function is temporarily muted for up to 2 seconds + 1 safety task period.

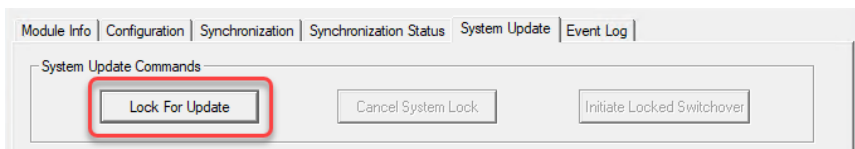
IMPORTANT

Remain offline with your controller while completing this procedure:

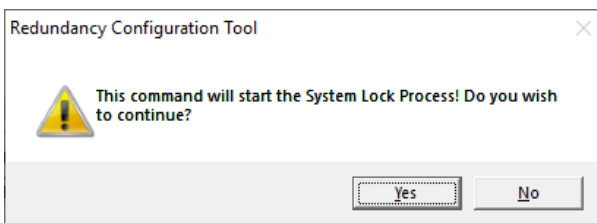
- Once you have locked the system, keep the system locked. If you unlock the system during this procedure, the project is cleared from the secondary controller.
- Do not disconnect any communication cables during these steps.
- A locked switchover resets sequential function chart (SFC) instructions to their initial state and causes the SFC instructions to execute twice.
- After the locked switchover, the new secondary controller no longer contains an application and the configuration parameters are reset to the default settings.

To lock the system for update and initiate a switchover, complete these steps.

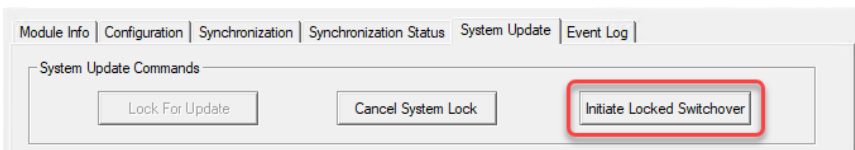
1. Access the RMCT for the redundancy module in the primary chassis.
2. On the System Update tab, select Lock for Update.



3. When the following message appears, select Yes to begin the system lock process.



4. Wait for the system to lock.
To troubleshoot errors, see Knowledgebase Technote [Lock for Update Fails](#).
5. Select Initiate Locked Switchover, and then select Yes.



The secondary chassis assumes control and becomes the new primary chassis:

- The Locked Switchover Attempts log indicates success.
 - The chassis status indicates the switchover state in the bottom left of the RMCT.
6. Close the RMCT.
 7. Proceed to update other module firmware in the secondary chassis.

Update Other Module Firmware in the New Secondary Chassis

To update firmware for other modules in the new secondary chassis, complete these steps.

1. Optional: To replace module hardware, remove the module from the secondary chassis and replace it with the new module.

Before you replace communication modules as part of this firmware update process, make sure that you first read [Module Replacement](#). When replacing communication modules, the rotary switches and port configuration for the new modules must match the existing modules.

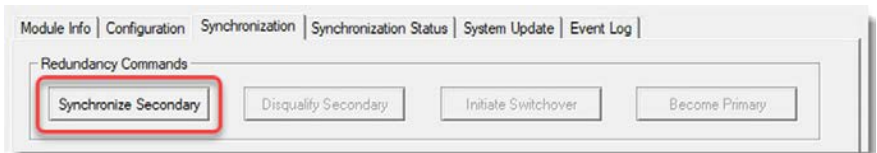
2. Launch ControlFLASH Plus software.
3. Update the firmware for modules other than the redundancy module.
4. Close the ControlFLASH Plus software.
5. Proceed to synchronize the redundant chassis pair.

Synchronize the Redundant Chassis Pair

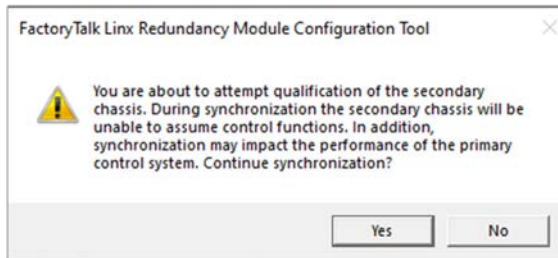
For details about the Synchronize Secondary and Initiate Switchover commands that are used in this procedure, see [Initiate Redundancy Commands in the RMCT](#).

To synchronize the redundant chassis pair after the firmware in both chassis have been updated to the same revision, complete these steps.

1. Access the RMCT for the redundancy module in the primary chassis.
2. On the Synchronization tab, select Synchronize Secondary.

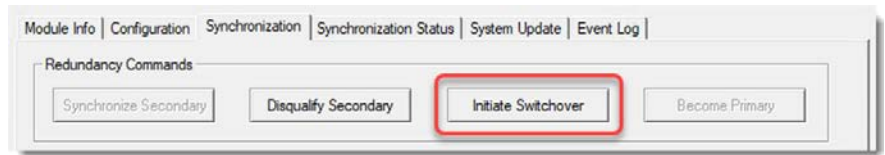


3. When the following warning appears, select Yes to proceed.

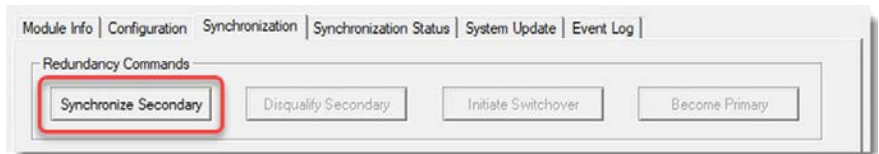


4. Wait for the synchronization to complete.

5. If the rotary switches on the communication modules in the redundant chassis are set between 2...254, complete these steps.
 - a. Initiate a switchover.



- b. In the new secondary chassis, set the rotary switches on the communication modules back to the original configuration.
 - c. Repeat this process for all communication modules that need the rotary switches set back to 2...254.
 - d. Set Auto-synchronization to your preferred setting.
 - e. If you set Auto-synchronization to Conditional, manually synchronize the chassis.



6. Set the redundancy module date and time according to your preference.
7. Select Apply.
8. Close the RMCT.

EDS Files

If you see modules that are displayed in the communication software with yellow question marks, the EDS files for the modules are not registered. You can right-click on the module and proceed with the "Upload EDS files from device" wizard to upload the EDS file. If this option is not available or as an alternative, follow this link to obtain the EDS files for modules in your system: [Electronic Data Sheets \(EDS\)](#)

1. Download the required EDS file.
2. Select Start > Programs > Rockwell Software > EDS Hardware Installation Tool.
The tool prompts you to Add or Remove EDS files.

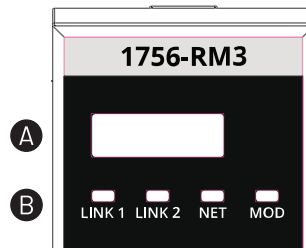
Your redundant system firmware update is now complete.

Notes:

Status Indicators

1756-RM3 Status Indicators

The 1756-RM3XT status indicators operate the same as 1756-RM3 status indicators.



Item	Description
A	Alphanumeric display that scrolls messages approximately every 15 seconds.
B	Status indicators: <ul style="list-style-type: none"> • Link 1 and Link 2—Indicates the current state of Link 1 and Link 2. • NET—The Network status indicator represents the status of the EtherNet/IP™ network. • MOD—The Module status indicator represents the entire state of the redundancy module.

Table 63 - 1756-RM3 Status Messages

Message	Description
????	The initial state of the module is resolving. Wait for the resolution to finish. No action is required.
CPU Internal Thermal Fault	The module had to shut down after becoming too hot. This is a major nonrecoverable fault with fault code 0x2. To recover from the fault, reset the module. For more information, see Understand Temperature Monitoring and Fault Behavior .
Critical Temperature	The module is too hot or too cold. This is a major recoverable fault with fault code 0x5. For more information, see Understand Temperature Monitoring and Fault Behavior .
DISQ	The secondary redundancy module is disqualified. Check the type and revision of the secondary partner module.
Duplicate RM - Remove This RM	A redundancy module already exists in the chassis. Remove the duplicate redundancy module.
Exxx	An error occurred during powerup. Following this error, the module will reset and restart. If the problem persists, provide the error message to Technical Support for further guidance.
Firmware Installation Required	The module is using boot firmware (revision 1.xxx) and requires a firmware update.
Flash in Progress	The module is updating its firmware. Wait for the firmware update to finish. No action is required.
Link X - 1 Gb/FULL	A supported SFP transceiver is detected in the specified channel (1 or 2), and the link is operating normally with no faults.
Link X - Disabled	The SFP transceiver in the specified channel (1 or 2) is disabled.
Link X - Down	No SFP transceiver is detected in the specified channel (1 or 2) and the transceiver has not been disabled. Possible causes include the following: <ul style="list-style-type: none"> • The cable is loose, disconnected, broken, or damaged • The signal is attenuated • The connector is loose • The partner redundancy module is powered down or in a major fault state This is a minor recoverable fault. Once the link is detected, the redundancy module clears the fault.
LKNG	The secondary redundancy module is in the process of locking for update.
LOCK	The secondary redundancy module is locked for update.
Module Configuration Failure	Possible causes include the following: <ul style="list-style-type: none"> • The module configuration was not successfully stored to nonvolatile memory. • The redundancy module failed to apply fiber security configuration changes.
Module Configuration Load Failure	The module configuration was not successfully retrieved from nonvolatile memory.

Table 63 - 1756-RM3 Status Messages (Continued)

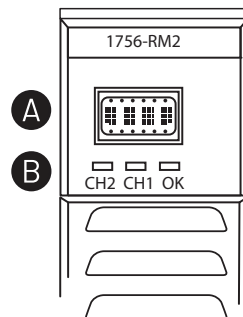
Message	Description
Module Fault - Power Cycle or Reset Module	The module has a major nonrecoverable fault. Remove and reinsert the module. If module continues to display this message repeatedly after subsequent restarts, try the following: 1. Disconnect the module from its partner. 2. Remove all other modules from chassis. 3. Restart the faulted module. 4. If the module powers up correctly, reinsert modules into the chassis and update the redundancy module firmware.
Module Fault (AAA-BBB-CCC) - Power Cycle or Reset Module	The module has a major nonrecoverable fault. Save the displayed 9-character fault ID and then remove and reinsert module. For further investigation, provide the fault ID along with the fault log on the microSD™ card to Technical Support. If module continues to display this message repeatedly after subsequent restarts, try the following: 1. Disconnect the module from its partner. 2. Remove all other modules from chassis. 3. Restart the faulted module. 4. If the module powers up correctly, reinsert modules into the chassis and update the redundancy module firmware.
Module in Slot X Failed - Replace Module	The module in the specified slot (0...16) cannot reliably participate in the redundancy system because it not able to notify the redundancy module of failure. Remove and replace the module in the specified slot.
RM Failed - Replace Module	The redundancy module failed to successfully pass the SysFail test. Remove and replace the redundancy module.
Not Compatible Partner Connected	The module is connected to a partner module with a different major firmware revision or different major or minor software version.
Over Temperature	The module is hot, but not at a critical temperature. This is a minor recoverable fault with fault code 0x6. For more information, see Understand Temperature Monitoring and Fault Behavior .
PASS	Power-up tests successfully completed.
PRIM	The module is operating as the primary redundancy module. No action is required.
QFNG	The redundancy system is qualifying the secondary redundancy module. No action is required.
Rev XX.xxx	The major and minor firmware revision of the module.
RM Log Lost	Event logs were lost and the redundancy module is reinitializing the event log instances. The high availability of the module is not impacted, but the module may not be able to correctly propagate events into the RMCT. This message can appear after a redundancy module firmware update or redundancy module replacement. The message disappears in 180 seconds.
SD Card Failure	The microSD card has a fault. Possible causes include the following: <ul style="list-style-type: none"> • Power faults • Problems with partitions on the card • Card not mounting after a long wait
SD Card Format Invalid	The microSD card does not have a compatible FAT32 format.
SD Power Fault	The microSD card has a power fault.
SFP X - Missing	No SFP transceiver is detected in the specified channel (1 or 2). Possible causes include the following: <ul style="list-style-type: none"> • The transceiver is loosely connected • The transceiver is not installed The message indicates a minor recoverable fault. The redundancy module clears the fault if the transceiver is detected or disabled.
SFP X - Unsupported	The SFP transceiver in the specified channel (1 or 2) is not supported by Rockwell Automation or the SFP standard is not recognized. The message indicates a minor recoverable fault. Once the transceiver is removed or disabled, the redundancy module clears the fault.
SFP X - Faulted	The SFP transceiver in the specified channel (1 or 2) is faulted. The message indicates a minor recoverable fault. Once the transceiver is removed or disabled, the redundancy module clears the fault.
SYNC	The redundancy system is synchronized with a qualified secondary redundancy module. No action is required.
TEST	The module is performing power-up tests.

Table 64 - 1756-RM3 Status Indicators

Indicator	Status	Description
Link 1/Link 2	Steady off	One of these conditions exist: <ul style="list-style-type: none"> The module has a major recoverable or major nonrecoverable fault. A non-volatile storage (NVS) update is in process. The port is not connected. The port is disabled. No power is applied to the module.
	Flashing green	The module is receiving traffic on the port.
	Steady green	The port is active, but not receiving data.
	Flashing red	One of these conditions exist: <ul style="list-style-type: none"> Link 1 is connected to Link 2. The port has an intermittent loss of communication.
	Steady red	One of these conditions exist: <ul style="list-style-type: none"> The port is enabled, but no SFP module is installed. The SFP module is faulted or failed. The SFP module is installed and operating, but has a mismatched vendor ID.
	Flashing green, red, off	When green for approximately 250 ms, red for approximately 250 ms, and then off, the module is performing its power-up testing. The status indicator continues this sequence until the power-up testing is complete.
NET	Steady off	One of these conditions exist: <ul style="list-style-type: none"> No power is applied to the module. The module has a major nonrecoverable fault.
	Flashing green	The module is ready to communicate with its partner but no connection has been made yet.
	Steady green	The module is communicating with its partner.
	Flashing green, red, off	When green for approximately 250 ms, red for approximately 250 ms, and then off, the module is performing its power-up testing. The status indicator continues this sequence until the power-up testing is complete.
MOD	Steady off	No power is applied to the module.
	Flashing green	One of these conditions exist: <ul style="list-style-type: none"> The module has not been configured. A non-volatile storage (NVS) update is in process.
	Steady green	The module is operating normally.
	Flashing red	One of these conditions exist: <ul style="list-style-type: none"> The module has a major recoverable fault. A firmware update is required.
	Steady red	The module has a major nonrecoverable fault.
	Flashing green, red, green	When green for approximately 250 ms, red for approximately 250 ms, and then steady green, the module is performing its power-up testing. The status indicator continues this sequence until the power-up testing is complete.

1756-RM2 Status Indicators

The 1756-RM2XT status indicators operate the same as 1756-RM2 status indicators.



Item	Description
A	Status messages—Provide diagnostic information.
B	Status indicators: <ul style="list-style-type: none"> CH1 and CH2—Indicates the current state of Channel 1 and Channel 2. OK—Indicates the current state of the redundancy module.

Table 65 - 1756-RM2 Status Messages

Message	Description
Txxx	The redundancy module is executing a self-test at powerup. (xxx represents a hexadecimal test identification number.) Wait for the self-test to finish. No action is required.
XFER	Application firmware update is in progress. Wait for the firmware update to finish. No action is required.
ERAS	Boot mode - Erasing current redundancy module firmware
PROG	Update mode - Updating redundancy module firmware Wait for the firmware update to finish. No action is required.
????	Resolving initial redundancy module state Wait for the state resolution to finish. No action is required.
PRIM	Primary redundancy module. The module is operating as the primary module. No action is required.
DISQ	Disqualified secondary redundancy module. Check the type and revision of the secondary partner module.
QFNG	Qualifying secondary redundancy module. Redundant system status. No action is required.
SYNC	Qualified secondary redundancy module. Redundant system status. No action is required.
LKNG	Secondary redundancy module that is in the process of locking for update.
LOCK	Secondary redundancy module that is locked for update.
Exxx	Major fault has occurred (xxx represents an error or fault code, with the two least-significant characters in decimal). Use the Error ID code to diagnose and address the error.
EEPROM Update Required	Onboard EEPROM is empty. Replace the module.
BOOT Erase Error	Error in erasing NVS device while updating boot image. Cycle power to the module. If the error persists, replace the module.
BOOT Program Error	Error in writing in NVS device while updating boot image. Cycle power to the module. If the error persists, replace the module.
APP Erase Error	Error in erasing NVS device while updating application image. Cycle power to the redundancy module. If the error persists, replace the module.
APP Program Error	Error in writing in NVS device while updating application image. Cycle power to the redundancy module. If the error persists, replace the module.
CONFIG Erase Error	Error in erasing NVS device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
CONFIG Program Error	Error in writing in NVS device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
EEPROM Write Error	Error in writing in EEPROM device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
Application Update Required	The module is running boot firmware. Download the application firmware that is obtained from the respective redundancy bundle.
ICPT	A test line on the backplane is asserted. Check if the error message goes away after removing each module, one at a time. If the error persists, cycle power to the chassis, or replace the chassis.
!Cpt	All modules in the chassis do not belong to the same redundancy platform.
Untrusted Certificate Error	The 1756-RM2 and 1756-RM2XT modules use signed firmware. This error appears when either the contents of the downloaded certificate or its signature for the downloaded firmware is invalid.
Unknown ⁽¹⁾	Operating state is not yet determined.
Active ⁽¹⁾	The channel is operating normally as the active channel.
Redundant ⁽¹⁾	The channel is operating normally as the redundant channel.
Link Down ⁽¹⁾	The channel is disconnected. Several causes could be: <ul style="list-style-type: none"> - The cable is disconnected, broken, or damaged - The signal is attenuated - The connector is loose - The partner 1756-RM2 module is powered down or in a major fault state
No SFP ⁽¹⁾	No transceiver was detected. Several causes could be: <ul style="list-style-type: none"> - It has failed - It is loosely connected - It is not installed
SFP !Cpt ⁽¹⁾	Rockwell Automation does not support the transceiver.
SFP Fail ⁽¹⁾	The transceiver is in a failed state.

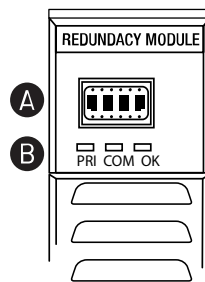
(1) Can be present for either CH1 or CH2, but not both simultaneously.

Table 66 - 1756-RM2 Status Indicators

Indicator	Status	Description
OK	Off	No power is applied to the redundancy module. If necessary, apply power.
	Steady red	One of these conditions exists: <ul style="list-style-type: none"> The redundancy module is conducting a self-test during powerup. No action is necessary. The redundancy module has experienced a major shutdown fault. Cycle power to clear the fault. If the major fault does not clear, replace the module.
	Flashing red	One of these conditions exists: <ul style="list-style-type: none"> The redundancy module is updating its firmware. No action is necessary. The redundancy module has been configured improperly. Check the module configuration and correct any issues. The redundancy module has experienced a major fault that can be cleared remotely using the RMCT.
	Steady green	The redundancy module is operating normally. No action is required.
	Flashing green	The redundancy module is operating normally but is not communicating with the other redundancy modules in the same chassis. If necessary, establish communication with the other redundancy module.
CH1/CH2	Off	One of these conditions exists: <ul style="list-style-type: none"> No power RM major fault NVS update
	Steady green ⁽¹⁾	Channel is operating as the active channel.
	Steady red	One of these conditions exists: <ul style="list-style-type: none"> No transceiver plugged in Faulted or failed transceiver detected Transceiver with incorrect or vendor ID detected
	Intermittent red	For 1 s, then off, indicates powerup.
	Flashing red	One of these conditions exists: <ul style="list-style-type: none"> Redundant channel error No cable connection
	Intermittent green ⁽¹⁾	On for 256 ms for each packet that is received, then off. Active operating channel. (Channel that is used for data communication between the partner 1756-RM2 modules.)
	Flashing green ⁽¹⁾	The channel is operating as the back-up channel and is ready to become the Active channel if the current Active channel fails.

(1) Can be present for either CH1 or CH2, but not both simultaneously.

1756-RM Status Indicators



Item	Description
A	Status messages—Provide diagnostic information.
B	Status indicators: <ul style="list-style-type: none"> PRI—Indicates whether the module is functioning as the primary module. COM—Indicates state of communication between the redundant chassis pair. OK—Indicates the current state of the redundancy module.

Table 67 - 1756-RM Status Messages

Message	Description
Txxx	The redundancy module is executing a self-test at power-up. (xxx represents a hexadecimal test identification number.) Wait for the self-test to finish. No action is required.
XFER	Application firmware update is in progress. Wait for the firmware update to finish. No action is required.
ERAS	Boot mode - Erasing current redundancy module firmware.
PROG	Boot mode - Updating redundancy module firmware. Wait for the firmware update to finish. No action is required.
????	Resolving initial redundancy module state. Wait for the state resolution to finish. No action is required.
PRIM	Primary redundancy module. The module is operating as the primary module. No action is required.
DISQ	Disqualified secondary redundancy module. Check the type and revision of the secondary partner module.
QFNG	Qualifying secondary redundancy module. Redundant system status. No action is required.
SYNC	Qualified secondary redundancy module. Redundant system status. No action is required.
LKNG	Secondary redundancy module that is in the process of locking for update.
LOCK	Secondary redundancy module that is locked for update.
Exxx	Major fault has occurred (xxx represents an error or fault code, with the two least-significant characters in decimal). Use the Error ID code to diagnose and address the error.
EEPROM Update Required	Onboard EEPROM is empty. Replace the module.
BOOT Erase Error	Error in erasing NVS device while updating boot image. Cycle power to the module. If the error persists, replace the module.
BOOT Program Error	Error in writing in NVS device while updating boot image. Cycle power to the module. If the error persists, replace the module.
APP Erase Error	Error in erasing NVS device while updating application image. Cycle power to the redundancy module. If the error persists, replace the module.
APP Program Error	Error in writing in NVS device while updating application image. Cycle power to the redundancy module. If the error persists, replace the module.
CONFIG Erase Error	Error in erasing NVS device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
CONFIG Program Error	Error in writing in NVS device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
EEPROM Write Error	Error in writing in EEPROM device while updating configuration log image. Cycle power to the redundancy module. If the error persists, replace the module.
Application Update Required	The module is running boot firmware. Download the application firmware that is obtained from the respective redundancy bundle.
ICPT	A test line on the backplane is asserted. Check if the error message goes away after removing each module, one at a time. If the error persists, cycle power to the chassis, or replace the chassis.
!Cpt	All modules in the chassis do not belong to the same redundancy platform.

Table 68 - 1756-RM Status Indicators

Indicator	Status	Description
COM	Off	One of these conditions exists: <ul style="list-style-type: none"> No power is applied to the module. Apply power to the module. There is no communication between redundancy modules in the redundant chassis pair. Diagnose the redundancy configuration to determine why no communication is taking place.
	Red < 1 second	The module has been started and has established partner communication. No action is required.
	Steady red	The module has experienced a critical communication failure. Cycle power to clear the fault. If the major fault does not clear, replace the module.
	Flashing green > 250 ms	Communication activity is present. No action is required.

Table 68 - 1756-RM Status Indicators (Continued)

Indicator	Status	Description
OK	Off	No power is applied to the redundancy module. If necessary, apply power.
	Steady red	One of these conditions exists: <ul style="list-style-type: none"> The redundancy module is conducting a self-test during power-up. No action is necessary. The redundancy module has experienced a major fault. Cycle power to clear the fault. If the major fault does not clear, replace the module.
	Flashing red	One of these conditions exists: <ul style="list-style-type: none"> The redundancy module is updating its firmware. No action is necessary. The redundancy module has been configured improperly. Check the module configuration and correct any issues. The redundancy module has experienced a minor failure. Cycle power to clear the fault. If the major fault does not clear, replace the module.
	Steady green	The redundancy module is operating normally. No action is required.
	Flashing green	The redundancy module is operating normally but is not communicating with the other redundancy module. If necessary, establish communication with the other redundancy module.
PRI	Steady green	Indicates that the module is functioning as the primary module.
	Off	Indicates that the module is functioning as the secondary module.

Notes:

Redundancy Object Attributes

Use this table of redundancy object attributes as a reference when programming to obtain the status of your redundancy system.

Table 69 - Redundancy Object Attributes

Status Information	Attribute	Data Type	GSV/SSV	Description	
				If	Then
Redundancy status of the entire chassis.	ChassisRedundancyState	INT	GSV	16#2	Primary with synchronized secondary
				16#3	Primary with disqualified secondary
				16#4	Primary with no secondary
				16#10	Primary locked for update
Redundancy state of the partner chassis.	PartnerChassisRedundancyState	INT	GSV	16#8	Synchronized secondary
				16#9	Disqualified secondary with primary
				16#E	No partner
				16#12	Secondary locked for update
Redundancy status of the controller.	ModuleRedundancy State	INT	GSV	16#2	Primary with synchronized secondary
				16#3	Primary with disqualified secondary
				16#4	Primary with no secondary
				16#6	Primary with synchronizing secondary
				16#F	Primary locking for update.
				16#10	Primary locked for update
Redundancy state of the partner.	PartnerModuleRedundancyState	INT	GSV	16#7	Synchronizing secondary
				16#8	Synchronized secondary
				16#9	Disqualified secondary with primary
				16#E	No partner
				16#11	Secondary locking for update
				16#12	Secondary locked for update
Results of the compatibility checks with the partner controller.	CompatibilityResults	INT	GSV	0	Undetermined
				1	No compatible partner
				2	Fully compatible partner
Status of the synchronization (qualification) process.	Qualification InProgress	INT	GSV	-1	Synchronization (qualification) is not in progress.
				0	Unsupported
				1...99	For modules that can measure their completion percentage, the percent of synchronization (qualification) that is complete.
				50	For modules that cannot measure their completion percentage, synchronization (qualification) is in progress.
				100	Synchronization (qualification) is complete.
Keyswitch settings of the controller and its partner match or do not match.	KeyswitchAlarm	DINT	GSV	0	<ul style="list-style-type: none"> • The keyswitches match OR • No partner is present.
				1	Keyswitches do not match

Table 69 - Redundancy Object Attributes (Continued)

Status Information	Attribute	Data Type	GSV/SSV	Description	
Position of the keyswitch of the partner.	PartnerKeyswitch	DINT	GSV	If	Then the keyswitch is in
				0	Unknown
				1	RUN
				2	PROG
				3	REM
Status of the minor faults of the partner (if the ModuleRedundancyState indicates that a partner is present).	PartnerMinorFaults	DINT	GSV	This bit	Means this minor fault
				1	Power-up fault
				3	I/O fault
				4	Problem with an instruction (program)
				6	Periodic task overlap (watchdog)
				10	Issue with the energy storage module
Mode of the partner.	PartnerMode	DINT	GSV	If	Then
				16#0	Power up
				16#1	Program
				16#2	Run
				16#3	Test
				16#4	Faulted
				16#5	Run-to-program
				16#6	Test-to-program
				16#7	Program-to-run
				16#8	Test-to-run
				16#9	Run-to-test
				16#A	Program-to-test
				16#B	Into faulted
				16#C	Faulted-to-program
In a pair of redundant chassis, identification of a chassis without regard to the state of the chassis.	PhysicalChassisID	INT	GSV	If	Then
				0	Unknown
				1	Chassis A
				2	Chassis B
Slot number of the redundancy module in this chassis.	SRMSlotNumber	INT	GSV	This attribute identifies the slot number in which the redundancy module is installed.	
<ul style="list-style-type: none"> Size of the last crossload. Size of the last crossload if you had a secondary chassis. 	LastDataTransfer Size	DINT	GSV	This attribute gives the size of data that was or would have been crossloaded in the last scan in the number of DINTs (4-byte words). The secondary chassis does not have to be connected or online. If you do not have a secondary chassis, the number of DINTs that would have been crossloaded is indicated.	
<ul style="list-style-type: none"> Size of the biggest crossload. Size of the biggest crossload if you had a secondary chassis. 	MaxDataTransfer Size	DINT	GSV SSV	This attribute gives the biggest size of the LastDataTransfer Size attribute in DINTs (4-byte words). The secondary chassis does not have to be connected or online. If you do not have a secondary chassis, the largest number of DINTs that would have been crossloaded is indicated. If you must reset this value, use an SSV instruction with a Source value of 0.	

Redundancy System Checklists

Chassis Configuration Checklist

✓	Requirement
	The redundant chassis are the same size, for example, both are 1756-A7, 7-slot chassis.
	For Logix SIS and ControlLogix® 5580 chassis, use only one controller in each chassis. For ControlLogix 5570 chassis, use up to two controllers in each chassis.
	Modules in the redundant chassis pair meet the requirements described in Redundant Chassis Pair .
	Each chassis of the pair is composed of identical modules that are of identical redundancy firmware revisions and catalog numbers.
	Partner modules are placed in the same slots of both chassis of the redundant pair.
	I/O modules are not placed in the redundant chassis.

Remote I/O Checklist

✓	Requirement
	I/O is not placed in redundant chassis.
	I/O is connected to the redundant chassis by the same network as the redundant controller chassis without bridging.
	(ControlLogix 5580 and 5570 redundancy). If you do not use concurrent communication with I/O, all I/O and consumed tag connections in the I/O tree of the redundancy controller must be multicast connections. The I/O tree of the redundancy controller can contain produced unicast tags that remote devices consume. Produced and consumed safety tags are not configured in Logix SIS.

Redundancy Module Checklist

✓	Requirement
	One redundancy module is placed in the same slot of each redundant chassis.
	Redundancy modules meet the requirements that are described in Redundancy Module Requirements .
	A fiber-optic cable connects the redundancy modules in the redundant chassis pair. The following are catalog numbers of fiber-optic cables you can order from Rockwell Automation: <ul style="list-style-type: none"> • 1756-RMC1 (1 m, 3.28 ft) • 1756-RMC3 (3 m, 9.84 ft) • 1756-RMC10 (10 m, 32.81 ft) You can make your own fiber-optic cable that is up to 10 km (32,808.40 ft) for 1756-RM2 modules or up to 70 km (229,659 ft) for 1756-RM3 modules, depending on the SFP used. For more information, see the Redundancy Module Installation Instructions, publication 1756-IN095 .

Controller Checklist

✓	Requirement
	Identical ControlLogix controllers are placed in the same slot of both chassis of the redundant pair.
	Partnered controllers are identical in firmware revision.
	Controllers meet the requirements that are described in Redundant Controller Requirements .
	(ControlLogix 5570 redundancy). Each controller in the redundant chassis has enough memory to store twice the amount of controller data and I/O memory. See Knowledgebase Technote, Understanding ControlLogix Redundancy Memory Usage .

EtherNet/IP Checklist

✓	Requirement
EtherNet/IP™ Module	
	Identical EtherNet/IP communication modules are placed in the same slot of both chassis of the redundant chassis pair.
	EtherNet/IP communication modules meet the requirements that are described in Communication Module Requirements .
EtherNet/IP Network	
	Produced and consumed tags meet the requirements that are described in Produced and Consumed Tags . Produced and consumed safety tags are not supported in Logix SIS redundancy.
	USB ports of communication modules in the redundant chassis are not used while the system is running (online).
	IP addresses of devices on the EtherNet/IP network are static and IP address swapping is enabled. Other IP address configurations are permitted, but require additional considerations. See IP Address Swapping .
	The partner EtherNet/IP communication modules must be able to communicate to each other over the Ethernet network.
EtherNet/IP HMI	
	Data server communication recovery time is the time during a switchover from primary to secondary, when tag data from the controller is unavailable for reading or writing. See Reduce Data Server Recovery Time .
	HMI meets the requirements that are described in HMI .

ControlNet Checklist for ControlLogix 5570 Redundancy

✓	Requirement
ControlNet® Module	
	Identical ControlNet modules are placed in the same slot of both chassis of the redundant pair.
	ControlNet modules are identical in redundancy firmware revision and in catalog number.
	ControlNet communication modules meet the requirements that are described in Communication Module Requirements .
	Partnered ControlNet modules both have identical keeper information as explained in the ControlNet Network Configuration User Manual, publication CNET-UM001 .
	Three connections of the ControlNet module are appropriately reserved for redundancy system use.
ControlNet Network	
	USB ports of communication modules in the redundant chassis are not used while the system is running (online).
	At least four ControlNet nodes are used on the ControlNet network. That is, at least two ControlNet nodes are on the ControlNet network along with the two ControlNet modules in the redundant chassis.
	These requirements apply to at least one ControlNet node: <ul style="list-style-type: none"> • It is not in the redundant chassis pair. • It uses a node address lower than the ControlNet node addresses of modules in redundant chassis pair.
	ControlNet module partners in the redundant chassis have the following: <ul style="list-style-type: none"> • Node address switches are set to the same address (for example, the switches of both modules are set to node address 13). • Two consecutive node addresses are reserved (for example, nodes 13 and 14) to accommodate a switchover. The primary ControlNet module can have an even or odd-numbered node address.
	The ControlNet network is scheduled by using techniques that are described in the ControlNet Network Configuration User Manual, publication CNET-UM001 .
	Devices on other communication networks are bridged to the ControlNet network appropriately.
ControlNet HMI	
	A ControlNet network or a ControlNet-to-EtherNet/IP gateway is used to connect to HMI because your system requires that HMI be updated immediately after a switchover. <ul style="list-style-type: none"> • PanelView™ Standard terminal, PanelView 1000e, or 1400e terminal For an unscheduled network, ≤ 4 HMI terminals per controller are used. For a scheduled network, any number of terminals within the limits of the ControlNet network are used. • PanelView Plus terminal, VersaView® industrial computer that runs a Windows® CE operating system FactoryTalk® Linx software, version 5.0 or later, is used. Within each controller and communication module, five connections for each PanelView Plus or VersaView terminal are reserved. • FactoryTalk View SE software with RSLinx® communication software, version 2.52 or later, FactoryTalk Linx software, version 5.0 The number of RSLinx servers that a controller uses is limited to 1..4 (maximum).

Project and Programming Checklist

✓	Requirement								
	The redundancy module date and time have been set by using the RMCT. This is not required, but recommended.								
	One project is created by using programming software and is downloaded to the primary controller.								
	Enable redundancy on the Redundancy tab of the Controller Properties dialog box. This is the only setting on the Controller Properties dialog box that is required for redundancy to function. The configurable settings on other tabs of the Controller Properties dialog box are optional, and not required for redundancy to function.								
	Time synchronization is not required for redundancy to function. If your application requires time synchronization, then do the following: <ul style="list-style-type: none"> • Enable time synchronization on the Date/Time tab of the Controller Properties dialog box. • Select Time Sync and Motion on the Module Definition dialog box for the Ethernet module that is in the local chassis. 								
	Task configuration is either: <ul style="list-style-type: none"> • One continuous task within the project. <li style="text-align: center;">or • Multiple periodic tasks with only one task at the highest priority. Also, multiple tasks are structured at all different priorities and periods so that the fewest possible separate tasks are used. 								
	The redundant controller program does not contain these tasks: <ul style="list-style-type: none"> • Event tasks • Inhibited tasks 								
	Programming for critical I/O that must be bumpless is placed in the highest-priority user task according to your task configuration. <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th style="text-align: center;">If you use this task structure</th> <th style="text-align: center;">Then programming for bumpless I/O is in</th> </tr> </thead> <tbody> <tr> <td>One continuous task</td> <td>The continuous task.</td> </tr> <tr> <td>One continuous task and one or more periodic tasks</td> <td>The highest-priority periodic task where only that one task is at the highest priority.</td> </tr> <tr> <td>Multiple periodic tasks</td> <td>The highest-priority periodic task where only that one task is at the highest priority.</td> </tr> </tbody> </table>	If you use this task structure	Then programming for bumpless I/O is in	One continuous task	The continuous task.	One continuous task and one or more periodic tasks	The highest-priority periodic task where only that one task is at the highest priority.	Multiple periodic tasks	The highest-priority periodic task where only that one task is at the highest priority.
If you use this task structure	Then programming for bumpless I/O is in								
One continuous task	The continuous task.								
One continuous task and one or more periodic tasks	The highest-priority periodic task where only that one task is at the highest priority.								
Multiple periodic tasks	The highest-priority periodic task where only that one task is at the highest priority.								
	To calculate watchdog time for ControlLogix 5580 controllers, see Set Minimum Values for Standard Task Watchdog Time .								
	Scan time is minimized by using these techniques when possible: <ul style="list-style-type: none"> • Unused tags are eliminated. • Arrays and user-defined data types are used instead of individual tags. • Redundancy data is synchronized at strategic points by using the Synchronize Data after Execution setting in the Program Properties dialog box. • Programming is written as compactly and efficiently as possible. • Programs are executed only when necessary. • Data is grouped according to frequency of use. 								
	For produced and consumed data, the communication module in the remote chassis that holds the consuming controller uses the Comm Format: None.								
	Critical messages from a remote chassis to a redundant chassis use cached connections.								
	Active tags on scan per controller are less than 10,000 tags/second.								
	Measure potential alarm bursts during system commissioning and modify the commissioned project if measured scan times are not acceptable								

Notes:

Module Replacement

To replace modules and update firmware in a redundancy system, you can use these methods:

- Method 1—Modules are replaced and firmware is updated while the redundancy system is powered up and the controllers are in RUN mode. To use this method, refer to the procedures in the appendix.
- Method 2—Modules are replaced while the redundancy system is powered down and the controllers are not in RUN mode. To use this method, perform the same steps as during initial setup. See [Chapter 5](#).

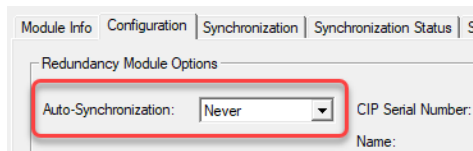
Perform a Direct Module Replacement in the Secondary Chassis

A direct module replacement in the secondary chassis requires the new module to have the same catalog number, series, and firmware.

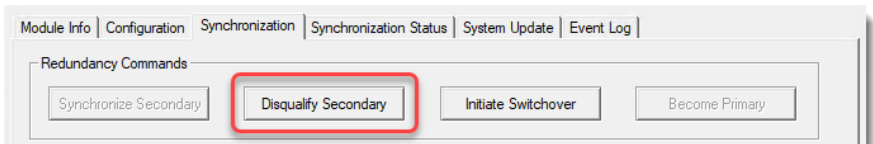
IMPORTANT When you replace communication modules, make sure that the rotary switches and port configuration match the existing modules.

To perform a direct module replacement in the secondary chassis, follow these steps.

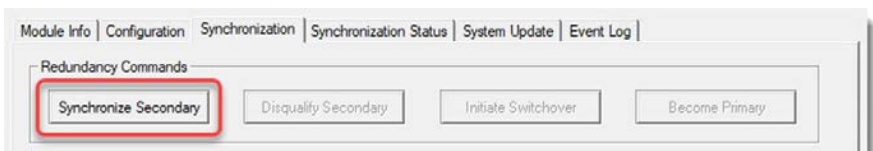
1. Access the RMCT for the redundancy module in either chassis.
2. On the Configuration tab, set Auto-synchronization to Never.



3. On the Synchronization tab, select Disqualify Secondary.



4. With the redundancy module fiber cables still connected, remove the module from the secondary chassis.
5. Insert the replacement module in the same slot in the secondary chassis.
6. If applicable, update the module firmware by using ControlFLASH Plus™ software.
7. On the Configuration tab of the RMCT, set Auto-synchronization to the original setting.
8. On the Synchronization tab, select Synchronize Secondary.



Replace Communication Modules with a New Series

This section describes how to replace EtherNet/IP™ communication modules with a new series without updating controller firmware.

You can replace communication modules with a new series by using these methods:

- Synchronization and switchover—Use this method if electronic keying is **not** set to Exact Match.
- Redundancy System Update (RSU)—Use this method if electronic keying is set to Exact Match. You must configure the new modules to use Exact Match. See [Chapter 14](#).

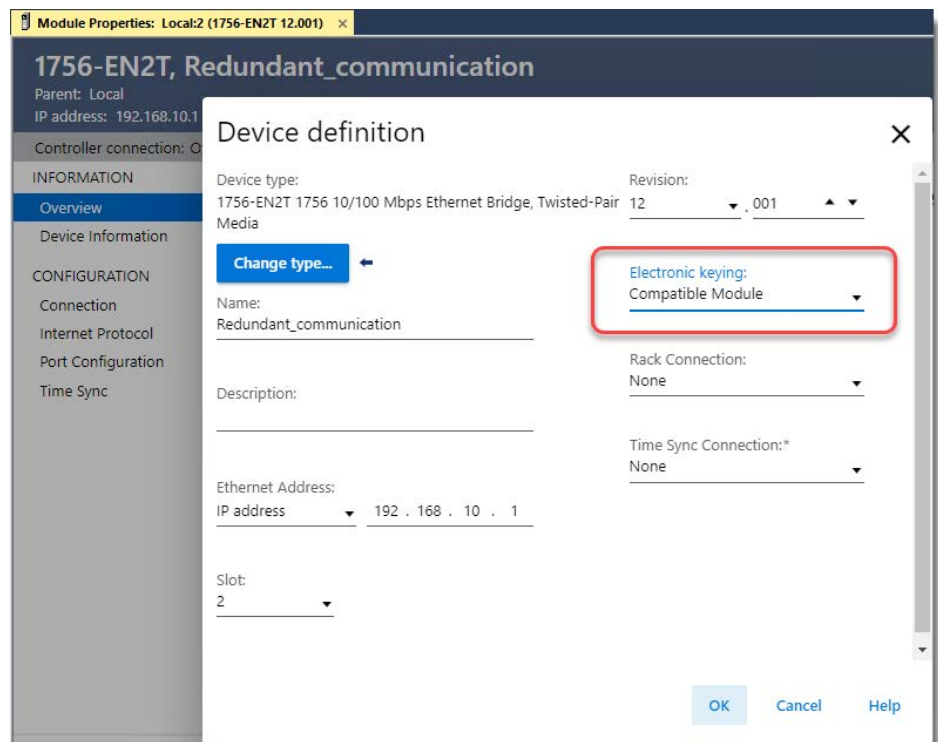
IMPORTANT

- Before you replace modules, make sure that you have the correct firmware for all new modules.
- When you replace modules, you must do so in pairs or the system cannot synchronize after a switchover.
- Partnered pairs of EtherNet/IP modules must use the same values for the following parameters for IP address swapping to work: IP addresses, network mask, gateway address

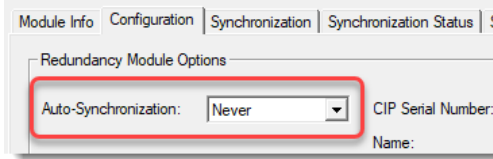
Synchronization and Switchover for Communication Module Series Replacement

If electronic keying is not set to Exact Match, follow these steps to replace communication modules with a new series.

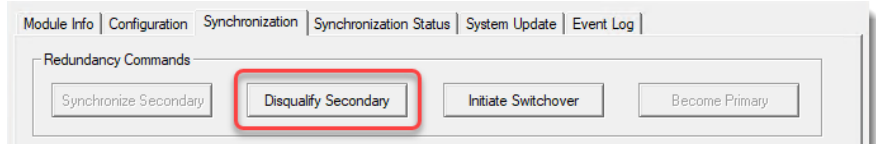
1. Make sure the existing modules and the new series modules use the same IP address, network mask, and gateway address.
2. Make sure that the RMCT version is compatible with your redundancy firmware.
3. Make sure that the redundancy module firmware is at the firmware revision for the specified bundle.
4. Go online with the primary controller.
5. For each module, verify that the Electronic Keying is set to Compatible Module or Disable Keying.



6. Access the RMCT for a redundancy module in either chassis
7. On the Configuration tab, set Auto-synchronization to Never.



8. Select Apply.
9. On the Synchronization tab, select Disqualify Secondary.



10. Make a note of the port configuration of the secondary communication module:
 - IP address
 - Network mask
 - Gateway address
11. Disconnect the Ethernet cables from the secondary communication module.
12. Turn off power to the secondary chassis.
13. Remove the communication module from the secondary chassis.
14. Set the switches on the new series communication module to 888, insert the module in the secondary chassis, and apply power to the chassis.
 - a. After the reset is complete, turn power off to the secondary chassis and remove the module from the secondary chassis.
 - b. Set the switches to the same settings as on the module that was removed.
 - c. Reinsert the module into the secondary chassis, reattach the cable, and apply power to the secondary chassis.
 - d. To support bridging across the backplane or USB port, configure the port configuration of the secondary module to match the port configuration of the primary module.
15. Update the firmware of the new communication module.
16. After the update completes, connect the Ethernet cable to the secondary communication module and wait for communication to resume on the network.
17. Repeat steps [10](#)...[15](#).

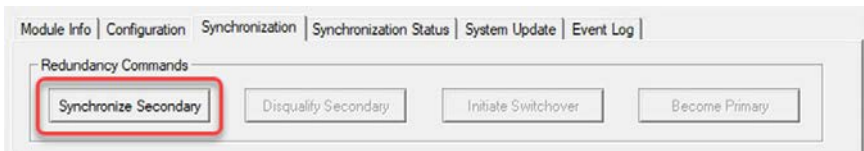
Verify Module Compatibility and Synchronization

To verify module compatibility and synchronization, follow these steps.

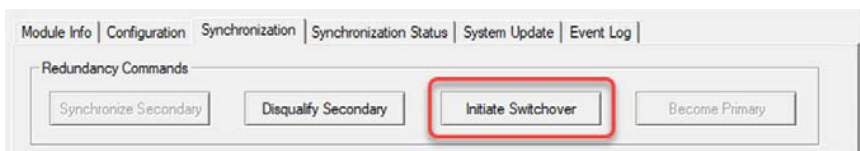
1. On the Synchronization Status tab of the RMCT, verify that the modules are fully compatible.

Slot	% Complete	Module Name	Module Revision	Secondary Readiness	State	Compatibility
0	0	1756-L85E/B	37.11	Disqualified	Primary	Full
1	0	1756-EN2TR/C	7.1	Disqualified	Primary	Full
2	0	CLX Redundancy Premium Mod...	21.11	Disqualified	Primary	Full
3	---	<empty>	---	---	---	---
4	---	<empty>	---	---	---	---
5	---	<empty>	---	---	---	---
6	---	<empty>	---	---	---	---

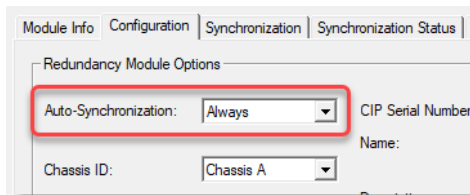
2. On the Synchronization tab, select Synchronize Secondary.



3. Wait for the synchronization to complete.
4. On the Synchronization tab, select Initiate a switchover.



5. Disconnect the Ethernet cables from the communication module in the secondary chassis.
6. Turn off power to the secondary chassis.
7. Remove the communication module from the secondary chassis.
8. Set the switches on the new series module to 888 and insert it in the secondary chassis.
 - a. After the reset is complete, remove the module from the secondary chassis.
 - b. Set the switches to the same settings as on the module that was removed.
 - c. Reinsert the module into the secondary chassis, reattach the cable, and apply power to the secondary chassis.
 - d. To support bridging across the backplane (or via the USB port), configure the Port Configuration of the secondary module to match the Port Configuration of the primary module.
 - e. Update the firmware of the new series module.
9. Repeat the steps 5...8 for all EtherNet/IP modules in secondary chassis.
10. On the Configuration tab of the RMCT, set Auto-synchronization to Always.



11. Select Apply, Yes, and OK.
12. Verify that the secondary chassis has qualified.

Replace Redundancy Modules with a New Catalog Number

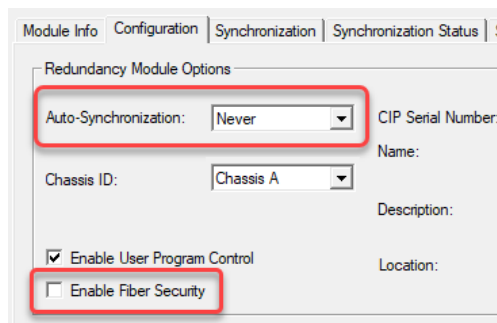
Partner redundancy modules must have the same catalog number, series, and firmware. To change the catalog number of a redundancy module, you must replace both partner modules with the same catalog number. For example, replace a pair of 1756-RM2 modules with a pair of 1756-RM3 modules. A switchover is not required to replace a redundancy module pair.

To replace a redundancy module in the secondary chassis with a new module that has the same catalog number, series, and firmware, see [Perform a Direct Module Replacement in the Secondary Chassis](#).

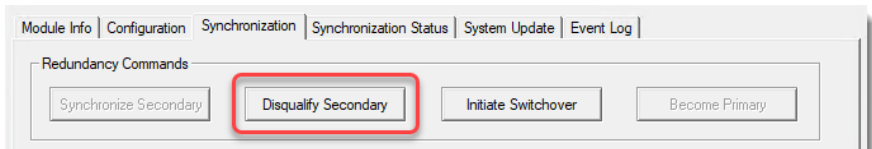
To replace redundancy modules with a new catalog number, follow these steps.

1. Access the RMCT for the redundancy module in the primary chassis.
2. On the Configuration tab, set the following redundancy module options:
 - Set Auto-synchronization to Never.
 - Disable fiber security, if applicable

IMPORTANT Replacing a module while fiber security is enabled can result in system performance issues, including a loss of control.



3. On the Synchronization tab, select Disqualify Secondary.

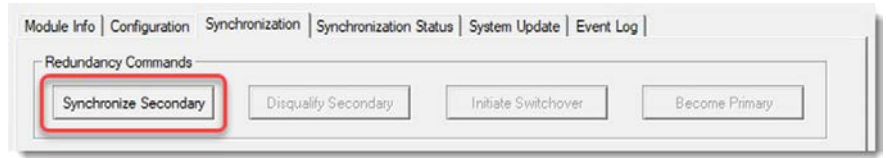


4. Unplug the fiber cables from both of the redundancy modules.
5. Close any open RMCT sessions that are connected to the redundancy modules.
6. Remove both redundancy modules in any order from the redundant chassis pair.
7. Insert the new primary redundancy module into the same slot in the primary chassis.
8. Wait for the status message 'PRIM' to appear on the front panel of the primary redundancy module.
9. Before inserting the new secondary redundancy module, reconnect the fiber cables between the new redundancy modules.
10. Insert the new secondary redundancy module into the same slot in the secondary chassis.
11. If not already installed, upload the EDS files for the redundancy modules.
For more details, see [EDS Files](#).
12. Update the firmware for the redundancy module in the secondary chassis.

IMPORTANT To maintain the crossload communication path between redundant modules during the update process, you must update the redundancy module firmware in the secondary chassis before the primary chassis.

13. Update the firmware for the redundancy module in the primary chassis.
14. Access the RMCT for the redundancy module in the primary chassis.

- 15. On the Configuration tab, set Auto-synchronization and fiber security to the original settings.
- 16. On the Synchronization tab, select Synchronize Secondary.



Install Earlier Redundancy Firmware Bundles

This appendix describes how to install redundancy firmware bundles earlier than version 34.xxx_kit1. For bundles 34.xxx_kit1 and later, see [Download Redundancy Firmware](#).

Create a firmware directory on your computer first, so you can extract the firmware files to the directory.

1. Shut down the communication software.
2. Browse to the location of the redundancy firmware revision ZIP file.
3. Extract the redundancy firmware bundle to your computer.

After you extract the files, you will have the following:

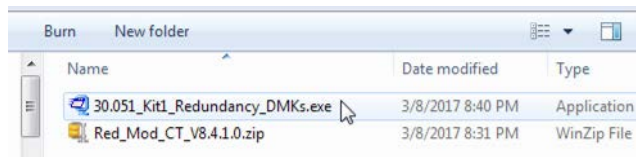
- DMK file for the firmware revision you downloaded
- Redundancy Module Configuration Tool ZIP file

4. Extract the Redundancy Module Configuration Tool to your computer.

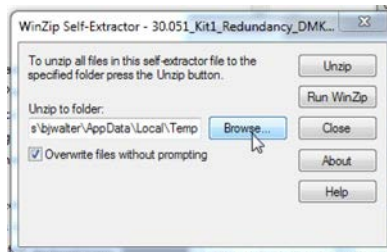
Install Bundles 30.051_kit1 and 24.053_kit1

Create a firmware directory on your computer first, so you can extract the firmware files to the directory.

1. Shut down the communication software.
2. Browse to the location of the redundancy firmware kit.
3. Extract the redundancy firmware bundle on your computer.
4. Browse to the directory on your computer that has the redundancy firmware bundle, and extract the Redundancy Module Configuration Tool to your computer.
5. Browse to the directory on your computer that has the redundancy firmware kit, and double-click xxx_Redundancy_DMKs.exe.



6. On the WinZip Self-Extractor dialog box, select Browse and choose the location to install the files.

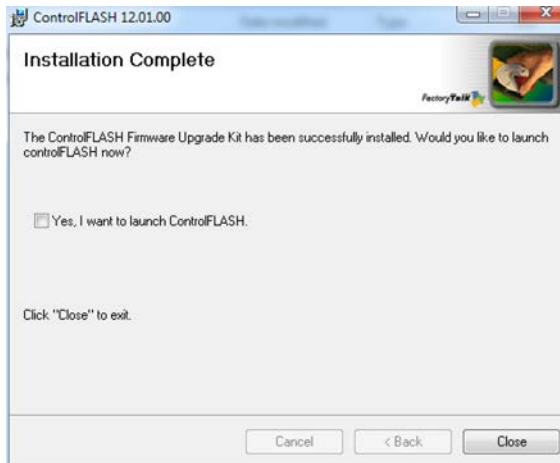


7. After you choose your location, select Unzip.
8. On the installation successful dialog box, select OK.
9. On the WinZip Self-Extractor dialog box, select Close.

Install Bundle 24.052_kit1

Create a 24.052 firmware directory on your computer first, so you can extract the firmware files to the directory.

1. Shut down the communication software.
2. Browse to the location of the redundancy firmware revision 24.052_kit1
3. Extract the redundancy firmware kit on your computer.
4. Browse to the directory on your computer that has the redundancy firmware bundle, and extract the Redundancy Module Configuration Tool version 8.3.1.0 on your computer.
5. Browse to the directory on your computer that has the redundancy firmware kit, and double-click ControlFlash.msi.
6. When the installation is complete, a dialog box appears.
7. Clear the Yes, I want to launch ControlFLASH™ checkbox.



8. Select Close.

ControlLogix 5560 Redundancy Considerations

Later controllers scan the controller program faster than ControlLogix® 5560 controllers. If you use ControlLogix 5560 redundancy and your application needs better controller performance, we recommend that you use ControlLogix 5580 controllers.

ControlLogix 5560 Controllers in Redundant Chassis

Remember these points when you place ControlLogix 5560 controllers in a redundant chassis:

- ControlLogix 5560 controllers are not compatible with 1756-RM3 redundancy modules.
- With ControlLogix 5560 redundancy, firmware revision 16.081 or earlier, you cannot use two 1756-L64 controllers in the same chassis. However, you can use a 1756-L64 controller in the same chassis as a 1756-L61, 1756-L62, or 1756-L63 controller.
- Each ControlLogix 5560 controller must have enough data memory to store twice the amount of tag data that is associated with a redundant controller project.
- When you use the Redundancy System Update (RSU) feature to update a redundancy system while the system continues operation, the updated controllers must provide the same or greater memory than the existing controllers.

This table describes the controllers to which you can upgrade, based on the existing controller that is used, when using RSU.

Existing	New Controller
1756-L61	1756-L61, 1756-L62, 1756-L63, 1756-L64, 1756-L65
1756-L62	1756-L62, 1756-L63, 1756-L64, 1756-L65
1756-L63	1756-L63, 1756-L64, 1756-L65
1756-L64	1756-L64, 1756-L65
1756-L65	1756-L65

Plan for Controller Connections

Consider these conditions when you plan controller connection use:

- ControlLogix 5560 controllers provide 250 total connections.
- If you use the redundant controller at, or very near the connection limits, you can experience difficulty synchronizing your chassis.

Estimate Crossload Times

Use this equation to estimate the crossload time of ControlLogix 5560 controllers for each program after you have either of the following:

- The size of the last data transfer
- The maximum size of data that is transferred

$$\text{Crossload time per sync point (ms)} = (\text{DINTs} * 0.00091) + 0.6 \text{ ms}$$

Set Watchdog Time

To set Watchdog time for ControlLogix 5560 controllers, use this table to determine which equation to use to calculate the time for each task.

Network	Equation
ControlNet® I/O ms	$(2 * \text{maximum_scan_time}) + 150$
EtherNet/IP™ I/O ms	$(2 * \text{maximum_scan_time}) + 100$

The *maximum_scan_time* is the maximum scan time for the entire task when the secondary controller is synchronized.

Instruction Based Alarms (IBA)

ControlLogix 5560 supports up to 250 IBAs with 250 burst. For more information, see the Knowledgebase Technote, [Studio 5000 & ControlLogix: ALMA/ALMD instructions limits](#).

Firmware Updates and System Time

If you use the Redundancy System Update (RSU) feature to update a redundancy system with firmware revision **16.081 or earlier**, which uses Coordinated System Time (CST), the redundancy system, revision 19.052 or later, does not permit a locked switchover and the update fails to complete.

To work around this restriction, first disable CST Mastership in the original redundancy system and then use RSU to update the redundancy system to revision 19.052 or later.

Convert from a Non-redundant System

To convert a non-redundant system to ControlLogix 5560 redundancy, refer to the following redundancy firmware compatibility information.

For details about converting from a non-redundant system, see [Appendix H](#).

Table 70 - Compatible Redundancy Firmware Revisions for ControlLogix 5560 Controllers

Cat. No.	24.05x or later	19.5x, 20.05x	16.08x
1756-L61, 1756-L62, 1756-L63, 1756-L63XT, 1756-L64	No	Yes	Yes
1756-L65	No	Yes	No

ControlNet Considerations

ControlNet Modules in Redundant Chassis

Remember the following when you use ControlNet® communication modules in a redundant chassis pair:

- For a ControlNet network in a redundant chassis pair, you must have two ControlNet communication modules outside of the redundant chassis pair. When you assign node address numbers, assign the lowest node number address to a ControlNet communication module outside of the redundant chassis pair.

For more information, see [Use at Least Four ControlNet Network Nodes through Assign Lowest Node Numbers to Remote ControlNet Modules](#).

- You cannot use Series A ControlNet communication modules in a redundancy system.

Plan for Communication Module Connections

ControlNet communication modules provide 131 CIP™ connections:

- Three of the 131 CIP connections are reserved for redundancy. The three redundancy CIP connections always appear to be in use, even when no connections are open.
- You can use the remaining 128 CIP connections in any manner that your application requires.

Bridge from an EtherNet/IP Network to a ControlNet Network

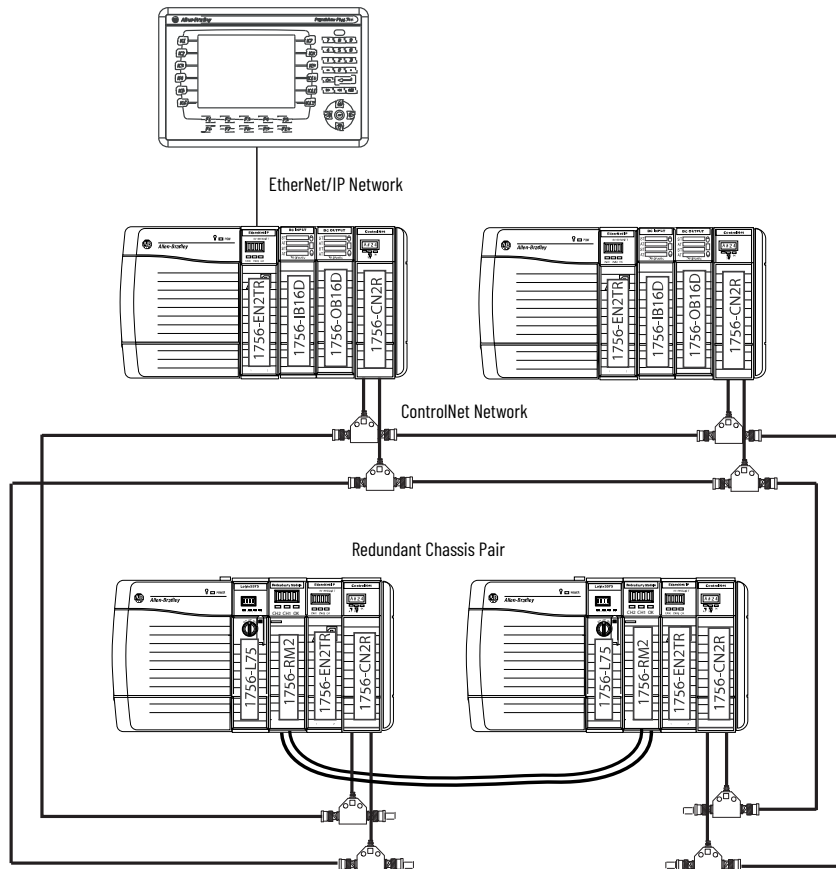
To maintain the connection between a component and a redundant chassis pair during a switchover, you can bridge from an EtherNet/IP™ network to a ControlNet network.

IMPORTANT Redundancy firmware bundles earlier than 30.051 do not support bridging from an EtherNet/IP network to a ControlNet network. I/O connections are not supported in any bridge configurations in any version.

See [Possible Communication Delays During a Switchover](#).

The following illustration shows the recommended method to connect an HMI to a redundant chassis pair to avoid connection drops. In this example, the remote chassis contains I/O modules and the EtherNet/IP and ControlNet communication modules. The I/O modules are not required and are shown for example only. For all requirements, see [ControlNet Configuration Considerations](#).

Figure 72 - Configuration Used to Help Prevent Communication Delays on Switchover



ControlNet Configuration Considerations

ControlNet networks are used to connect a redundant chassis pair to remote I/O and to other devices in the system.

IMPORTANT A remote chassis can be accessed over a ControlNet network that uses any ControlNet module that works in a non-redundant chassis with no additional firmware requirement.

If you use a ControlNet network in your redundancy system, be aware of the following configuration considerations:

- Use at least four ControlNet network nodes.
- Assign the lowest node numbers to remote ControlNet modules.
- Set partnered ControlNet module switches to the same address.
- Reserve consecutive node addresses for partner modules.

Use at Least Four ControlNet Network Nodes

At least four ControlNet network nodes are required per ControlNet network in a redundancy system. This configuration is required because two or more ControlNet nodes must be used with the two ControlNet modules that are used in the redundant chassis pair. One of the two nodes outside of the redundant chassis pair must be at a lower node address than the ControlNet modules in the redundant chassis pair.

If your ControlNet network uses fewer than four nodes and a switchover occurs, connections can drop and outputs connected to that node can change state during the switchover.

You can include these ControlNet modules and redundant ControlNet nodes:

- ControlNet bridges in remote chassis
- Any other ControlNet devices on the ControlNet network
- A workstation running communication software that is connected via a ControlNet network

For more information, see Knowledgebase Technote [ControlNet Network Keeper and ControlLogix Redundancy](#).

Assign Lowest Node Numbers to Remote ControlNet Modules

Do not assign the lowest ControlNet node addresses to ControlNet modules in the redundant chassis pair.

If you assign the lowest ControlNet node addresses to ControlNet modules in the redundant chassis pair, you can experience these system behaviors:

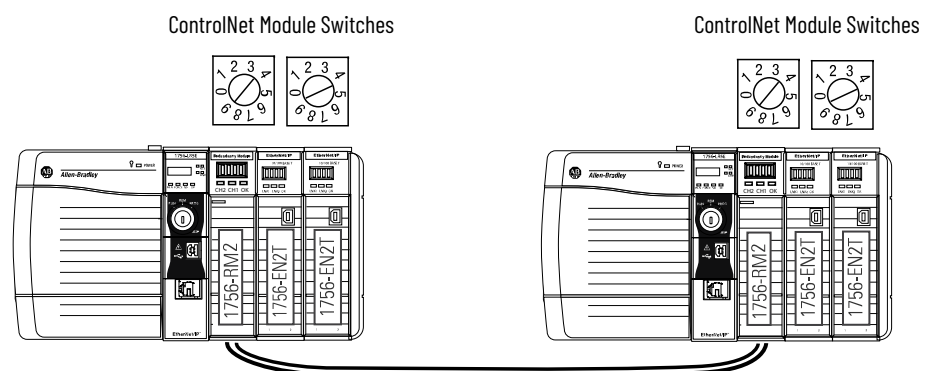
- Upon a switchover, you can lose communication with I/O modules, produced tags, and consumed tags.
- If you remove a ControlNet module from the redundant chassis, it can result in lost communication with I/O modules, produced tags, and consumed tags.
- If the entire system loses power, you can be required to cycle power to the primary chassis to restore communication.

Set Partnered ControlNet Module Switches to the Same Address

Where ControlNet modules are used as partners in a redundant chassis pair, you must set the node address switches to the same node address. The primary ControlNet modules can be at even or odd node addresses.

For example, if partnered ControlNet modules are assigned to nodes 12 and 13 of the ControlNet network, set the node address switches of the modules to the same address of 12.

Figure 73 - Example of Switch Address for Partnered ControlNet Modules

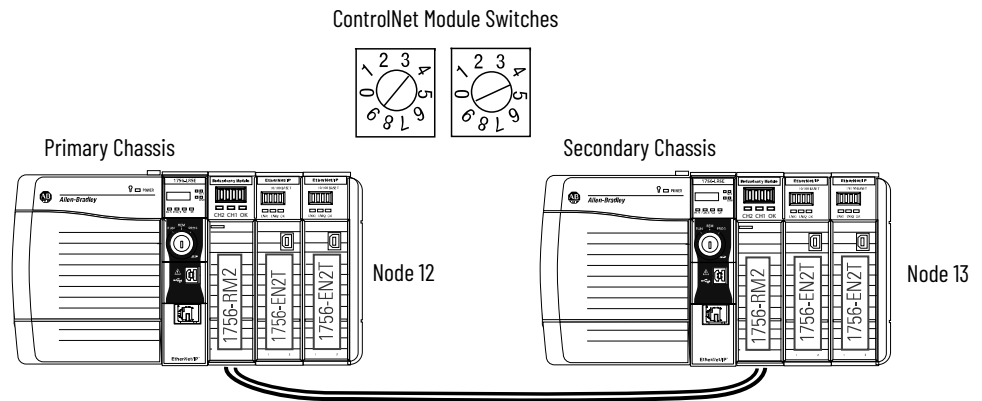


Reserve Consecutive Node Addresses for Partner Modules

Partnered ControlNet modules in a redundant chassis pair must have consecutive node numbers. Plan for consecutive node addresses because the redundancy system automatically assigns the consecutive node address to the secondary ControlNet module.

For example, partnered ControlNet modules with address switches set at 12 are assigned ControlNet node numbers 12 and 13 by the system. The primary chassis always assumes the lower of the two node addresses.

Figure 74 - Example of Redundant ControlNet Modules at Consecutive Addresses

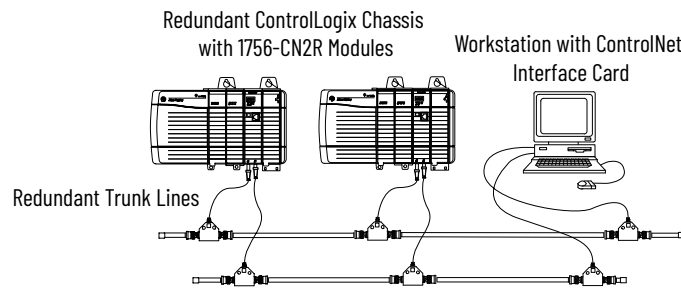


Redundant ControlNet Media

The use of redundant ControlNet media helps to prevent a loss of communication if a trunkline or tap is severed or disconnected. A system that uses redundant ControlNet media uses these components:

- 1756-CN2R, series B or later, communication modules in each redundant chassis
- ControlNet modules that are designed for redundant media at each ControlNet node on the network
- Redundant trunk cabling
- Redundant tap connections for each ControlNet module connected

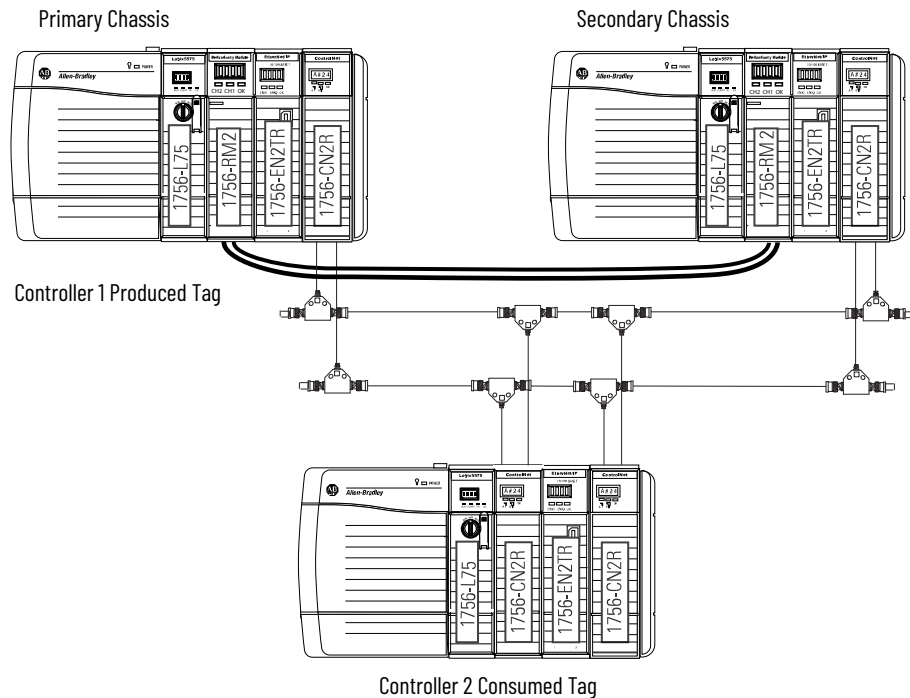
Figure 75 - Redundant ControlNet Media with Redundant ControlLogix Chassis



Produce/Consume Connections

You can use produce/consume connections over a ControlNet network. Controllers let you produce (broadcast) and consume (receive) system-shared tags.

Figure 76 - Example System Using Produced and Consumed Tags



Consider the following for produced and consumed connections over a ControlNet network in a redundancy system:

- During a switchover, the connection for tags that are consumed from a redundant controller can drop briefly:
 - The data does not update.
 - The logic acts on the last data that was received.

After the switchover, the connection is re-established and the data begins to update again.

- You cannot bridge produced and consumed tags over two networks. For two controllers to share produced or consumed tags, both must be attached to the same network.
- Produced and consumed tags use connections in both the controllers and the communication modules being used.
- Because produced and consumed tags use connections, the number of connections available for other tasks, such as the exchange of I/O data, is reduced.

The number of connections available in a system depends on the controller type and network communication modules used. Closely track the number of produced and consumed connections to leave as many as necessary for other system tasks.

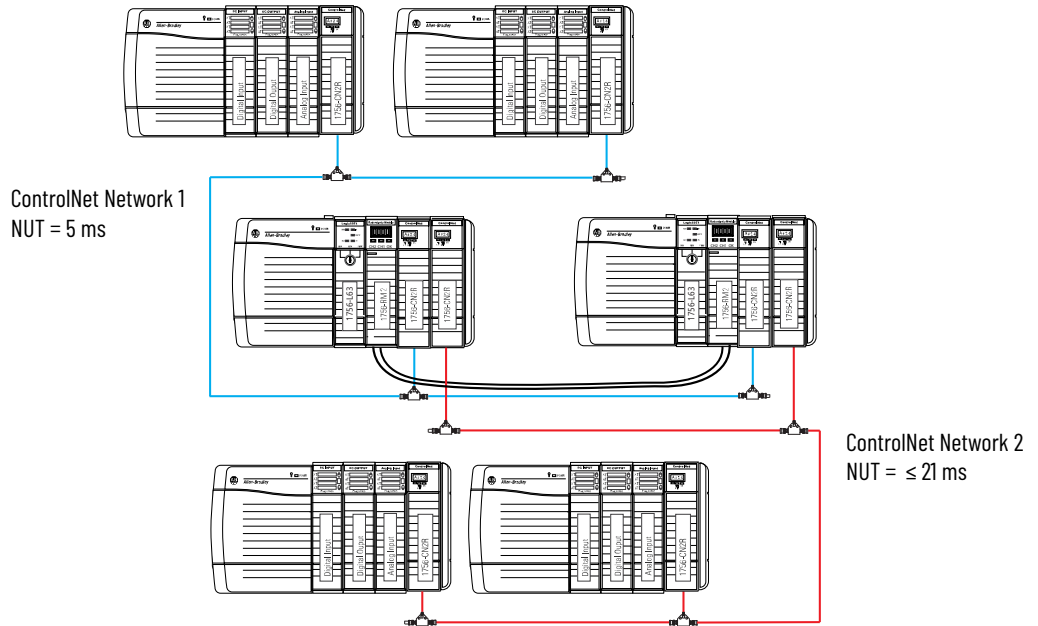
Network Update Time

The network update time (NUT) that you specify for the redundancy system affects performance and switchover response time. Typical NUTs used with redundant systems range from 5...10 ms.

NUTs with Multiple ControlNet Networks

You can choose to use multiple ControlNet networks with your redundancy system.

Figure 77 - Example of Two ControlNet Networks



When you use multiple ControlNet networks, the networks must use compatible NUTs. Compatible NUTs are determined based on the network that uses the smallest NUT.

Use the following table to determine the compatible NUTs for your system.

Table 71 - Compatible NUT Values for Multiple ControlNet Networks

Smallest NUT of Network (ms)	Largest NUT of Other Networks Must Be ≤ (ms)
2	15
3	17
4	19
5	21
6	23
7	25
8	27
9	29
10	31
11	33
12	35
13	37
14	39
15	41
16	43
17	46
18	48
19	50
20	52

Table 71 - Compatible NUT Values for Multiple ControlNet Networks (Continued)

Smallest NUT of Network (ms)	Largest NUT of Other Networks Must Be ≤ (ms)
21	55
22	57
23	59
24	62
25	64
26	66
27	68
28	71
29	73
30	75
31	78
32	80
33	82
34	84
35	87
36	89
37...90	90

Scheduled or Unscheduled Network

Determine whether to use a scheduled or unscheduled network.

Use a Scheduled Network

Schedule or reschedule your ControlNet network when you execute these tasks:

- Commission a new redundant system.
- Add a chassis of remote ControlLogix® I/O that is set to use the Rack Optimized communication format.
- Add any remote I/O besides ControlLogix I/O. For example, if you add FLEX™ I/O modules, you must schedule the network.
- Use produced/consumed data. If you add a produced/consumed data tag, you must reschedule the ControlNet network.

To schedule or reschedule your ControlNet network, you put your redundant system in Program mode.

Use an Unscheduled Network

You can use an unscheduled network when you:

- Add a remote I/O chassis of ControlLogix I/O that does not use the Rack Optimized communication format. That is, direct connections to the I/O are used.
- Add a ControlLogix I/O module to a chassis that has already been scheduled and uses the Rack Optimized communication format.
- Add some drives that support adding I/O while online.
- Use ControlNet to monitor HMI or the controller program execution online.

You can add those components to the unscheduled network while your redundant system is online and in Run mode. We recommend that you do not use an unscheduled network for all of your I/O connections.

The use of 1756-CN2, 1756-CN2R, and 1756-CN2RXT modules provide increased capacity for adding I/O while online compared to 1756-CNB or 1756-CNBR modules. With this increased capacity, you can easily add I/O and increase ControlNet connections that are used without affecting your redundant system performance.

Add Remote ControlNet Modules While Online

If you are adding a remote I/O chassis that is composed of a ControlLogix ControlNet module and ControlLogix I/O while your redundant system is running (online), make these considerations:

- Do not use Rack Optimized communication formats. The ControlNet module and I/O must be configured for direct connections.
- For each remote I/O module used, plan for one direct connection to be used.

ControlNet Module CPU Usage

The CPU usage of the ControlNet modules must be at 80% or less. CPU usage below 80% reserves enough CPU functionality for the ControlNet module to facilitate a switchover.

If the CPU usage is above 80%, the secondary chassis can fail to synchronize with the primary chassis after a switchover occurs. In addition, unscheduled communication can be slowed.

If you must reduce the CPU usage of your ControlNet modules, consider making the following changes:

- Increase the Network Update Time (NUT) of the ControlNet network.
- Increase the Requested Packet Interval (RPI) of your connections.
- Reduce the number of connections through the ControlNet modules.
- Reduce the number of messages that are used in the program.

ControlNet Module Connections Used

If the connections used by ControlNet modules are near the limits, you can experience difficulty when attempting to go online with the system. This difficulty arises because going online with a controller also consumes a connection. You can also experience difficulty when attempting to add modules to the system.

Monitor the ControlNet Network

For most applications, monitoring the status of the ControlNet network is important for maintenance and troubleshooting. For programming samples to monitor the ControlNet network, visit the [Sample Code Library](#). Applicable sample programs include the following:

- ME Faceplates for ControlNet Diagnostics
- ControlNet Connection and Media Status

Keeper Status Causing Synchronize Failure

To determine if a keeper status anomaly is causing a synchronization failure, you can view the status display on the front of the ControlNet modules. You can also check the keeper status by using RSNetWorx™ for ControlNet software.



To avoid anomalies with the Keeper Status, always reset the ControlNet module configuration of a module being used as a replacement **before** inserting and connecting the module in a ControlNet network.

Check the Module Status Display

If the status display of a ControlNet module in the redundant chassis pair indicates these errors, you must take corrective action:

- Keeper: Unconfigured
- Keeper: Unconfigured (data format changed)
- Keeper: Unconfigured (slot changed)
- Keeper: Unconfigured (net address changed)
- Keeper: Signature Mismatch
- Keeper: None Valid on Network

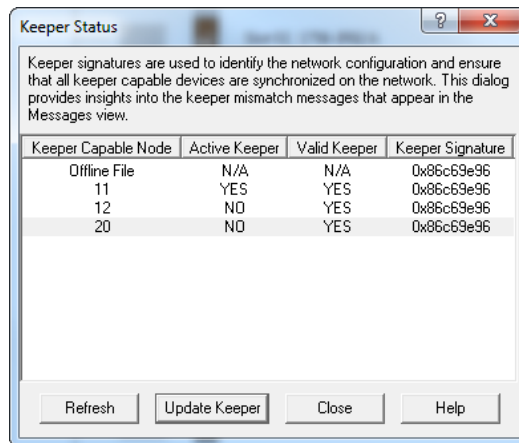
Check Keeper Status in RSNetWorx for ControlNet Software

To check the status of keepers on the ControlNet network, open RSNetWorx for ControlNet access the Keeper Status from the Network menu.

Valid Keepers and Signatures

This example shows a Keeper Status dialog box where the ControlNet network is composed of valid keepers and signatures.

Figure 78 - Valid Keeper Status and Signatures

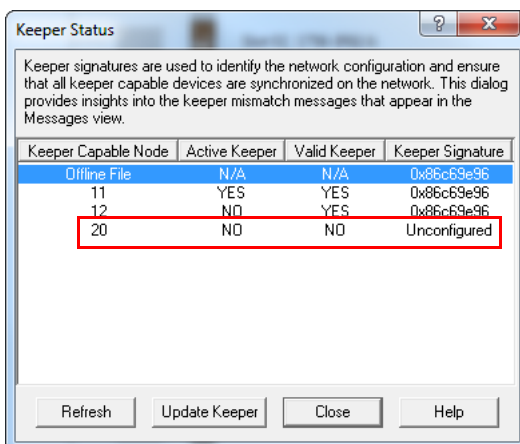


Unconfigured Keeper

The following example shows the Keeper Status dialog box where a module has an unconfigured status. Besides the status that is shown, the module status display indicates Keeper: Unconfigured (node address changed).

This error results when the node address of the module has been changed. After changing the node address, the module was used as a replacement and inserted into the redundant chassis.

Figure 79 - Keeper Status - Unconfigured



To correct this anomaly, do one of the following:

- Select the unconfigured module and select Update Keeper.
- Reschedule the ControlNet network.

Keeper Signature Mismatch

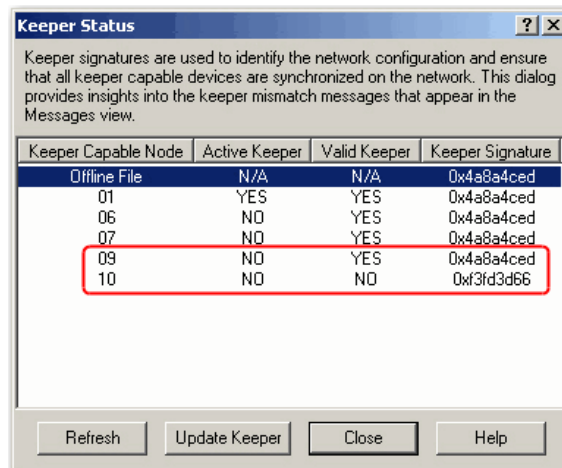
This example shows ControlNet modules in the redundant chassis that do not have the same keeper signatures. With this anomaly, the ControlNet module display indicates Keeper: Signature Mismatch.

This anomaly can occur if a ControlNet module that is configured for the same node of another network replaces a ControlNet module with the same node address in the redundant chassis.

To **correct** this anomaly, do one of the following:

- Select the unconfigured module and select Update Keeper.
- Reschedule the ControlNet network.

Figure 80 - Keeper Status - Signature Mismatch



Replace a 1756-CN2 Module with a New Series

You can replace the 1756-CN2/B modules with 1756-CN2/C modules by using the following methods:

- Synchronization and switchover for the ControlNet modules
Use this method if Electronic Keying is set to Disable or Compatible Module.
- Redundancy system firmware update
Use this method if Electronic Keying is set to Exact Match.

IMPORTANT

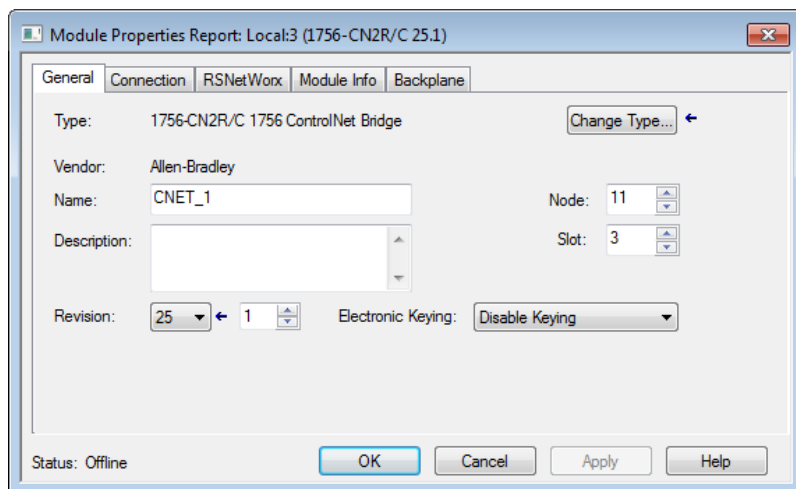
- Before you replace modules, verify that you have the correct firmware for all modules.
- You must replace and update module in pairs so that the system can synchronize after a switchover.
- Replace 1756-CN2/B modules with 1756-CN2/C modules and 1756-CN2RXT/B modules with 1756-CN2RXT/C modules.

Synchronization and Switchover for the ControlNet Modules

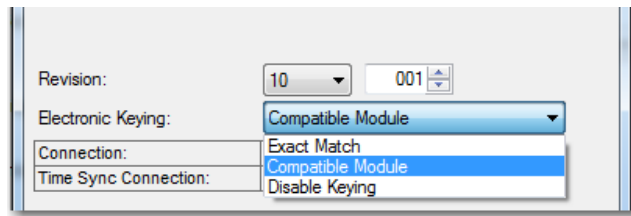
Complete these steps to replace ControlNet modules.

1. Add the EDS files for the modules.
2. Note of the Node configuration of the ControlNet module.

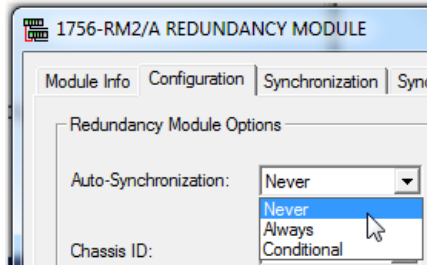
In this example, the primary ControlNet node is configured as Node 11. The Node value of the secondary ControlNet module must have the same value as the primary module.



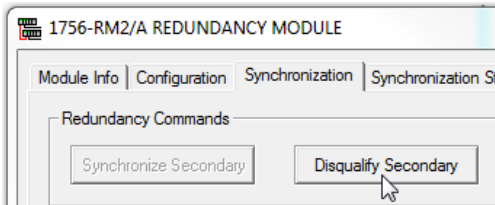
3. Make sure that your version of the Redundancy Module Configuration Tool (RMCT) is compatible with your redundancy firmware bundle.
4. Make sure that the firmware revision of your redundancy module is compatible with your redundancy firmware bundle.
5. Go online with the primary controller.
6. For each module, verify that Electronic Keying is set to Compatible Module or Disable Keying.



7. In RSLinx Classic software, start the RMCT for the redundancy module in the primary chassis.
 - a. Start RSLinx Classic Software.
 - b. Select Communications and choose RSWho.
 - c. Open the branches of your network until you find the redundancy module in the primary chassis.
 - d. Right-click the redundancy module, and choose Module Configuration.
8. On the Configuration tab, select Never for the Auto-Synchronization setting.

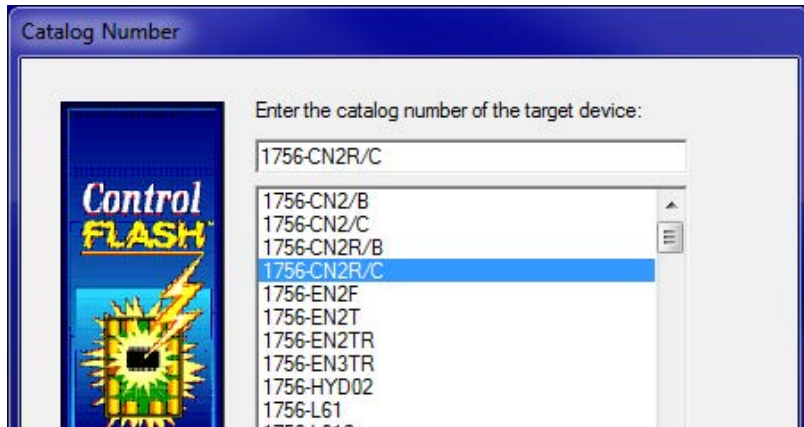


9. Select Apply and then Yes.
10. On the Synchronization tab, select Disqualify Secondary and then select Yes.

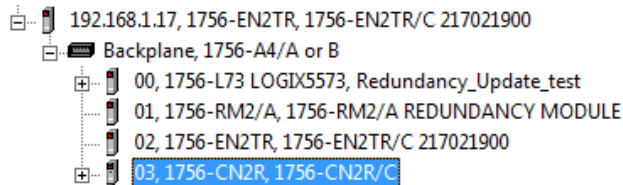


11. Disconnect the coaxial cables from the secondary ControlNet module.
12. Remove the original ControlNet module from the secondary chassis.
13. Set the switches in the new module to 00 and insert the module into the secondary chassis.
14. After the reset is complete in the new ControlNet module, remove the module from the secondary chassis.
15. Set the switches in the new ControlNet module to the correct Node value and reinsert the module into the secondary chassis.
16. Reconnect the coaxial cable to the new secondary ControlNet module.

17. Update the firmware of the ControlNet module in the secondary chassis.
 - a. If necessary, complete the following steps to update module firmware.
 - b. Launch ControlFLASH software, and select Next.
 - c. Select the ControlNet module catalog number and select Next.



- d. Browse to the module and select it.



- e. Select OK.
- f. Select the firmware revision to update to and select Next.
- g. Select Finish.

The firmware begins to update. When the update is complete, the Update status dialog box indicates completion.

Wait for the update to complete.

18. Wait for communication to resume on the network.
19. Verify that the Synchronization Status tab indicates that the modules are fully compatible.
20. On the Synchronization tab, synchronize the secondary chassis.

Wait for synchronization to complete.
21. Initiate a switchover.
22. Remove the ControlNet modules from the new secondary chassis.
23. Make sure to match the node address of replacing the ControlNet module with existing module.
24. Insert the ControlNet module into the new secondary chassis, reconnect the module to the network, and turn on power to the chassis.
25. If you have not already done so, update the firmware of the ControlNet module in the primary chassis.

Complete these steps to verify module compatibility and synchronization.

1. In the RMCT, from the Auto-Synchronization pull-down menu, choose your preferred method.
2. If necessary, manually synchronize the chassis.
3. Select Apply, Yes, and OK.
4. Verify that the secondary chassis has qualified.

Notes:

Convert from a Non-redundant System

Before you convert from a non-redundant to a redundant system, make sure that your controller firmware revision supports redundancy. For controller firmware requirements, see [Table 4](#).

Also consider the following:

- The redundant chassis pair has controller, communication module and I/O module restrictions.
- The program scan time can increase because of the additional time required for crossloading.

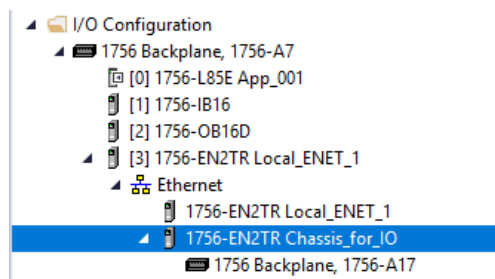
For more information, see Replacement Guidelines: Logix 5000 Controllers Reference Manual, publication [1756-RM100](#).

Update the Configuration in the Logix Designer Application

These steps provide an overview of the process that is required to update the I/O Configuration tree in the Logix Designer application.

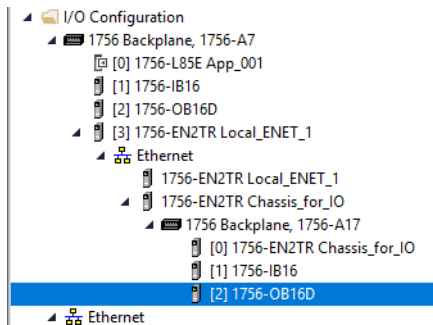
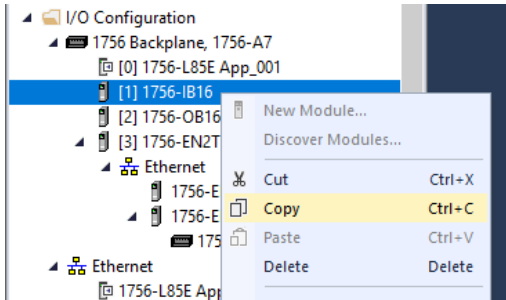
IMPORTANT Do not place I/O modules in a redundant chassis.

1. If you have I/O modules in the chassis with the controller, add an EtherNet/IP™ communication module.
1756-EN3TR communication modules are not supported in a redundant chassis.
2. Because I/O modules must be in a separate chassis, add another EtherNet/IP adapter under the adapter you added.

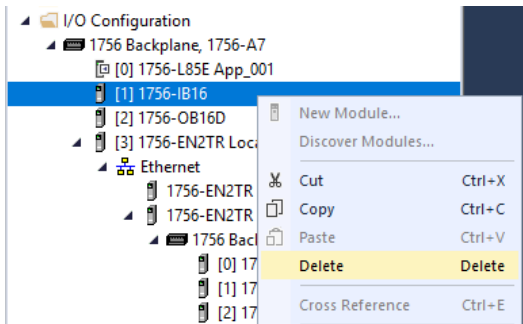


You can now move the I/O modules to the new chassis in the I/O Configuration tree.

- Copy the I/O modules and paste them into the chassis of the newly added communication module.



- Delete the I/O modules from the controller chassis configuration.

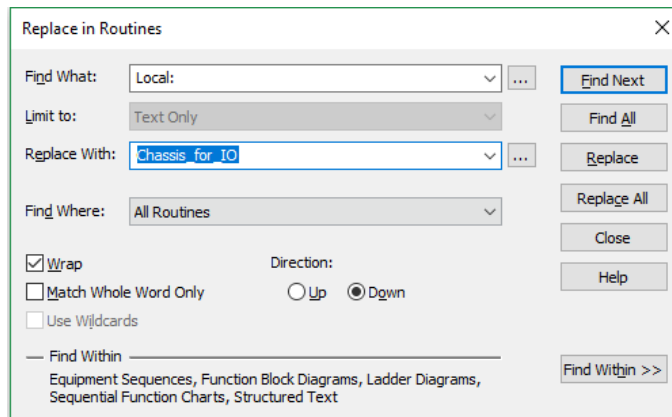


- Because the front Ethernet port of the controller is disabled once you enable the controller for redundancy, you must first move any remote communication from the front port to an EtherNet/IP module in the local chassis.
- Continue by completing the following procedures:
 - [Replace Local I/O Tags](#)
 - [Replace Aliases to Local I/O Tags.](#)

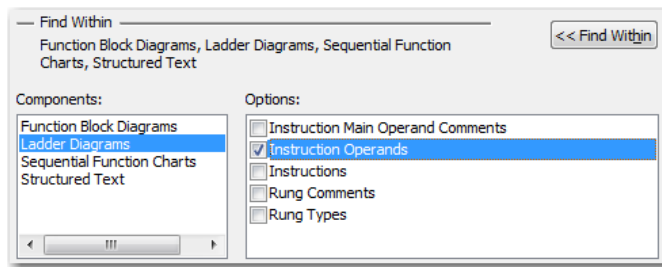
Replace Local I/O Tags

If you have moved I/O modules out of the local controller chassis and into the remote I/O chassis, complete these steps to find and replace the local I/O tags in your program.

1. Open the routine where the local I/O tags must be updated.
2. Press CTRL+H to open the Replace in Routines dialog box.



3. In the Find What field, select Local.
4. In the Replace With field, select the name of the communication module where the remote I/O was placed.
5. In the Find Where field, select All Routines.
6. Select Find Within >>.
7. Select Ladder Diagrams.
8. Select Instruction Operands.



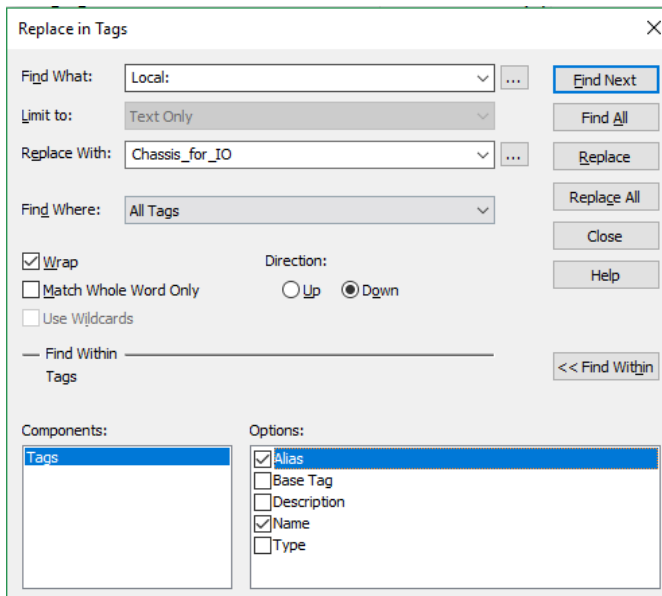
9. Select Replace All.

The find/replace is complete and the results are indicated in the Search Results tab.

Replace Aliases to Local I/O Tags

If your program uses alias tags for the I/O modules that you are moving, complete these steps to replace alias tags.

1. In the Logix Designer application, open the Controller Tags.
2. Press CTRL+H to open the Replace in Tags dialog box.



3. In the Find What field, select Local.
4. In the Replace With field, select the name of the communication module where the remote I/O was placed.
5. In the Find Where field, select All Tags.
6. Select Find Within >>.
7. Select Alias and select Replace All.

The Search Results tab indicates the changed tags.

Remove Other Modules from the Controller Chassis

If modules other than those modules listed in [Chapter 2](#) are in the controller chassis, you must remove them. Not all components are compatible with all redundancy system revisions. To make sure of component compatibility, see the release notes for your redundancy system revision in the Product Compatibility and Download Center at rok.auto/pcdc.

Add an Identical Chassis

After you have configured your primary chassis with the modules that are listed in [Chapter 2](#) add an identical chassis that contains the same modules with the same module-placement.

Upgrade to Redundancy Firmware

Once you have changed your system configuration and program and have added the identical chassis, upgrade your system firmware.

For information about how to upgrade the redundant system firmware, see [Chapter 5](#).

Update the Controller Revision and Download the Project

After you upgrade the firmware, use the Logix Designer application to access the controller properties and update the controller major revision to match your redundancy firmware major revision.

Once you update the controller firmware revision and save the changes, download the updated program to the controller.

History of Changes

This appendix contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

Change Log

1756-UM015L-EN-P, May 2025

Change
Added 1756-RM3 and 1756-RM3XT catalog numbers
Moved content from 1756-RM010 into this publication
Added security considerations
Added support for GuardLogix-XT™ 5580 and ControlLogix-XT™ 5580 controllers
Revised redundancy module requirements
Revised the operation of redundant fiber channels to include 1756-RM3 modules
Revised instructions for installing a redundancy firmware bundle
Added redundancy bundle firmware requirements for FactoryTalk® Linx and RSLinx® RMCT
Added prerequisites for access to FactoryTalk Linx RMCT
Changed the order of updating firmware in redundant chassis
Revised how to verify synchronization and qualification
Added information about Protection Mode
Added the fiber security feature
Added information about how to set the redundancy module date and time
Added instructions for disabling or re-enabling an SFP port
Added information about Class 1 and Class 3 connections to I/O modules
Added information about time synchronization and 1756-RM3 modules
Added crossload times for 1756-RM3 modules
Added how to align LINT members on 8-byte boundaries for ControlLogix 5570 controllers
Added information about temperature monitoring and faults for 1756-RM3 modules
Added Chapter 12: Troubleshoot Systems with 1756-RM3 Modules
Added migration paths for redundancy system updates
Added status messages and status indicators for 1756-RM3 modules
Updated redundancy system checklists
Revised Appendix D: Module Replacement Considerations
Added Appendix E: Install Earlier Redundancy Firmware Bundles
Added instructions to replace a 1756-CN2 module with a new series

1756-UM015K-EN-P, September 2024**Change**

Moved ControlLogix® 5570 redundancy information from 1756-UM535 to this publication

Added Logix SIS redundancy system information

Added Chapter 1: Redundancy Systems

Added Chapter 2: System Components

Added Chapter 3: Logix SIS Operation

Added considerations for 1756-EN4TR communication module RPI rates

Revised Concurrent Connection section

Add firmware requirements for communication with remote chassis

Added Standard Task Settings section

Added crossload times

Added Calculate RPI Timeout section

Added Redundancy System Status Bit section

Added details about how redundancy module faults clear

Added new major fault codes for redundant controllers

Added Appendix F: ControlLogix 5560 Redundancy Considerations

Added Appendix G: ControlNet® Considerations

1756-UM015J-EN-P, June 2024**Change**

Moved the Redundancy System Update Migration Paths section to a release note in the PCDC

1756-UM015I-EN-P, March 2024**Change**

Added redundancy bundles 34.014_kit1 and 35.013_kit1

1756-UM015H-EN-P, November 2023**Change**

Added redundancy bundles 34.014_kit1 and 36.011_kit1

1756-UM015G-EN-P, October 2023**Change**

Added redundancy bundle 35.011_kit3

1756-UM015F-EN-P, July 2023**Change**

Added redundancy bundles 33.015_kit2, 34.011_kit2, and 35.011_kit2

1756-UM015E-EN-P, November 2022**Change**

Removed Table 3 - Minimum Firmware Revision for Communication Modules in Remote Chassis. This information is in the ControlLogix 5580 and 1756-L8x Redundancy Bundle Release Notes available from the Product Compatibility and Download Center.

SequenceManager is supported on ControlLogix 5580 Process controllers firmware revision 35.011

Added Concurrent Communication information

Added redundancy bundles 33.015_kit1 and 35.011_kit1

Added considerations and best practices when using a redundancy system

1756-UM015D-EN-P, March 2022**Change**

Updated Controller Keyswitch

Updated Communication Modules in Redundant Chassis

Updated Table 1 - Components Available for Use in a Redundant Chassis Pair

Updated Fiber-optic Cable table

Updated Install the Redundancy Module Configuration Tool

Updated Enable Time Synchronization

Updated Check the EtherNet/IP™ Module Status

Updated Chassis Configuration Checklist

Updated EtherNet/IP Module Checklist

Updated Redundancy System Update Migration Paths

Added 1756-EN4TR modules

1756-UM015C-EN-P, July 2021**Change**

Added Communication Modules in Redundant Chassis.

Updated Data Server Communication Recovery Time Reduction During a Switchover.

Added Redundant Chassis Requirements.

Updated Install the Redundancy Module Configuration Tool.

Added 33.012_kit1 to Online Firmware Update Considerations

Notes:

Numerics

1756-EN4TR 23, 30

1756-RM3 22, 34, 47, 51, 53, 55, 121, 171, 181, 189

A

access the RMCT 40

annunciator wiring 20

Array (File)/Shift instructions 87

assign chassis ID 50

auto-synchronization setting 49

B

behavior

thermal fault 119

C

calculate

task watchdog 82, 193

calculate RPI timeout 106

certification

safety 16

chassis

assign ID 50

convert 42

chassis configuration list 181

chassis ID 50

CIP Security 16

CIP Sync time synchronization 51, 69

clear a fault 131, 147, 158

communication delays 31

communication module 42

connections 24, 195

firmware requirements 61

unicast 17

communication, concurrent 58

concise, program 86

concurrent communication 58

configuration

1756-EN4TR 59

ControlNet network 196

EtherNet/IP network 57

HMI 26

redundancy modules 47

redundant controllers 67

connections

communication module 24, 195

controller 21, 193

continuous task

execution 76

recommended 75

ControlFLASH Plus software 42

controller

connections 21, 193

status 121, 133

troubleshoot 156

use multiple 87

controller Ethernet port 20

ControlLogix 5570 redundancy

about 15

crossload times 80

memory usage slider 106

ControlLogix 5580 redundancy

crossload times 80

ControlLogix chassis 20

ControlNet

CPU usage 202

monitor CPU usage 202

network update time 200

node requirements 197 - 198

produce/consume connections 199

redundant media 198

sample programs 202

unscheduled 201

conversion

non-redundant to redundant 42

crossload

ControlLogix 5580 80

default 75

redundancy object attributes 79

redundant system 30, 31

scan time 79

crossload times 80

D

Data Highway Plus 28

date and time 51

designation

qualification after 44

DeviceNet 28

DLR 16

download application to primary controller 44

DSwNP

qualification status indicators 141

DSwP

qualification status indicators 141

duplex setting 64

E

environmental considerations 37

Ethernet port 20

Ethernet sockets 16

EtherNet/IP

duplex setting 64

IP address swapping 62 - 63

produce/consume connections 60

requested packet interval 57

with HMI 26

event log

1756-RM2 137
1756-RM3 125

execution

continuous task 76
periodic task 77

export diagnostics button 145**export event log** 143**extended event information** 140**F****fault codes** 131, 160**faults, redundancy module** 131, 158**features**

redundancy system 16

fiber channel switchover 34**fiber ports, redundant** 22**firmware**

signed and unsigned 23

firmware requirements

communication module 61
redundancy system 21

firmware update 161**front Ethernet port** 20**H****Human-Machine-Interface (HMI)** 26

use over EtherNet/IP 26

I**I/O**

concurrent communication 58
multicast 181
products 25

install

redundancy firmware 38
redundant components 42
RMCT 39

IP address

swapping 62 - 63

K**keeper**

status
mismatch 204
module status display 203
RSNetWorx for ControlNet software
203
unconfigured 204
valid 203

L**lock for update logs** 124**logic, scan-dependent** 88**Logix SIS**

firmware update considerations 161
operation 29
operation after a fault 30
safety considerations 13
safety task 13
SIL 2/3 functions 29
watchdog time 81

M**major fault codes** 131, 160**mapping** 91, 92**memory usage slider**

ControlLogix 5570 106

MSG instruction 111**multicast**

I/O 181

muting, safety function 30**N****network** 201

ControlNet
monitor CPU usage 202
Data Highway Plus 28
DeviceNet 27, 28
Remote I/O 27
Universal Remote I/O 28
update time 200

network update time 200**networks** 25**non-redundant controller** 156**non-redundant to redundant**

conversion 42

O**online edits** 102, 102 - 105

finalize 103
reserve memory 105
retain edits 103
test edits 102

online firmware update 161**operations**

crossload 30, 31
fiber channel 34
qualification 29, 31
synchronization 29, 31

P**Partial Import Online** 102**periodic task**

execution 77
recommended 75

PlantPAX 16**PlantPAX System Estimator** 20**PLGU**

qualification status indicators 141

PLU

qualification status indicators 141

port, Ethernet 20**power supplies, redundant** 20

power supply 42

produce/consume connections

over ControlNet 199
over EtherNet/IP 60

produced/consumed tags 16

program

default synchronization 75
finalize test edits 103
logic after switchover 99
maintain data integrity 87 - 89
manage tags 84
messages for redundancy commands 53 - 99
online edits 102, 102 - 105
optimize task execution 93
Partial Import Online 102
reserve memory 105
tags 84
task type 75
test edits 102
use concise 86

Protection Mode 47

PRP 16

PsDS

qualification status indicators 141

PwNS

qualification status indicators 141

PwQgS

qualification status indicators 141

PwQS

qualification status indicators 141

Q

QSwP

qualification status indicators 141

qualification

aborted 156
after designation 44
ControlLogix 31
description of 29, 31
Logix SIS 29

qualification status indicators 141

DSwNP 141
DSwP 141
PLgU 141
PLU 141
PwDS 141
PwNS 141
PwQgS 141
PwQS 141
QSwP 141
SLgU 141
SLU 141

R

redundancy module

catalog number replacement 189
configure 47
missing 155
troubleshoot 1756-RM2 133
troubleshoot 1756-RM3 121

redundancy module date and time 51

redundancy object attributes

for crossload time 79

Redundancy Status bit 117

redundancy system

ControlLogix 5570 15
ControlNet considerations 195 - 204
features 16
firmware requirements 21
I/O products 25
networks 25
restrictions 17
SIL 2/3 safety functions 29

redundant chassis pair 19

redundant media

ControlNet 198

redundant module

remove 45
replace 45
reset 45

redundant system components

fiber ports 22
power supplies 20

remote

communication modules 27
I/O 30, 58

remove

redundant module 45

replace

communication module series 186
redundancy module catalog number 189
redundant module 45

requested packet interval

over EtherNet/IP 57

reset

redundant module 45

restrictions

redundancy system 17

RMCT

access 40
install 39
obtain 39
troubleshoot 125, 137
version 39, 41

RPI timeout 106

S

safety certification 16

safety considerations 13

safety controller operation 29

safety function muting 30

safety signature 29

safety task execution 13

safety task faults 30

safety task watchdog 81

scan time

concise programming 86
crossload 79
efficient crossloads 84
multiple controllers 87
number of programs 83

scan-dependent logic 88

set date and time 51

signed and unsigned

firmware 23

SIL 2/3 support 29

SLgU
 qualification status indicators 141

SLU
 qualification status indicators 141

software
 FactoryTalk Alarms and Events 26
 FactoryTalk Batch 26
 FactoryTalk View Site Edition 26
 optional 26
 RSNetWorx for ControlNet 26
 RSNetWorx for EtherNet/IP 26

specifications 119

standard controller operation 31

standard task watchdog 81

status bit, Redundancy Status 117

Studio 5000 Logix Designer
 use to troubleshoot 121, 133

switchover
 description 32
 example 113
 locked attempts 149
 logic after 99
 monitor synchronization after 98

synchronization
 default 75
 description of 29, 31
 Logix SIS 29
 monitor after switchover 98

Synchronization tab
 commands in 107

syncsynchronization
 ControlLogix 31

system
 qualification 29, 31
 synchronization 29, 31

System Update commands
 abort system lock 113
 initiate locked switchover 113
 lock for update 112

system update lock attempts 124, 148

T

tags
 manage 84
 produced/consumed 16
 safety 16
 standard 16

task 77
 continuous, execution 76
 optimize execution 93
 recommended 75

temperature
 limit 119

time synchronization 51, 69

timeout, RPI 106

troubleshoot
 missing redundancy module 155
 qualification abort 156
 redundancy module missing 155
 RMCT 125, 137
 use
 RSNetWorx for ControlNet software
 203
 use Studio 5000 Logix Designer 121, 133

U

unicast
 communication module 17

Universal Remote I/O 28

unscheduled
 ControlNet network 201

update firmware 161

V

version
 redundancy firmware 21
 RMCT 39, 41

W

watchdog time 81, 82, 183, 193

When 121

wiring, annunciator 20

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, Knowledgebase, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental compliance information on its website at rok.auto/pec.

Allen-Bradley, ControlFLASH Plus, ControlLogix, ControlLogix-XT, DH+, Data Highway Plus, expanding human possibility, FactoryTalk, FLEX 5000, FLEXHA 5000, FLEX I/O, GuardLogix, Integrated Architecture, Logix 5000, Optix, OptixPanel, PanelView, PhaseManager, PlantPAx, PLC-2, PLC-3, PLC-5, SLC, POINT I/O, PointMax, Rockwell Automation, RSLinx, RSNetWorx, RSView, SequenceManager, Stratix, Studio 5000 Logix Designer, and VersaView are trademarks of Rockwell Automation, Inc.





CIP, CIP Security, CIP Sync, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc.

microSD is a trademark of SD-3C.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

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

Connect with us.    

rockwellautomation.com ————— **expanding human possibility®**

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1)414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800

Publication 1756-UM015M-EN-P - September 2025

Supersedes Publication 1756-UM015L-EN-P - May 2025

Copyright © 2025 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.