Reference Manual

Original Instructions

Allen-Bradley

Using ControlLogix SIL 2 with 1715 I/O

Catalog Numbers ControlLogix 5570, 1715-AENTR, 1715-IB16D, 1715-IF16, 1715-OB8DE, 1715-OF8I

Allen-Bradley • Rockwell Software

Rockwell Automation

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.

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).

Notes:

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation® industrial system.
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Disclaimer

Rockwell Automation is not responsible or liable for indirect or consequential damage that results from the use or application of this equipment. The examples that are given in this manual are included solely for illustrative purposes. Because of the many variables and requirements that are related to any particular installation, Rockwell Automation does not assume responsibility or liability for actual use that based on the examples and diagrams. No patent liability is assumed by Rockwell Automation concerning the use of information, circuits, equipment, or software described in this manual. All trademarks are acknowledged.

It is not intended that the information in this publication covers every possible detail about the construction, operation, or maintenance of a SIL 2 system installation. You must follow your own local laws and regulations and refer to your own local (or supplied) system safety manual, installation and operator/maintenance manuals. Ultimately you are responsible to apply the correct installation to satisfy your safety requirements.

Usage

This manual is intended primarily for system designers and technical sales people who are required to understand the requirements of a ControlLogix® /1715 SIL 2 system. The information that is contained in this guide is intended to be used with (and not as an alternative for) reading the ControlLogix SIL 2 user manual and 1715 User Manual, expertise and knowledge about safety-related systems. It is expected that the reader has an in-depth knowledge of the intended application and can understand the generic terms that are used inside this guide and the terminology that is used in the integrator's or project's application area.

IMPORTANT In this guide, the term Duplex or Redundant can be used interchangeably. In this usage, it is considered an automatic feature that you do not have to apply user-generated code to use it.

Introduction

The ControlLogix/1715 SIL 2 system uses Standard ControlLogix processor modules along with 1715 I/O modules. A SIL 2 system is formed by one or more controllers, I/O modules, their power sources, communications networks, and workstations. This tips guide helps to give a quick start for using the ControlLogix/1715 SIL 2 controller and systems.

There is usually some confusion between GuardLogix® and ControlLogix SIL 2 since GuardLogix can be used in a SIL 2 system and it is based on ControlLogix. In this guide we refer to ControlLogix only, NOT the red safety GuardLogix controller, and it uses only 1715 I/O.

ControlLogix SIL 2 can be used with 1756 or 1794 IO as well. 1756 and1794 IO are covered in the ControlLogix SIL 2 Safety Reference Manual (1756-rm001) and are not discussed here. Note if you are using 1715 IO instead of 1756 or 1794 IO then the information on those IO platforms in the information in the Safety Reference Manual does not apply.

The ControlLogix/1715 SIL 2 System

Overview

A ControlLogix® SIL 2 system consists of a standard ControlLogix controller with proper SIL 2 approved firmware, field connections, 1715 I/O modules with proper SIL 2 approved firmware, power sources, and network connections. This system is not a GuardLogix® controller system. The flexibility of the design means that a system can meet a wide variety of business needs while maintaining a desirable level of commonality and or simplicity. This is known as a configured safety system, meaning the control system must be configured in a specific manner to meet SIL 2 requirements. This tips guide helps introduce the primary components that can be used to assemble a ControlLogix/1715 SIL 2 Safety System.

The 1715 I/O system takes much the configuration work out of the ControlLogix SIL 2 system. Since the I/O was specifically designed to operate in a safety system, there is no longer any need for special wiring or IFMs to use ControlLogix in a SIL 2 manner. Either or Both the I/O system or controller system can be simplex or duplex, making the system scalable to fit the customer's application.

ControlLogix Controllers

Simplex ControlLogix Controller

The following components are needed for a Simplex ControlLogix controller. Redundancy is not required for SIL 2.

TIP Redundancy can be selected for availability if needed.

For hardware selection, refer Appendix B of Using ControlLogix in SIL 2 Applications Safety Reference Manual (1756-RM001) for the SIL2-certified ControlLogix catalog/revision numbers.

- 1756 Chassis
- Power Supply
  - If the 1756-PA75 or 1756-PB75 power supply is used with a Series B controller, the Series B version of the power supply must be used (1756-PA75/B or 1756-PB75/B)
- 1756-L7x Controller
- EtherNet/IP communication card
  - Use of a 1756-EN2TR or 1756-EN2TRXT is required to achieve SIL 2 in the application. EN2TR is the only communication module Rockwell Automation will continue to certify for ControlLogix SIL 2 safety functions in the future

– Other EtherNet/IP communication modules can be used for non-safety loop communication

Redundant ControlLogix Controllers

See the following manuals for the components necessary for a redundant ControlLogix controller.

- ControlLogix Redundancy User Manual (1756-UM535).
- Appendix B of Using ControlLogix in SIL 2 Applications Safety Reference Manual (1756-RM001) for the SIL2-certified ControlLogix catalog/ revision numbers.

Controllers, power supplies, adapters, and I/O modules can all be architected in duplex configurations. Diagnostics can indicate whether each module is running duplex, simplex, or is faulted. For de-energize to action applications, you can programmatically decide to Fail to Safe or Run Degraded in the event of a fault. Note that if Running Degraded on one controller or 1715 I/O module, the system is still SIL 2 capable since 1756 ControlLogix is capable of running SIL 2 with one controller or 1715 I/O module. It is up to the user if they want to continue running in this state.

ControlLogix Redundancy uses different firmware than a non-redundant system does. The major revision is the same but the minor will differ. An example would be V20.050. This example is the redundancy version of V20 firmware. You must download the entire bundle from the download site. The bundle contains all redundancy tested versions for that controller revision.

Theory of Operation

ControlLogix redundancy operates on a Primary and Secondary basis. The Primary chassis contains the modules that are currently controlling the application. All the modules in the Secondary chassis are ready to take control but are currently not running the application. The primary controller keeps the secondary controller synchronized by sending the data that has changed during its scan multiple times per scan. That allows the secondary chassis to take control quickly. For more information on switchover times, see ControlLogix Redundancy User Manual (1756-UM535.)

Diagnostics

IMPORTANT If there is a redundancy switch over, it is always recommended to investigate why it switched over.

IMPORTANT When programming your redundant system, program so your redundancy system status is continuously 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 of status via your HMI or other status-monitoring device

See the following table when programming the controller to obtain the status of the redundancy system.

Add a GSV instruction in the standard task (non-safety task) and use the output to determine what you want to do if it returns with any code other than 16#2.

Always monitor the status of the redundancy system. If the system is running properly, the secondary controller is always present and synchronized.

For this information	Get This Attribute	Data Type	GSV/SSV	Description	
Redundancy Status of the Controller	ModuleRedundancy State	INT	GSV	**IF**	**Then**
				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 looking for update
				16#10	Primary locked for update

If the system is running normally, the 1756-RM modules show the following status codes.

Figure 1 - Primary Controller

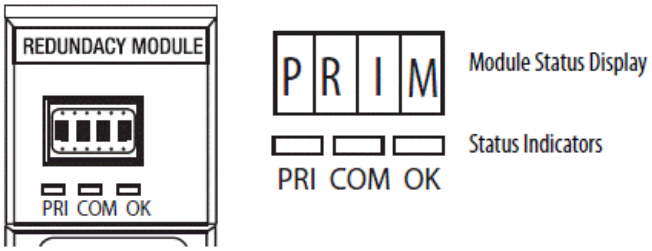
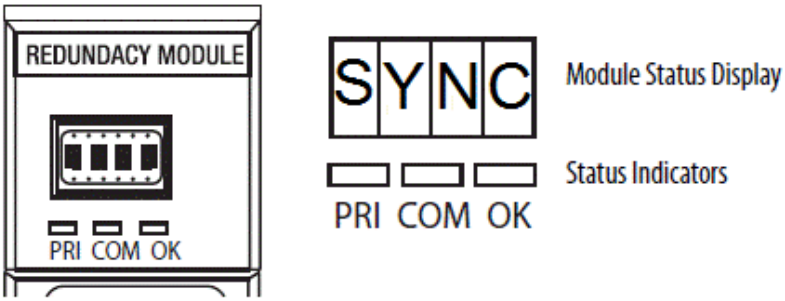


Figure 2 - Synchronized Secondary Controller



IMPORTANT There are different versions for redundant and non-redundant firmware. Only certain ones are certified for use in an SIL 2 system. See the revision release list from the product certifications link for more information.

1715 Redundant I/O System - Safety certificate - 1715-CT007

Logix Safety certificate - Logix-CT008

Features not Supported

The following features are not supported in a ControlLogix Redundancy system.

- Any motion feature or instructions
- Any SIL 3 functional safety feature
- Firmware Supervisor
- You cannot use the Match Project to Controller feature available in Studio 5000 Logix Designer® in a redundancy system.
- You cannot use consumed Unicast connections in a redundancy system. The redundancy controllers can be the producer.
- Unicast I/O is not supported in a redundancy system.
  - If you attempt to use consumed Unicast connections, disqualification occurs and qualification of an unsynchronized redundant chassis pair is not allowed. You can use produced Unicast connections that remote controllers consume.
- Local I/O is not supported in either of the Controller chassis

The redundant controller application cannot contain these tasks:

- Event tasks
- Inhibited tasks

Redundancy System Considerations

- You can experience difficulty synchronizing your chassis if you use the redundant controller at or very near the connection limits.
- A redundant controller uses more memory than the same application in a simplex system. If you are at or near the memory limit, you can run out of memory even though the controller reports it has free memory. This is due to the crossload mechanism.
- Do not use the USB ports of communication modules in the controller chassis to access the redundant controllers or networks. Use of the USB ports in either of the controller chassis to go online results in a loss of communication after a switchover for the device plugged into the USB port.
- Task scan time is longer when redundancy is enabled. Make sure that you consider this when designing your safety system. Do not do your testing and settings based on a simplex system and then make it redundant.
- You should never communicate with the controller in the secondary chassis other than to obtain diagnostics.

Redundancy System Details

Two 1756 chassis that have the following equipment provisioned the same:

- Chassis size
- Modules in the same slots
- One 1756-RM2 or 17560RM2XT module per chassis
- Up to two controllers per chassis (for safety systems only one is recommended)
- Up to seven EtherNet/IP communications modules per chassis.
- 1756-RMCx cables
  - These connect the RM modules together between chassis
  - You can choose one or two cables
  - The cables are fiber-optic Cables
  - The redundancy module cables are available in three different pre-made lengths or you can make your own up to 4KM in length:

Catalog Number	Cable Length
1756-RMC1	1 meter
1756-RMC3	3 meters
1756-RMC10	10 meters

1756 Power supplies

- Use simplex power supplies or redundant power supplies
- If the 1756-PA75 or 1756-PB75 (non-redundant) power supply is used with a ControlLogix 5560 Series B or ControlLogix 5570 Series B controller, the Series B version of the power supply must be used (1756-PA75/B or 1756-PB75/B)

Controllers

- Only 1756-L7x controllers are supported

EtherNet/IP communication cards

- Use of a 1756-EN2TR or 1756-EN2TRXT is required to achieve SIL 2 in the application
- Other EtherNet/IP communication modules (1756-ENBT, 1756-EN2T, 1756-EN2TXT) can be used for non-safety loop communication
- 1715 IO only communicates via EtherNet/IP so no ControlNet modules are listed here.

Figure 3 - Redundancy System Configuration Example

Features of the ControlLogix SIL 2 System

Overview

The ControlLogix® controller consists of a central processor, I/O interfaces, and memory.

The ControlLogix controller can be a simplex (Single Chassis) or redundant configuration (Dual Chassis with RM). This makes no impact on the SIL calculation of the safety function. This adds availability to the safety function, but no change to safety. In a Duplex configuration, the system switches from a 1oo1 controller to another 1oo1 controller if there is a fault in the controller chassis.

Operating Modes

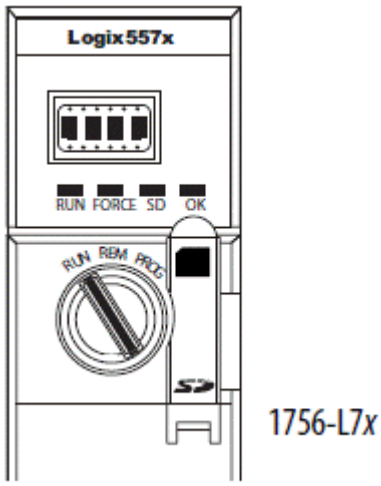
A three-position keyswitch on the front of the controller governs ControlLogix system operational modes. The following modes are available:

- Run – This is known as Hard Run. No online changes are possible
- Program – This stops the execution of the application code and allow online changes
- Remote - This software-enabled mode can be Program or Run. In this mode, you can make online changes while the application is running but the change requires a confirmation. You can also put the controller into program mode via a command. Because of these functions, it is required for the controller to be in Hard Run when operating in Safety Mode.

IMPORTANT The keyswitch must be in the RUN position to be SIL 2 certified. If you put the keyswitch into the REMOTE position to make an online edit, you are not in safety mode. When you are finished with the online edit, you must put the keyswitch into RUN position and remove the key.

Making any edit always involves following your own MOC (Management of Change) procedures. There must be a validation before putting the changed code into service. Online edits are the most risky method of doing this and are not recommended.

Figure 4 - Controller in RUN Mode



IMPORTANT There are different versions for redundant and non-redundant firmware. Only certain ones are certified for use in an SIL 2 system. See the revision release list from the product certifications link for more information.

1715 Redundant I/O System - Safety certificate - 1715-CT007

Logix Safety certificate - Logix-CT008

Redundant Power Supply Recommendations

If you are using Redundant 1756 Power supplies, wire the solid-state fault relay on each power supply from an appropriate voltage source to an input point in the ControlLogix system so that the application program can detect faults and react appropriately.

Safety Configurations

When used with 1715 I/O the ControlLogix SIL 2 system supports the following safety configurations. These SIL 2 architectures are for fail-safe low and high demand applications. All SIL 2 architectures can be used for de-energize to trip applications. With special precautions, CLX/1715 SIL 2 can be used in energize-to-trip applications.

- SIL 2 low demand applications
- SIL 2 high demand – up to 10 demands per year
- SIL 2 fail-safe applications
- SIL 2 with fault tolerant inputs
- SIL 2 with fault tolerant outputs
- SIL 2 with fault tolerant inputs/outputs

Application Development Requirements

IMPORTANT This document does not cover the specifics of creating the application code. It is assumed the use knows the requirements of IEC-61511 and their specific application when designing their system. This document only covers the steps if it is necessary for ControlLogix to meet SIL 2.

The application software for the SIL2-related automation system is created using the programming tool, that is, RSLogix 5000® software or the Studio 5000 Logix Designer® application, according to IEC 61131-3.

The application program has to be created by using the programming tool and contains the specific equipment functions that the ControlLogix system implements. Parameters for the operating function are also entered into the system with the programming software.

The safety concept of the SIL 2 ControlLogix system assumes the following:

- The user who is responsible for creating, operating, and maintaining the application is fully qualified, specially trained, and experienced in safety systems.
- The programming software is installed correctly.
- Control system hardware is installed in accordance with product installation guidelines.
- User application code (user program) uses common and good design practices.
- A test plan is documented and adhered to, including well-understood proof test requirements and procedures.
- A well-designed validation process is defined and implemented.
- A well-designed Management of Change (MOC) procedure is in place

Security

In the ControlLogix system and in the programming software, protection mechanisms are available that help prevent unintentional or unauthorized modifications to the safety system.

The following tools can be employed for security reasons in a SIL2-certified ControlLogix application:

- Source Protection
- FactoryTalk® AssetCentre
- FactoryTalk® Security

In RSLogix 5000® software, V18 and later, and in the Studio 5000 Logix Designer® application, tags have two attributes: External Access and Constant. External Access controls access from external applications like HMIs. It can have values of read/write, read-only, or none. Set all SIL 2 safety-related tags to read-only. The Constant attribute is either on or off. When enabled, it helps

prevent programmatic changes of a tag's value. Where possible, it is highly recommended to configure SIL 2 safety-related tags as Constant.

Always take proper physical security precautions to achieve safe operation of the system. The following is a list of recommended precautions.

- Keep the controller and IO chassis in a locked cabinet and limit access to only those that need access
- Secure all network access points either by physically disabling them or making sure that they are in locked cabinets
- Keep all passwords secure
- Configure role-based access to the system
- Install network-based firewalls with proper configurations

Safety SIL Task

Include one Periodic task designated as the Safety task composed of programs and routines to contain the user application. The SIL 2 task must be the highest priority task of the controller and the user-defined watchdog must be set to accommodate the SIL 2 task.

IMPORTANT	You must dedicate a specific task for safety-related functions and set that task to the highest priority (1). If you decide to use non-safety logic in the same controller, that code must be separate. It is recommended to use separate controllers for safety-related code and Process Control non-safety code.

Having a non-safety task in the safety controller for things like determining the status of the redundancy system or diagnostics does not violate the above statement since there are no BPCS (Basic Process Control System) control elements present.

Confirm that the properties of the task that is used for safety is configured correctly for your application.

- Watchdog: the value that is entered for the SIL 2 safety task must be large enough for all logic in the task to be scanned.

If the task execution time exceeds the watchdog time, a major fault occurs on the controller. Even if you are using redundant controllers the watchdog is set the same in both controllers automatically and the new primary will eventually fault as well if the cause was just a too tight watchdog setting. You must monitor the watchdog and program the system outputs to transition to the safe state (typically the OFF state) if there is a major fault occurring on the controller. See Chapter 3 - Using the1715 I/O.

Setting the SIL 2 Task 'Period' Configuration

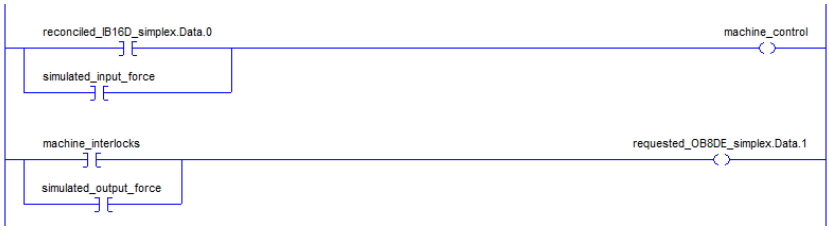
The following are recommendations to serve as a starting point to configure the periodic task 'period' for SIL 2 applications. Set the period to the minimum 1715 SIL 2 module RPI divided by 2. For example, if the default RPIs are used it would be 60/2=30 ms. Fine-tune your task period based on other factors such as your safety reaction time requirements.

1715 Module	RPI
Adapters	180 ms
Digital Modules	60 ms (lowest)
Analog Modules	120 ms

Forcing

Forcing of SIL 2 tags is not possible in a ControlLogix/1715 SIL 2 system. Because the Inputs and Outputs are controlled by the Add-On Instructions and not directly, any attempt to force one causes it to fail the data integrity checks built into the Add-On Instructions. The 1715 output module will generate a CRC error when it receives packets with this inconsistency, and discard the data. From the controller, you will notice 'SIL 2 Reset Needed' on both the AOI and AOP.

The ability to manually control 1715 inputs and outputs would have to be added within Logix routines. Examples of this are shown here.



Since this is considered a "force," the following rules must be followed.

- You must remove forces on all SIL 2 tags before beginning normal operation for the project.
- You must not force SIL 2 tags after validation is performed and during normal controller operation.
- Forcing must not be used as a temporary bypass for equipment that malfunctions.
- This method may be used for a proof test but must be removed as soon as that is over.

Verify Download

Verify the download of the application program for proper operation. A typical technique is to upload the completed program file and perform a compare of that file against what is stored in the programming terminal. (Offline and uploaded program)

To perform program verification, follow these steps in RSLogix 5000 software or the Studio 5000 Logix Designer application.

1. With the programming software closed rename the project.
2. Start the programming software, upload the controller project, and save it.
3. Open the compare tool and select both files.
4. Start the compare operation.
5. Review the compare output results and verify that everything matches without error. (Project documentation differences can exist.)
6. Save the compare results as part of the verification process.
7. Delete the upload file.
8. To maintain project documentation, rename the original project file (change back) to the original project name.

IMPORTANT Do not use memory cards to transfer the safety application automatically. The AutoFlash firmware feature is not supported for SIL 2 safety applications.

HMI Precautions

You must exercise precautions and implement specific techniques on HMI devices. These precautions include, but are not limited to the following:

- Limited access and security
- Specifications, testing, and validation
- Restrictions on data and access
- Limits on data and parameters

HMI- related functions consist of two primary activities: reading and writing data.

Reading Data

Reading data is unrestricted because reading doesn't affect the operation or behavior of the safety system. However, the number, frequency, and size of the data being read can affect controller performance. To avoid safety-related nuisance trips, use good communication practices to limit the impact of communication processing on the controller. Do not set read rates to the fastest rate possible.

Writing Data

A parameter change in a safety-related loop via an external (that is, outside the safety loop) device (for example, an HMI) is allowed only with the following restrictions:

- The customer MOC procedure is followed.
- Only authorized, specially trained personnel (operators) can change the parameters in safety-related systems via HMIs.
- The operator who changes a safety-related system via an HMI is responsible for the effect of those changes on the safety loop.
- You must clearly document variables that need changed.
- You must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI (MOC Procedure).
- Changes can only be accepted in a safety-related system if the following sequence of events occurs.

1. The new variable must be sent twice to two different tags; that is, both values must not be written to with one command.
2. Safety-related code that executes in the controller, must check both tags for equivalency and make sure that they are within range (boundary checks).
3. Both new variables must be read back and displayed on the HMI device.
4. Trained operators must visually check that both variables are the same and are the correct value.
5. Trained operators must manually acknowledge that the values are correct on the HMI display that sends a command to the safety logic, which allows the new values to be used in the safety function.

In every case, the operator must confirm the validity of the change before they are accepted and applied in the safety loop.

The remainder of the steps need to follow IEC 61511 standard on process safety, section 11.7.1 Operator Interface requirements.

IMPORTANT The High-Speed Jog function is not allowed and must not be used in the project.

Notes:

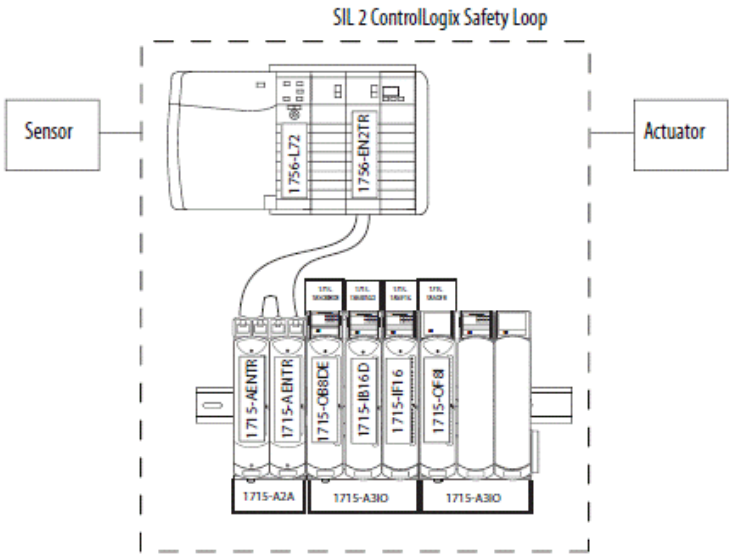
Using the 1715 I/O

Select the Mix of 1715 I/O Required

1715 I/O simplifies the configuration choices for a ControlLogix® SIL 2 system. All I/O modules in the 1715 family are approved for use up to SIL 2, but proper firmware is required. The system can be configured with any combination of I/O modules, either in simplex or duplex mode and the redundancy features are built into the hardware so no cross wiring of outputs to inputs is needed any longer nor is the requirement to have two separate I/O chassis for Fault Tolerance.

For hardware selection, refer Chapter 6 of Redundant I/O System User Manual (1715-UM001.)

Figure 5 - Typical Simplex Application

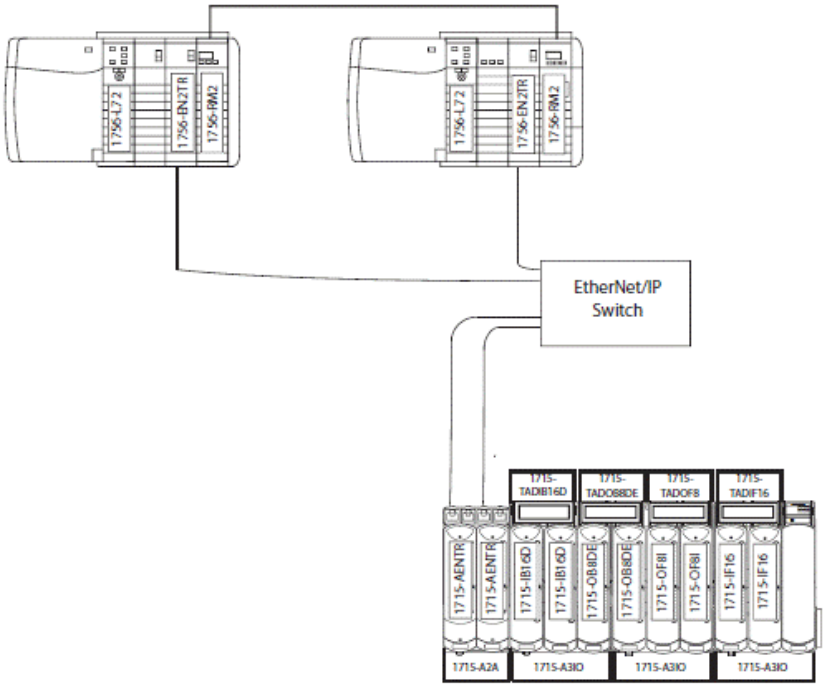


IMPORTANT The 1715 uses dual adapters even with simplex I/O.

For SIL 2 safety applications, you must have the following:

- Firmware for the 1715-AENTR adapters, revision 2.001 or later
- Add-on Profile for the adapter, version 2.01.014 or later
- Add-on Profile for the I/O modules, version 3.01.014 or later
- Add-On Instructions when using a ControlLogix system, version 2.001 or later
- A 1756-L7 ControlLogix controller

Figure 6 - Typical Duplex Configuration



IMPORTANT For duplex configurations, a SIL 2 fault-tolerant architecture has dual-input, dual adapter, and dual output modules.

1715 Redundant I/O

Overview

The 1715 Redundant I/O System lets a ControlLogix SIL 2 controller communicate to a remote, redundant I/O chassis by using EtherNet/IP. The SIL 2 1715 Redundant I/O system provides fault tolerance and redundancy for critical processes by using a redundant adapter pair and multiple redundant I/O modules that have diagnostics and are easily replaceable while the system is running.

The 1715 Redundant I/O System is a modular system in which the adapter and I/O base units snap together by using mating connectors and retaining clips to form the backplane. One module in a duplex pair can be removed and replaced without system interruption. The base units, via termination assemblies, provide the interconnections for power, adapter, and I/O data. Once connected, the base units form the single mechanical assembly or backplane.

The modular architecture lets you build and adapt a system to suit the specific needs of an installation. The architecture lets you choose from different levels of I/O fault tolerance. Any of the modules can be used Simplex, Duplex, and/or a combination of both. For example, there can be redundant adapters, two duplex input module pairs, a duplex output module pair, and then simplex input and output modules in the same I/O system. The system is designed to have two adapters at all times but the system continues to run on one adapter on the occasion that one adapter faults. The missing module diagnostic cannot be disabled for this.

The 1715 Redundant I/O System consists of a two-slot adapter base unit that houses a redundant adapter pair. The adapter base unit is connected to up to eight I/O base units, which can hold up to 24 I/O modules (three I/O modules per I/O base unit) when connected together. The I/O modules can be configured in any combination of simplex or duplex pairs, depending on the mode of operation needed. The I/O base units can be connected directly to the adapter base unit and other I/O base units, or through expansion cables.

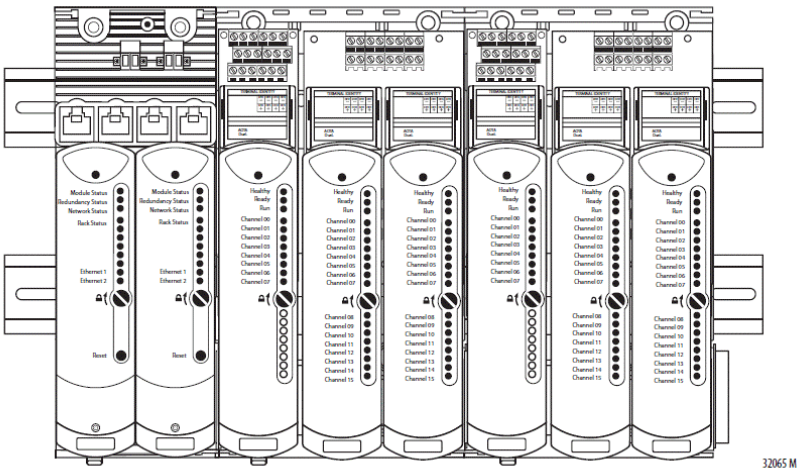
Components

See chapter 2 of the 1715 I/O user's manual (1715-UM001) for all warnings and important considerations.

The 1715 Redundant I/O System is a remote redundant I/O system that was developed to communicate with a Logix controller in a ControlLogix enhanced redundant system by using the EtherNet/IP network and includes these components:

- A pair of 1715-AENTR adapters.
- 1715 digital and analog I/O modules.
- A 1715-A2A redundant adapter base unit connects to a 1715-A3I0 I/O module base unit from its right side only to form the backplane for the system.
- Termination assemblies are available in Simplex and Duplex configuration. They mount onto the 1715-A3IO I/O module base unit, and connect the I/O modules to the I/O wiring.
- Each 1715-A3IO I/O base unit holds up to three I/O modules. Up to 24 I/O modules can be added to the system. That is either 24 simplex or 12 duplex or any combination of modules up to 24 I/O modules maximum.
- Module pairs can span across two bases.
- The system is built on DIN rails within a cabinet enclosure.
- 1715-C2 expansion cables can be used to allow for space restrictions of the system within the cabinet.

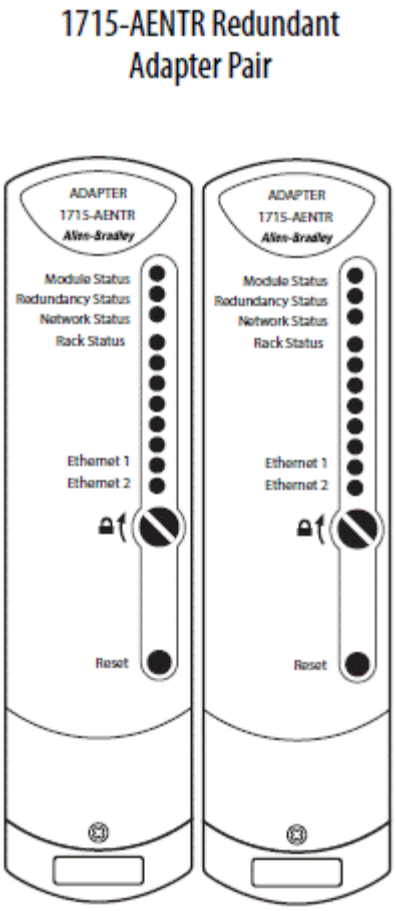
Figure 7 - Typical 1715 I/O System with Dual Adapters and a Mix of Simplex and Duplex I/O Modules



IMPORTANT The I/O base units only connect to the right side of the Adapter base unit.

1715-AENTR Adapter Redundant Pair

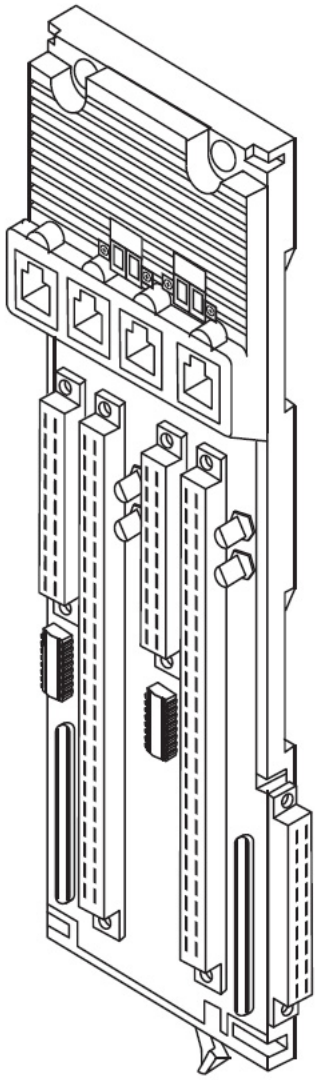
The 1715 adapter communicates via the EtherNet/IP network using CIP protocol to a 1756 ControlLogix controller, which conveys system I/O data.



1715-A2A Adapter Base Unit

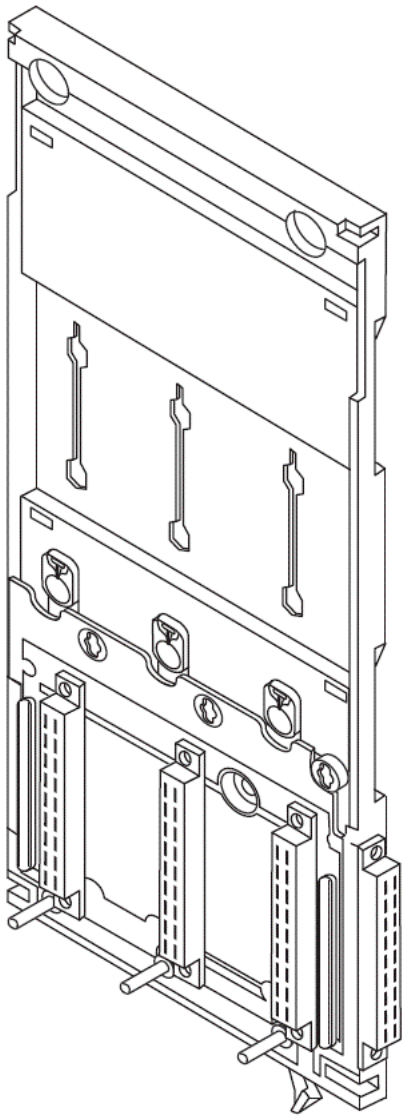
The adapter base unit holds a pair of adapters. It also contains connectors for power (2) and network connections (4).

The network connections can support Star or DLR protocols.



1715-A3IO I/O Base Unit

The I/O base unit holds up to three I/O modules. I/O modules can span across bases if a duplex pair is next to a duplex pair. There is no need to leave a space empty.



1715 Digital and Analog I/O modules

Your system can be configured with any combination of I/O modules, and in either Simplex or Duplex mode. These I/O modules can be included in your system:

- 1715-IB16D 16-channel digital input module
- 1715-OB8DE 8-channel digital output module
- 1715-IF16 16-channel analog input module
- 1715-OF8I 8-channel analog output module

I/O Termination Assemblies (TA)

I/O termination assemblies are inserted into the I/O base units. There are eight types of termination assemblies (two for each module) depending on the architecture of your system and the I/O modules you are going to use.

For this example, we only show the duplex assemblies.

- A 1715-TADIB16D, 16-channel duplex TA that provides termination for 16 digital input channels and mates with up to two 1715-IB16D digital input modules
- A 1715-TADOB8DE digital output, 24V DC 8-channel duplex TA that provides fault tolerant operation for eight digital output channels and mates with redundant 1715-OB8DE digital output modules
- A 1715-TADIF16, 16-channel duplex TA that provides termination for 16 isolated analog input channels and mates with up to two 1715-IF16 16-channel analog input modules. The channels are isolated.
- A 1715-TADOF8, 8-channel duplex termination assembly provides fault tolerant operation for eight analog output channels through inter-module communication and by routing the output source current from two modules to the same field device

Power Requirements

A 24V DC power supply is required. For proper duplex operation, two power supplies are recommended. This is not required for fail-safe safety systems but for availability or energize-to-action systems.

Module Placement

The following figure is only an example and is to be used for illustration purposes only. The adapter and base units are DIN rail mounted and connections are chained together from left to right.

Module Placement

A general overview of a typical redundant I/O system layout is shown here.

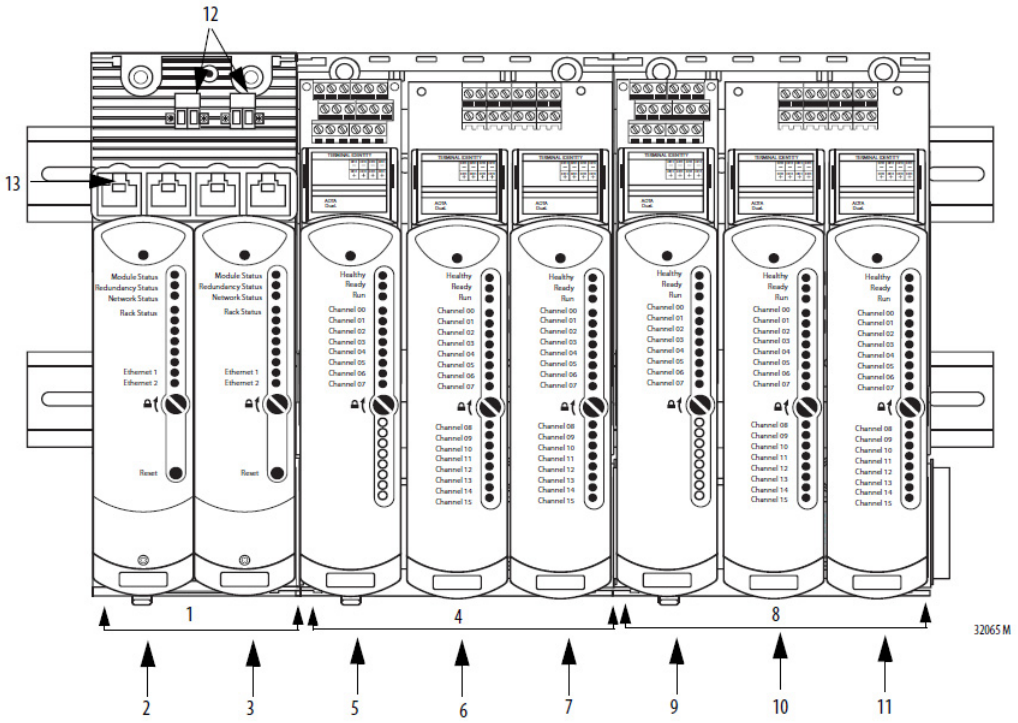


Figure 8 - Module Placement Description

Item	Description
1	Adapter base unit
2	Adapter A module
3	Adapter B module
4	I/O base unit
5	Simplex I/O module
6	Duplex I/O module (first in pair)
7	Duplex I/O module (second in pair)
8	I/O base unit
9	Simplex I/O module
10	Duplex I/O module (first in pair)
11	Duplex I/O module (second in pair)
12	Power connections
13	Ethernet connections

Notes:

Using 1715 Hardware in a ControlLogix SIL 2 System

Overview

For complete information, see the following chapters of the user manuals,

- Chapter 6 of 1715 Users Manual 1715-UM001
- Chapter 3 of 1756 SIL 2 Users Manual 1756-RM001

This chapter provides information on using 1715 I/O modules in a low demand ControlLogix®-based SIL 2 system.

IMPORTANT For complete information, you must consult the ControlLogix SIL 2 Safety Reference Manual - 1756-RM001.

This guide is only one example of using 1715 and ControlLogix SIL 2.

IMPORTANT The TÜV Rheinland Group has approved the 1715 Redundant I/O System for use in safety-related applications up to and including SIL 2 according to these standards:

- IEC 61508, edition 1,2000
- IEC 61511

IMPORTANT For SIL 2 safety applications, you must have the following:

- Firmware for the 1715 AENTR adapters, revision 2.001 or later
- Add-on Profile for the adapter, version 2.01.014 or later
- Add-on Profile for the I/O modules, version 3.01.014 or later
- Add-On Instructions when using a ControlLogix system, version 2.001 or later
- A 1756-L7 ControlLogix controller

IMPORTANT Safety functions that are being edited are not SIL 2 certified from the start of the online edits to the completions of the validation of the changes.

Firmware

To use 1715 modules in a ControlLogix SIL 2 system, you must use firmware that has been designed for SIL 2 use.

See 1715-CT007xxx for more information

Duplex Configurations

For duplex configurations, a SIL 2 fault-tolerant architecture has dual-input, dual adapter, and dual output modules. The input and output modules operate in 1oo2D (1 out of 2) under no fault conditions and degrade to 1oo1D (1 out of 1) upon detection of the first fault in either module. The modules fail-safe if faults occur on both modules. The adapters operate in 1oo2D under no-fault conditions and degrade to 1oo1D upon detection of the first fault. A duplex system could therefore be 1oo2D reverting to 1oo1D on the first detected fault and reverting to fail-safe when both modules have a fault. Fail-safe is defined as the 'de-energized' or 'off' state. A Simplex Input or Output module is SIL 2 capable. Configuring them in a Duplex configuration adds availability but doesn't add to the safety capability

Ethernet

The Ethernet architecture has no effect on SIL 2 safety functions. You can use any appropriate Ethernet network for your application. From a safety aspect, if the Ethernet packets are not sent successfully, then the SIL 2 safety functions go to their respective safe states.

Power Supplies

On de-energize-to-trip, two power supplies can be used if fault tolerance is required on the power supplies.

If only one power supply is used, both of the power connections on the adapter base must be connected to it (system power can be from another power supply to the I/O modules).

For energize-to-action, dual power supplies are required for both the system and field supplies. The system provides the power supply monitoring, but needs to be connected in the application.

I/O Module Considerations

All I/O modules feature status indicators and can also report faults via application variables. All modules provide the following status information:

- Module presence
- Module health and status
- Channel health and status
- Field faults
- An echo of the front panel indicators for each module

Input modules support high availability when configured for duplex operation and using the appropriate termination assembly.

Input modules can be configured to operate in SIL 2 energize-to-action or de-energize-to-trip applications.

The digital output module is rated at SIL 2 as a fail-safe module. Each module provides the following safety functions:

- Output channel signals are based on commands from the controller.
- Redundant voltage and current measurements are sent to the controller for monitoring and diagnostics.
- Modules feature overcurrent and overvoltage channel protection.
- Diagnostic tests are executed on command from the adapter and results are reported back to the adapter.
- On power-up or module insertion, all output channels are set to the de-energized (fail-safe) state until command states are received from the controller. Each channel is driven individually according to the command state values.
- The module enters a Shutdown mode when the time between controller communications exceeds the CRTL.
- If a module fails, then all of its channels are set to the de-energized state.

Output modules support high availability when configured for duplex operation and using the appropriate termination assembly.

The digital output module incorporates line test functionality that can detect and indicate 'no load' field faults. This functionality can be enabled or disabled.

The analog output module can be used in applications where the output current is in the range 4...20 mA during normal operation including trip/action value and where 0 mA is the fail-safe value. The analog output module is rated at SIL 2 as a fail-safe simplex module and when used in a 1oo2 configuration as a duplex module with these features:

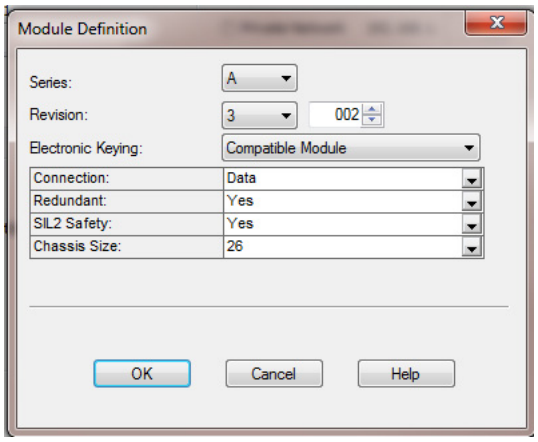
- Commanded values and scaling factor

The fail-safe lowest commanded value irrespective of the scaling factor is 0 mA. The application cannot change the scaling factor; only an online update can change the scaling factor.

The fail-safe guard is 1% (0...2 mA) and not user-configurable.

Configuring 1715 I/O for SIL 2 operation

Before you can use any 1715 modules in a SIL 2 application all 1715 modules, both adapter and I/O, must be configured for SIL 2 safety. This done by selecting YES for 'SIL 2 Safety' in the module properties. If you don't see this field, then you do not have the proper version firmware/software installed. In addition, you must set its connection reaction time limit (CRTL) and module requested packet interval (RPI) and for input modules, you must configure safe state input values.



IMPORTANT See the following document for more information:

Logix Safety certificate - Logix-CT008

One important consideration to set is the Connection Reaction Time Limit. This setting determines how long the connection can operate with old data before going to its configured safe state.

For an input module, if the CRTL expires before the Add-On Instruction detects valid data, the value of the affected input assembly transitions to the configured safe state value. A reset is required before inputs transition from the safe state to field values.

For an output module, if the CRTL expires before the 1715 firmware detects that valid output data is received from the Logix controller the output data transitions to the configured safe state values. In this case, a Reset is required before outputs can be re-energized.

The value of the CRTL forms part of the safety considerations for the system. You are responsible for calculating and verifying that the CRTL meets the safety reaction time for your safety function.

In a 1715 system, the CRTL value is assigned to individual modules during module configuration.

IMPORTANT It is recommended that the CRTL remain at the default of four times the RPI so that one invalid packet does not put the system into the safe state. For example, if the RPI = 120 ms, then consider 480 ms as the minimum CRTL. The information in the next section helps determine the maximum setting for the CRTL.

Use the following method to confirm whether the default value is acceptable or you must change the CRTL value for your application.

This equation governs the value of CRTL for the I/O connections:

$$CRTL \leq \frac{CRTL_{euc}}{2} - \left(\text{sensor delay} + \text{actuator delay} \right)$$

TIP CRTLeuc is the process safety time for the equipment under control (euc).

EXAMPLE Consider a system function using one sensor and one actuator given the following parameters.

- CRTLeuc: 10,000 ms
- Sensor Delay: 250 ms
- Time for actuator (an ESD valve) to fully operate: 1750 ms

In this example, the setting of CRTL for the I/O connections is less than or equal to 3000 ms.

Setting up 1715 SIL 2 Periodic Task Configuration

The most important recommendation is that the task period be set at a rate that allows the overall process safety time of the safety function to be met. See Table 48 in 1715-UM001 for the no fault worst case reaction time formula.

- In the ControlLogix task configuration dialog, set the task period according to the project needs and consider the following:
  a. Leave time for other controller tasks to complete. Even if you do not use any other tasks there are still other internal tasks running, like communications. In other words, if the SIL 2 periodic task is set too low, it is possible to use up all the processing time.
  b. The advantage of a lower task period is that it increases the number of times the Add-On Instruction is scanned; thus processing packets at a faster rate.

Add-On Instructions

IMPORTANT To meet SIL 2 application requirements in a ControlLogix system while using 1715 I/O, you must use the 1715 Add-On Instructions described in the following section.

See chapter 8 of 1715-UM001 from complete information.

IMPORTANT Before you import the Add-On Instructions to your project, you must do the following:

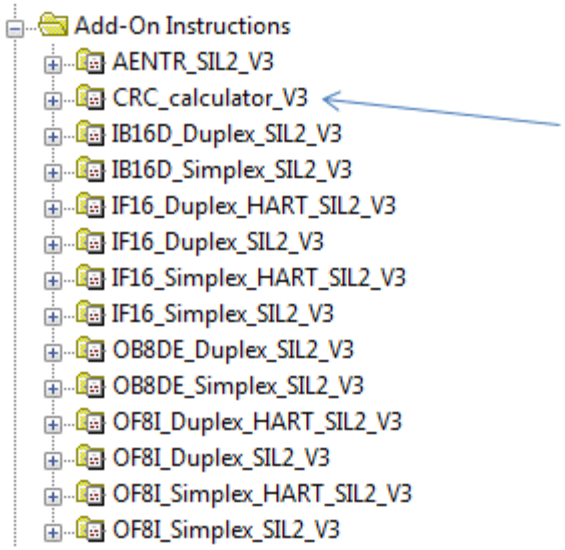
- Add your I/O modules to the project in the I/O configuration tree and configure them properly.
- SIL 2 = Yes must be selected when configuring the module. This creates the data types and tags that you must use in the Add-On Instruction.

The Add-On Instructions provide a mechanism to verify the validity of data that is transferred between the ControlLogix controller and the 1715 adapter. When you use the Add-On Instructions, the sender of the data adds check data to the produced data. The receiver of the data uses the check data to verify the integrity of the consumed data.

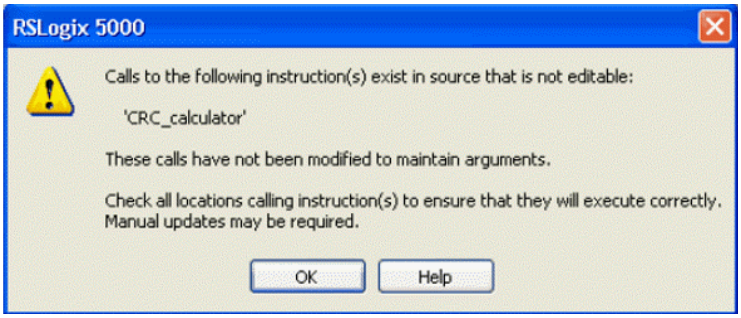
A 1715 SIL 2 Add-On Instruction must be added to the SIL 2 safety program for EACH simplex or duplex 1715 module that has channels that are used within SIL 2 safety function. Note that a duplex module only requires one Add-On Instruction.

1715 SIL 2 Add-On Instructions must be imported into the RSLogix 5000® project. Import only the Add-On Instructions you need based on your SIL 2 configuration. The CRC-calculator Add-On Instruction is imported when you import any of the other Add-On Instructions.

The SIL 2 Add-On Instructions are available from the Product Compatibility and Download Center website.

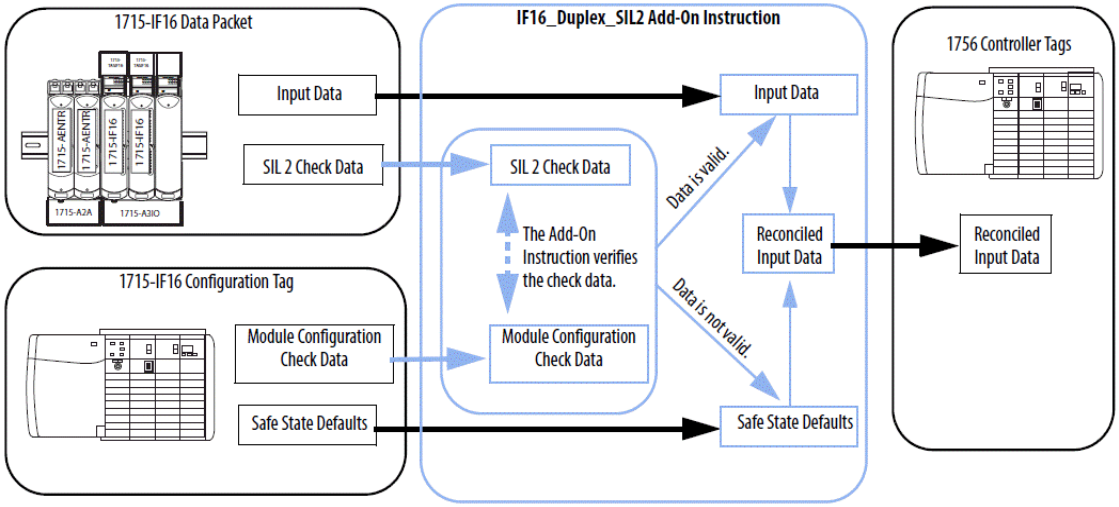


IMPORTANT You see the following warning for each Add-On Instruction import except the first one. Each Add-On Instruction import overwrites the CRC Calculator Add-On Instruction.Click OK to continue.



As you proceed, be aware that when using the 1715 SIL 2 Add-On Instructions, you do not read inputs directly from the input table, nor do you write directly to the output tags. You read inputs from an Add-On Instruction tag that is called 'reconciled input data', and write outputs to an Add-On Instruction tag called 'requested output data.'

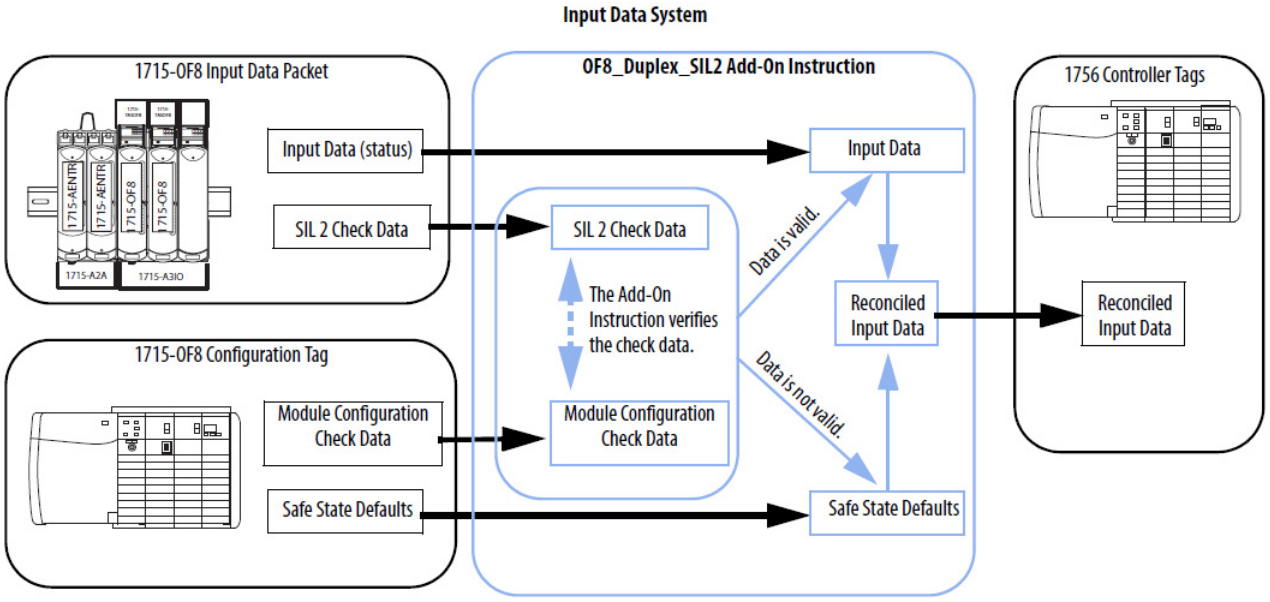
Figure 9 - Module Data Flow



Important: The 1715-IF16 module is shown, but the example also applies to the 1715-IB16D module.

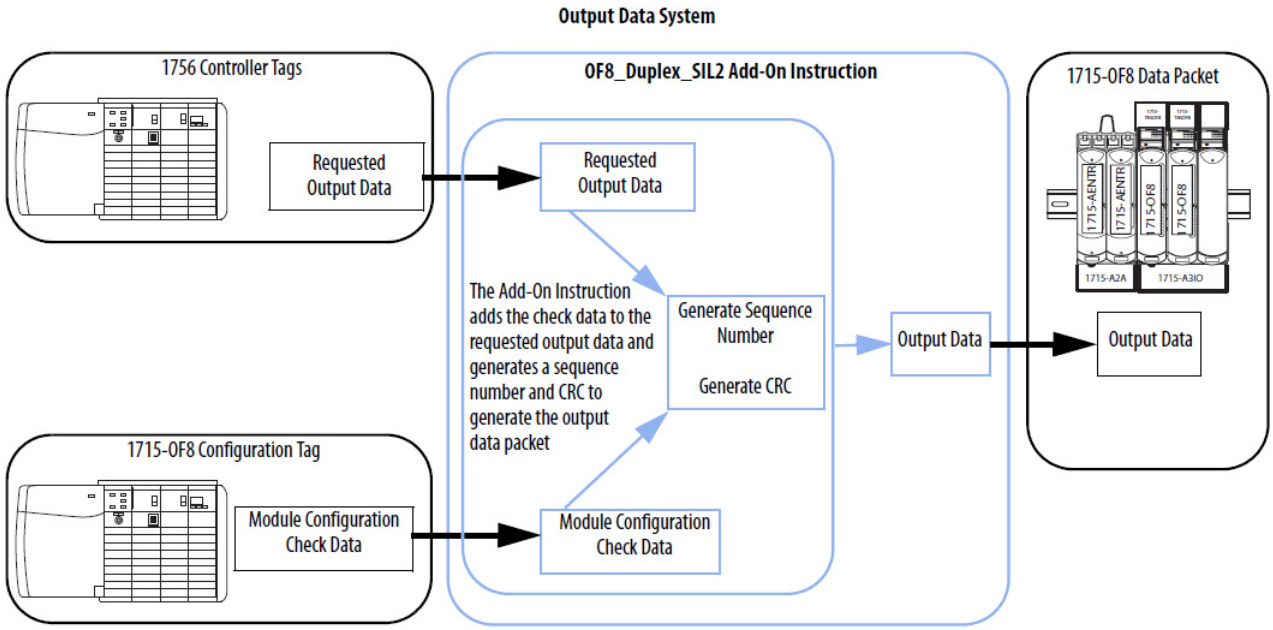
Input Data System

Input modules send data only one way; from the input module to the controller.



Output Data System

Output modules send data both ways. Status is sent from the module to the controller and the controller send output requests to the module.



Important: The 1715-OF8 module is shown, but the example also applies to the 1715-OB8DE module.

Energize-to-Action

Energize-to-action configurations can be used only if the following apply:

- At least two independent power sources must be used for both the system and field supplies. (four total) The system provides the power supply monitoring, but this needs to be connected in the application. You must write application code that monitors the diagnostics for the power supplies. These power sources must provide emergency power for a safe process shutdown or a time span that is required by the application.
- Each power source must feature power integrity monitoring with safety critical input read-back into the system controller or implicit power monitoring that is provided by the I/O modules. Any power failure must trigger an alarm.
- Unless provided implicitly in the I/O modules, all safety-critical inputs and outputs must be fitted with external line and load integrity monitoring and safety-critical read-back of the line-status signals. Any line or load failure must trigger an alarm.
  - See 1715-UM001 for more information on using external line devices, aka End- Of-Line devices.
- The application program must be designed to shut down energize-to-action SIL 2 safety instrumented functions if a faulty adapter or output module has not been replaced within the mean time to restoration (MTTR). That is, you cannot run on one adapter or output module for longer than the MTTR.
- You as the customer decides on the value of MTTR. Two typical values are 8 hours or 10 hours but you must determine the proper value for your application.
- For SIL 2 high demand, energize-to-action applications, you must use two output modules.

In cases where one or more outputs is used in an energize-to-action configuration, all specific requirements that are listed previously must be implemented for all associated inputs.

The user manual also contains all probability of a dangerous failure on demand (PFD) and probability of failure per hour (PFH) values for Energize-to-Action configurations.

Rockwell Automation Support

Use the following resources to access support information.

Technical Support Center	Knowledgebase Articles, How-to Videos, FAQs, Chat, User Forums, and Product Notification Updates.	https://rockwellautomation.custhelp.com/
Local Technical Support Phone Numbers	Locate the phone number for your country.	http://www.rockwellautomation.com/global/support/get-support-now.page
Direct Dial Codes	Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.	http://www.rockwellautomation.com/global/support/direct-dial.page
Literature Library	Installation Instructions, Manuals, Brochures, and Technical Data.	http://www.rockwellautomation.com/global/literature-library/overview.page
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	http://www.rockwellautomation.com/global/support/pcdc.page

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

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

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

Publication 1715-RM001A-EN-P - June 2019