Trusted TMR System

T8094 Issue 40

Rockwell Automation Publication ICSTT-RM459K-EN-P, November 2023
Supersedes Publication ICSTT-RM459J-EN-P, October 2021

Rockwell Automation

Safety 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.

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).

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.

Table of Contents

Summary of changes

This manual includes new and updated information. Use these reference tables to locate changed information.

Grammatical and editorial style changes are not included in this summary.

New or enhanced features

This table contains a list of topics changed in this version, the reason for the change, and a link to the topic that contains the changed information.

Topic name	Reason
Safety-related Configurations on page 34	Updated Peer-to-Peer usage conditions
EN 54 requirements on page 45	Changed "European Standard" to "standard"
Electromagnetic Compatibility (EMC) on page 74	UKCA update
System Power Requirements on page 76	Updated Power Supply Requirements precautionary note
Example I/O Architecture Checklist on page 80	Updated Power Supply Requirements in Table 4.4 checklist
System Security on page 85	Added reference for Network Firewall and precautionary Warning statement for changing default system password
Recommended Proof Test Methods on page 145	Updated 4-20 mA analog inputs (isolated) Proof Test method accuracy
Recommended Proof Test Methods on page 145	Deleted Expansion Channels Communications Path proof test

About this publication

The Trusted Triple Modular Redundant (TMR) System has been designed and certified for use in safety-related applications. To ensure that systems build upon these foundations, it is necessary to impose requirements on the way such systems are designed, built, configured, tested, installed, and commissioned, operated, maintained, and de-commissioned. This manual sets out the requirements to be met during these stages of a safety-related system to ensure that the safety-related objectives of a Trusted TMR System are achieved.

This manual is intended primarily for system integrators and is not intended to be a substitute for expertise or experience in safety-related systems. It is assumed that the reader has a thorough understanding of the intended application and can translate readily between the generic terms used within this manual and the terminology specific to the integrator's or project's application area.

Disclaimer

It is not intended that the information in this publication covers every possible detail about the construction, operation, or maintenance of a control system installation. You should also refer to your own local (or supplied) system safety manual, installation, and operator/maintenance manuals.

Revision and updating policy

This document is based on information available at the time of its publication, however, they are subject to change from time to time. The latest versions of the manuals are available at the Rockwell Automation Literature Library: rok.auto/literature.

The latest issue of the Safety Manual is also referenced at the TÜV Rheinland website:

http://fs-products.tuvasi.com

Latest product information

See the Trusted Release Note for the revision of this document applicable to the release at rok.auto/pcdc.

For the latest information about this product, review the Product Notifications and Technical Notes available at rok.auto/knowledgebase.

Some of the Articles in the Knowledgebase require a TechConnect℠ Support Contract. For more information, go to Knowledgebase Document ID: IP622-TechConnect Support Contract - Access Level & Features.

Tip: Sign in to your Rockwell Automation account to view Knowledgebase articles.

Precautionary information

CAUTION

Caution notices call attention to methods and procedures that must be followed to avoid damage to the equipment.

NOTES

Notes highlight procedures and contain information to assist the user in the understanding of the information contained in this document.

This symbol identifies items that must be thought about and put in place when designing and assembling a Trusted controller for use in a Safety Instrumented Function (SIF).

WARNING:

RADIO FREQUENCY INTERFERENCE

Most electronic equipment is influenced by Radio Frequency Interference (RFI). Caution should be exercised with regard to the use of portable communications equipment around such equipment. Signs should be posted in the vicinity of the equipment cautioning against the use of portable communications equipment.

MAINTENANCE

Maintenance must be performed only by qualified personnel. Otherwise personal injury or death, or damage to the system may be caused.

CAUTION: STATIC SENSITIVE DEVICES

Modules in the Trusted System may contain static sensitive devices that can be damaged by incorrect handling of the module. The procedure for module removal is detailed in the relevant product descriptions and must be followed. All Trusted Systems must have labels fitted to the exterior surface of all cabinet doors cautioning personnel to observe anti-static precautions when touching modules. These precautions are detailed in Chapter 3 of these product descriptions.

Abbreviations

This table describes the abbreviations that are used in this manual:

Abbreviation	Description
1oo2	One-out-of-Two
1oo2D	One-out-of-Two with diagnostics
2oo2	Two-out-of-Two
2oo2D	Two-out-of-Two with Diagnostics
2oo3	Two-out-of-Three
2oo3D	Two-out-of-Three with Diagnostics
DIN	Deutsche Industrie-Norm (German Industrial Standard)
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Emergency Shutdown
EUC	Equipment Under Control
FB	Function Block
IEC	International Electrotechnical Commission
IL	Instruction List
I/O	Input/Output
LD	Ladder Diagram
MooN	M-out-of-N
MTS	Manual Test Start
PC	Personal Computer
PST	Process Safety Times
PSU	Power Supply Unit
SFC	Sequential Function Chart
SFOC	Second Fault Occurrence Time
SIL	Safety Integrity Level
ST	Structured Text
TMR	Triple Modular Redundant
TÜV	Technischer Überwachungs-Verein

Introduction

In this Section

Purpose of safety

The Trusted Triple Modular Redundant (TMR) System has been designed and certified for use in safety-related applications. To ensure that systems build upon these foundations, it is necessary to impose requirements on the way such systems are designed, built, configured, tested, installed, and commissioned, operated, maintained, and de-commissioned. This manual sets out the requirements to be met during these stages of a safety-related system to ensure that the safety-related objectives of a Trusted TMR System are achieved.

This manual is intended primarily for system integrators and is not intended to be a substitute for expertise or experience in safety-related systems. It is assumed that the reader has a thorough understanding of the intended application and can translate readily between the generic terms used within this manual and the terminology specific to the integrator's or project's application area.

Safety Integrity Level (SIL) as defined in the International Electrotechnical Commission (IEC) standard: IEC 61508-4: 2010; Section 3.5.8 is used throughout industry and it is respected by the safety community.

The Trusted TMR System and this manual, in its English version, have been independently reviewed and certified by the German certification authority Technischer Überwachungs-Verein (TÜV Rheinland) to meet the requirements of IEC 61508 SIL 3.

The contents of this manual represent the requirements that shall be fulfilled to achieve certified safety-related systems up to Safety Integrity Level 3 (SIL 3). The conditions and configurations that shall be adhered to if the system is to remain in compliance with the requirements of SIL 3 are clearly marked.

Requirements for quality systems, documentation and competence are included within this document. These are requirements, but are NOT replacements for operating companies' or integrators' quality systems, procedures and practices. The system integrator remains responsible for the

generation of procedures and practices applicable to its business, and shall ensure that these are in accordance with the requirements defined herein. The application of such procedures and practices is also the responsibility of the system integrator, however, these shall be considered mandatory for systems for SIL 3 applications.

Associated documents

The following documents are associated with the safety requirements applicable to the Trusted System or provide supporting information via the TÜV Rheinland web site.

Table 1-1 - Referenced documents

Document	Title
IEC 61508	Functional Safety of Programmable Electronic Systems
IEC 61511	Functional safety: Safety Instrumented Systems for the process industry sector
EN 54-2	Fire Detection and Fire Alarm Systems
NFPA 72:2012	National Fire Alarm Code
NFPA 85:2015	Boiler and Combustion Systems Hazards Code
NFPA 86:2015	Standard for Ovens and Furnaces

An understanding of basic safety and functional safety principles and the content of these standards in particular are highly recommended. The principles of these standards should be thoroughly understood before generating procedures and practices to meet the requirements of this Safety Manual.

Terminology

The terms ‘certification’ and ‘certified’ are used widely within this Manual. Within the context of this Manual, these terms refer to the functional safety certification of the product to IEC 61508 SIL 3. The Trusted System as a product is certified to a wider range of standards that are outside the scope of this Safety Manual.

This Manual contains rules and recommendations:

Rules are mandatory and must be followed if the resulting system is to be a SIL 3 compliant application. These are identified by the term ‘shall’.

Recommendations are not mandatory, but if they are not followed, extra safety precautions must be taken in order to certify the system. Recommendations are identified by `it is highly recommended’.

Safety and functional safety

Safety: The expectation that a system will not lead to risk to human life or health.

Safety is traditionally associated with the characteristics or hazards resulting from the system itself; including fire hazards, electrical safety, etc. The requirements to be satisfied by the integrator here include wiring, protective covers, selection of materials, etc.

Functional Safety: The ability of a system to carry out the actions necessary to achieve or to maintain a safe state for the process and its associated equipment.

Functional safety is considered the ability of the system to perform its required safety function. The requirements on the integrator here are to take the steps necessary to ensure that system is free from faults, errors, and correctly executes the required safety functions.

This manual concentrates on functional safety; it is assumed that the reader is familiar with the methods of achieving basic health and safety standards.

Safety integrity and risk class levels

A Trusted TMR System is certified for use for applications up to SIL 3 for subsections of the system using low density Input / Output (I/O).

SIL is defined in IEC 61508/IEC 61511 as one of four possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related system. SIL 4 system has the highest level of safety integrity; SIL 1 system has the lowest.

However, IEC 61508/IEC 61511 requires that the complete installation meet these requirements in order to achieve an overall SIL. The system covered by this manual forms only a part of such requirements.

Trusted interfacing systems that have CS300, SC300E and Regent I/O Low Density modules are certified as non-interfering to the Trusted System but retain the German Industrial Standard; Deutsche Industrie-Norm (DIN) certification, which is referenced as DIN19250/AK5/AK6 certification of the original Triguard, Regent and Regent+Plus I/O system (see Appendix A on page 87 for Regent and Regent+Plus, Appendix B on page 93 for Triguard, and Appendix C on page 99 for CS300).

Process Safety Time (PST)

Every process has a safety time that is the period that the process can be controlled by a faulty control-output signal without entering a dangerous condition. This is a function of the process dynamic and the level of safety built into the process plant. The Process Safety Time[1] (PST) can range from seconds to hours, depending on the process. In instances where the process has a high demand rate and/or highly dynamic process the PST will be short. For example, turbine control applications may dictate process safety times down to around 100 ms.

The PST dictates the response time for the combination of the sensor, actuators and each realized control or safety function. For demand or event-driven elements of the system, the response time of the system shall be considerably less than:

(PST- Sensor and actuator delay)

For convenience within this document, we will refer to the element of the PST relevant to the system's response time as PST_E, effective PST.

[1] This data must form part of the safety considerations for the system and design reviews must be a fundamental part of safety engineering. The user should appoint an engineer with design knowledge of their installation to determine this data; e.g. a Loss Prevention Engineer.

For cyclic elements of the system, the system's scan time shall be considerably less than the *effective* PST, i.e.:

½ (PST- Sensor and actuator delay), or ½ (PST_E)

The response time in the context of the process safety time must consider the system's ability to respond, i.e. its probability of failure on demand (including its ability to fulfill the required function within the required time). The probability of failure on demand is a function of the system's architecture, its self-test interval and its β-factor[2]. If the system architecture provided no fault tolerance, it would be necessary to ensure that the sum of the response times (including sensors and actuators) and the fault detection time does not exceed the process safety time. In practice, many of a system's self-test intervals vary from seconds to hours depending on the element of the system under test.

Degraded operation

Non-fault tolerant (simplex) systems, by definition, do not have the ability to continue their operation in the presence of fault conditions. If we consider a digital point, the state may be 0, 1, or undefined (X). If there is a fault within a non-fault tolerant system, we would normally assume that the state becomes undefined in the presence of faults. For safety applications, however, it is necessary to be able to define how the system will respond in the presence of faults and as faults accumulate. This is the system's defined degraded operation. Traditionally, 0 is considered the fail-safe state, and 1 considered the operable condition. A standard non-fault tolerant system would therefore be 1 channel operating (or 1-out of-1), degrading to undefined (X) if there is a fault. Obviously, this would be undesirable for safety applications, where we require a fail-safe reaction if there is a fault, a system providing this operation would be 1001 fail-safe, or 1→0.

The additional element in the degradation path is that the fault may occur but may be hidden, or covert. The fault could be such that it prevents the system from responding when required to do so. Obviously, this would also be unacceptable for safety applications. To detect the presence of these covert faults, it is necessary to perform tests, or diagnostics on the system. Detection of the covert fault is then used to force the system to its fail-safe condition. For a non-fault tolerant (simplex) system with diagnostics, this is referred to as 1001D.

Fault tolerant systems have redundant elements that allow the system to continue operation or to ensure that the system fails safely in the presence of faults. For example, a dual system may be One-out-of-Two (1002 also known as 1v2), with either channel able to initiate the fail-safe reaction, or Two-out-of-Two (2002 or 2v2) requiring both channels to initiate the fail-safe

[2] The β-factor is a measure of common cause failure and is dependent on the equipment's original design, which is assessed and certified independently, and the implementation of the guidance provided within this Chapter. The compact nature of a Trusted TMR System provides a β-factor of better than 1%.

reaction. The 1oo2 system provides a greater period between potential failure to respond to a hazard, but a higher probability of spurious responses. The 2oo2 system providing a greater period between spurious responses, but a higher chance of not responding when required. It is also possible to have dual systems with diagnostics to address covert failures and help redress the balance between failure to respond and spurious response. A dual system could therefore be Two-out-of-Two with Diagnostics (2oo2D) reverting to 1oo1D reverting to fail-safe, or 2→1→0.

Consider a simple triplicated system, as shown in Figure 1. The input and output devices are assumed to be simply wired to the input and output channels to provide the requisite distribution and voting. We have assumed that the output vote is a simple majority vote for this purpose.

Tip: With non-Trusted systems, there may be a need for a common output-voting element.

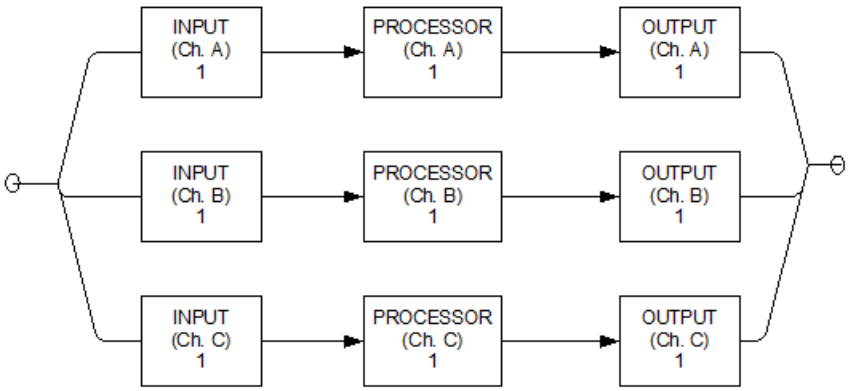


Figure 1: Simple Triplicated System

A failure in any element of each channel, for example, Ch. A INPUT, will result in that complete channel's failure. If this failure is fail-safe, only one of the remaining channels needs to respond to a demand condition to generate the safe reaction. If a second channel fails safe, then the overall system will fail-safe. This is therefore a 3-2-0 architecture. Typically, diagnostics are used to assure the fail-safe state, the operation is therefore Two-out-of-Three with Diagnostics (2oo3D), reverting to One-out-of Two with diagnostics (1oo2D), reverting to fail-safe.

The Trusted TMR System configured in a Triple Modular Redundant (TMR) architecture means that each stage of the system is triplicated, with the results from each preceding stage majority voted to provide both fault tolerance and fault detection. Diagnostics are also used to ensure that covert failures are detected and result in the correct fail-safe reaction. For example, a fault within INPUT Ch. A will be localized to that input, and unlike the standard triplicated system, will allow PROCESSOR Ch. A and OUTPUT Ch. A to continue operation, that is, the input is now operating 1oo2D while the remainder of the system continues to operate 2oo3.

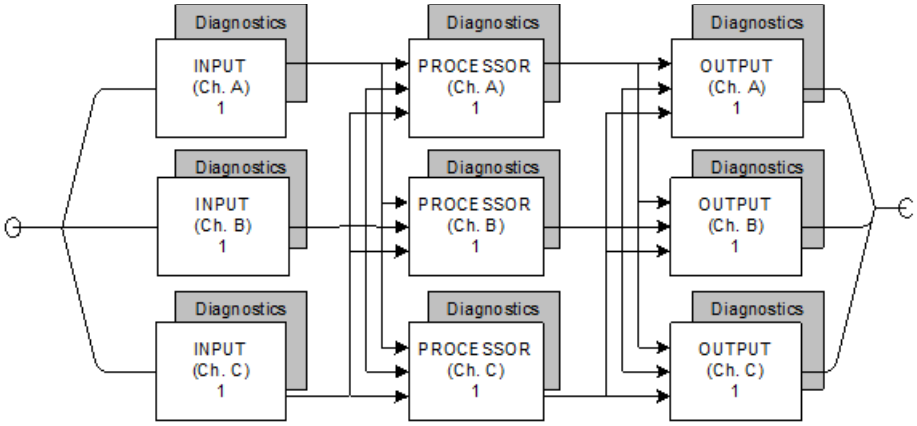


Figure 2: TMR Architecture

The Trusted TMR System uses this Triple Modular Redundant architecture with diagnostics, supporting a 2oo3D reverting to 1oo2D reverting to fail-safe, or 3-2-0 operation. The 1oo2D operation is a transient mode of operation where active and standby modules are installed; in this case, the degradation is 3-2-3-2-0.

The architecture, and hence degradation modes for low density I/O may be selected as required, refer to I/O architectures on page 34 for further details.

The Trusted TMR system overview

A Trusted TMR System is based on a triplicated microprocessor with internal redundancy of all critical circuits. The system controls complex and often critical processes in real time - executing programs that accept external sensor signals, solving logic equations, performing calculations for continuous process control and generating external control signals. These user-defined application programs monitor and control real-world processes in the oil and gas, refining, rail transit, power generation and related industries across a wide range of control and safety applications. A Trusted TMR System is certified for use in safety-related applications such as fire and gas detection, and emergency shutdown up to requirements of IEC 61508 SIL 3.

Write and monitor application programs for the Trusted System by using the AADvance-Trusted SIS Workstation Software (SIS Workstation Software) on

a desktop or laptop running a Windows® 10, Windows 7, Windows 8, Windows Server® 2008 or Windows Server 2012 operating system.

Alternatively, develop application programs with the legacy Trusted Toolset Suite, running on a personal computer (PC) using VMware to provide a Microsoft® Windows NT™, Windows 2000™, or Windows XP™ operating system.

The TMR architecture provides a flexibility that allows each system to be easily adapted to the different needs of any installation. This flexibility permits the user to choose from different levels of I/O fault protection and provides a variety of I/O interfacing and communications methods, allowing the system to communicate with other equipment and field devices.

Those elements of the system that are to be used in safety-related operations are certified to IEC 61508 SIL 3. The remaining elements of the system are certified for non-interfering operation.

This manual covers the release specified in the certified module list.

Safety principles

In this Section

Introduction to safety principles

This section provides an overview of generic safety principles with emphasis on the system integration process. These principles are applicable to all safety-related systems, including, but not limited to a Trusted TMR System.

Safety management

A prerequisite for the achievement of functional safety is the implementation of procedural measures applicable to the safety lifecycle; these procedural measures are collectively referred to as a Safety Management System. The Safety Management System defines the generic management and technical activities necessary for functional safety. In many cases, the Safety Management and Quality systems will be integrated within a single set of procedures.

The safety management system shall include:

- A statement of the policy and strategy to achieving functional safety.
- A Safety Planning Procedure. This safety planning procedure shall result in the definition of the safety lifecycle stages to be applied, the measures, and techniques to be applied at each stage, and responsibilities for completing these activities.
- Definitions of the records to be produced and methods of managing these records, including change control. The change control procedures shall include records of modification requests, the impact analysis of proposed modifications and the approval of modifications. The baseline for change control shall be defined clearly.
- Configuration items shall be uniquely identified and include version information, for example, system and safety requirements, system design documentation and drawings, application software source code, test plans, test procedures and results.
- Methods of ensuring that persons are competent to undertake their activities and fulfill their responsibilities.

Expansion of these requirements is included within the following subsections.

Safety lifecycle

The Safety Lifecycle is designed to structure a system's production into

defined stages and activities, and should include the following elements:

- Scope definition
- Functional requirements
- Safety requirements
- System engineering
- Application programming
- System production
- System integration
- Installation and commissioning
- System safety validation
- System operation and maintenance plan
- System modification
- Decommissioning

The definition of each lifecycle stage shall include its inputs, outputs, and verification activities. It is not necessary to have stages within the lifecycle addressing each of these elements independently; it is important that all of these stages be covered within the lifecycle. Specific items that need to be considered for each of these lifecycle elements are described in the following subsections.

Scope definition

The initial step in the system lifecycle should establish the bounds of the safety-related system and a clear definition of its interfaces with the process and all third-party equipment. This stage should also establish the requirements resulting from the intended installation environment, including climatic conditions, power sources, etc.

In most cases, the client will provide this information. It is necessary to review this information and establish a thorough understanding of the intended application, the bounds of the system to be provided, and its intended operating conditions. An example checklist for the review of the scope definition is given in Table 4-1.

Functional requirements

This stage is to establish the complete set of functions to be implemented by the system. The timing requirements for each of the functions are also to be established. Where possible, the functions should be allocated to defined modes of operation of the process.

For each function, it is necessary to identify the process interfaces involved. Similarly, where the function involves data interchanged with third-party equipment, the data and interface are to be clearly identified. Where non-standard field devices, communications interfaces or communications protocols are required, it is important that the detailed requirements for these interfaces be established and recorded at this stage. In general, the client will provide the functional requirements. It is, however, necessary to collate these requirements into a document, or document set, including any clarification of the functional requirements. In cases where the client provides the functional requirements in an ambiguous form it will be necessary to clarify, document

and establish agreement on the requirements with the client. It is recommended that logic diagrams be used to represent the required functionality. An example checklist for the review of the functional requirements is given in Table 4-2.

Safety requirements

The functional requirements shall be analyzed to determine their safety relevance. Where necessary, additional requirements shall be established to ensure that the plant will fail-safe if there are failures within the plant, the safety-related system, external equipment and communications or the safety-related system's environment.

For each safety-related function the required safety requirements class and safety-related timing requirements shall be defined. The client should supply this information. Where this information is not supplied it shall be established and agreed with the client as part of this phase. It is highly recommended that the client approve the resulting safety requirements. An example checklist for the review of the safety requirements is given in Table 4-3.

System engineering

This stage realizes the safety-related system design. It is recommended that the engineering comprise two stages, the first defining the overall system architecture, and the second detailing the engineering of the architectural blocks.

The overall system architecture shall identify the individual systems. The architecture for these systems and for their subsystems shall include any diverse or other technology elements.

The architectural definition shall include the required safety requirements class for each architectural element and identify the safety functions allocated to that element. Additional safety functions resulting from the selected system architecture shall be defined at this stage. The detailed engineering shall refine the architectural elements and culminate in detailed information for system build. The detailed design shall be in a form that is readable, readily understood, and allows for simple inspection/review.

Tools used within the system engineering process are to be carefully selected, with due consideration of the potential of introduction of error and the required safety requirements class. Where there remains the possibility of error, procedural methods of detecting such errors shall be included within the process.

Safety requirements allocations

The overall system architecture shall define the individual system. The architecture for these systems, and for their subsystems, shall include any diverse or other technology elements. The architectural definition shall also define the required safety requirements class for each architectural element and identify the safety functions allocated to that element. Additional safety

functions resulting from the selected system architecture will be defined at this stage.

The detailed engineering shall refine the architectural elements and culminate in detailed information for system build. The detailed design shall be in a form that is readable, readily understood, and allows for simple inspection/review.

Tools used within the system engineering process are to be carefully selected, with due consideration of the potential for the possibility of introduction of error and the required safety requirements class. Where there remains the possibility of error, procedural methods of detecting such errors shall be included within the process.

Application programming

An overall Application Program software architecture is to be defined. This architecture will identify the software blocks and their allotted functions.

The application architectural design shall be used to define the additional requirements resulting from the system hardware design. Specifically, methods for addressing system-specific testing, diagnostics and fault reporting are to be included.

It is highly recommended that simulation testing be performed on each software block. This simulation testing should be used to show that each block performs its intended functions and does not perform unintended functions.

It is also highly recommended that software integration testing be performed within the simulation environment before hardware-software integration. The software integration testing will show that all software blocks interact correctly to perform their intended functions and do not perform unintended functions.

The development of the application software shall follow a structured development cycle; the minimum requirements of which are:

- **Architectural definition**. The application program shall be divided into largely self-contained 'blocks' to simplify the implementation and testing. Safety and non-safety functions should be separated as far as possible at this stage.
- **Detailed design and coding**. This stage details the design, and implements each of the blocks identified during the architectural definition.
- **Testing**. This stage verifies the operation of the application; it is recommended that the application blocks first be tested individually and then integrated and tested as a whole. This should be initially undertaken within the simulation environment.

The resultant Application Programs shall be integrated with the system hardware and integration testing performed.

The system production stage implements the detailed system design. The production techniques, tools, and equipment used within the production

testing of the system shall be commensurate with the required safety requirements class.

This stage shall integrate the Application Programs with the target systems. Where multiple systems are used to meet the overall requirement, it is suggested that each system undergoes individual application program and target system integration before overall system integration is performed. To meet the requirements of the intended safety requirements class, the system integration shall ensure the compatibility of the software and hardware.

The system installation stage shall define the steps to be undertaken to ensure that the system is installed correctly and commissioned on the plant. These steps shall include the physical and electrical installation of the system.

The installation environment is a potential source of common cause failure. Therefore, it is vital that compatibility of the equipment is established. The `environment` for these purposes includes the climatic, hazardous area, power, earthing, and EMC conditions. In many cases, there may not be a single installation environment. Elements of the system may be installed in differing location, such as, central control room, equipment rooms and field installations. In these cases, it is important to establish the equipment and environment compatibility for each site.

The first step in the installation sequence is typically the physical installation of the system. Where the system comprises a number of physically separate units, it is important that the sequence of installation be established. This may include the installation of termination facilities before the remaining elements of the system. In these cases, it is important to establish that independent installation and testing facilities are available.

Each installation shall be designed to ensure that the control equipment is not operated in environments that are beyond its design tolerances. Therefore, consideration should be given to the proper control of temperature, humidity, vibration and shock, as well as adequate shielding and earthing to ensure that exposure to electromagnetic interference and electrostatic discharge sources are minimized.

The commissioning stage is to establish the system hook-up and verify its correct ‘end-to-end’ functionality, including the connection between the Trusted TMR system and the required sensors and final elements. It is likely that groups of functions are commissioned rather than the system as a whole, that is, accommodation area functions before production functions. In these cases, it is important to establish the commissioning sequence and the measures to be taken to maintain safe operation during periods of partial commissioning. These measures shall be system-specific and shall be defined clearly before commissioning. It is important to establish that any temporary measures implemented for test purposes or to allow partial commissioning are removed before the system, as a whole, becomes live.

Records shall be maintained throughout the commissioning process. These records shall include records of the tests completed, problem reports, and resolution of these problems.

Safety system validation shall test the integrated system to ensure compliance with the requirements specification at the intended safety requirements class. The validation activities should include those necessary to establish that the required safety functions have been implemented under normal startup, shutdown, and abnormal fault modes.

The validation shall ensure that each functional safety requirement has been implemented at the required safety integrity level, and that the realization of the function achieves its performance criteria, such as, but not limited to the SIF response time having been validated as being within the acceptable process safety time limits. The validation shall also consider potential external common cause failures (for example, power sources, environmental conditions) such that the influence of these external causes of failure is understood and that measures can be applied to ensure that the system does not exceed its published capabilities.

This Operation and Maintenance requirement is designed to maintain functional safety beyond the design, production, installation and commissioning of the system. The in-service operation and maintenance is normally beyond the system integrator responsibility. However, guidance and procedures shall be provided to ensure that the persons or organizations responsible for Operation and Maintenance maintain the intended safety levels.

The Operating and Maintenance Plan shall include the following:

- Although a Trusted TMR product requires no specific power-up and power-down requirements, it is possible that the project-specific implementation will dictate specific action sequences. These sequences shall be clearly defined, ensuring that the sequences cannot result in periods of the system's inability to respond safely while a hazard may be present.
- The Maintenance Plan shall detail the procedures to be adopted when recalibrating sensors, actuators and I/O modules. The recommended calibration periods shall also be included.
- The Maintenance Plan shall include the procedure to be adopted for testing the system, and the maximum intervals between manual testing.
- Sensor and actuator maintenance will require the application of overrides in certain circumstances. Where these are required, they shall be implemented in accordance with the guidance provided within this document.

Planned maintenance

In most system configurations, there will be some elements that are not tested by the system's internal diagnostics. These may be the final passive elements in some I/O modules types, the FTAs which provide the interface with the sensors, the actuators themselves, and the field wiring. A regime of Planned Maintenance testing shall be adopted to ensure that faults do not accumulate within those elements that could ultimately lead to the system's inability to perform its required safety functions. The maximum interval between these tests shall be defined during the system design, that is, before installation. It is highly recommended that the test interval be less than 12 months.

Refer to Appendix F on page 145 for recommended Proof Test methods.

Refer to Environmental requirements on page 72 for environmental requirements that must be maintained over the operating lifetime of system configurations.

Field device maintenance

During the lifetime of the system, it will be necessary to undertake a number of field maintenance activities that will include recalibration, testing, and replacement of devices. Facilities should be included within the system design to allow these maintenance activities to be undertaken. Similarly, the operating and maintenance plan needs to include these maintenance activities, and their effect on the system operation and design. In general, adequate provision for these measures will be defined by the client, and provided the facilities, i.e. maintenance overrides, are implemented within the requirements specified within this document. No further safety requirements will be required.

It is highly recommended that the I/O forcing capability NOT be used to support field device maintenance; this facility is provided to support application testing only. Should this facility be used, the requirements defined in Input and output forcing on page 55 shall be applied.

Module fault handling

When properly configured and installed, a Trusted TMR system is designed to operate continuously and correctly even if one of its modules has a fault. When a module does have a fault, it should be replaced promptly to ensure that faults do not accumulate and cause multiple failure conditions that could result in a plant shutdown. All modules permit live removal and replacement, and modules within a fault-tolerant configuration can be removed with no further action. Modules that do not have a partner slot or smart slot configured and have a fail-safe configuration will require the application of

override or bypass signals for the period of the module removal to ensure that unwanted safety responses are not generated inadvertently.

On-site repair of modules is not supported; all failed modules should be returned for repair and/or fault diagnosis. The return procedure for modules should include procedures to identify the nature and circumstances of the failure and the system response. Records of module failures and repair actions shall be maintained.

Monitoring

In order to establish that the safety objectives have been met through the lifetime of the system, it is important to maintain records of the faults, failures, and anomalies. This requires the maintenance of records by both the end user and the system integrator. The records maintained by the end user are outside the scope of this document; however, it is highly recommended that the following information be included:

- Description of the fault, failure or anomaly
- Details of the equipment involved, including module types and serial numbers where appropriate
- When the fault was experienced and any circumstances leading to its occurrence
- Any temporary measures implemented to correct or work-around the problem
- Description of the resolution of the problem and reference to remedial action plans and impact analysis

Each system integrator should define the field returns, repair, and defect handling procedure. The information requirements placed on the end user because of this procedure should be clearly documented and provided to the end user. The defect handling procedure shall include:

- Method of detecting product-related defects and the reporting of these to the original designers.
- Methods for detecting systematic failure that may affect other elements of the system or other systems, and links to the satisfactory resolution of the issues.
- Procedures for tracking all reported anomalies, their work around, and/or resultant corrective action where applicable.

Design changes will inevitably occur during the system lifecycle; to ensure that the system safety is maintained, such changes shall be carefully managed. Procedures defining the measures to be adopted when updating the plant or system shall be documented. These procedures shall be the responsibility of the end user. The system integrator shall provide sufficient guidance to ensure that these procedures maintain the required level of functional safety. Special consideration shall be given to the procedures to be adopted if there

are product-level updates and enhancements such as module and firmware updates. Updates to the system shall include considerations of the requirements for application changes and firmware changes. These procedural measures shall include:

- Requirement to undertake impact analysis of any such changes
- The measures to be implemented during the modification to the system and its programming. These measures shall be aligned with the requirements within this document. Specifically, the requirements defined in sections Safety management on page 21 to Installation and commissioning on page 25 shall be applied, as well as the additional requirements defined in this section.
- The definition of these procedures shall include the review and authorization process to be adopted for system changes.

Baselines

Baselines shall be declared beyond which any change shall follow the formal change management procedure. The point within the lifecycle at which these baselines are declared depends on the detail of the processes involved, the complexity of the system, how amenable to change these processes are, and the required safety requirements class. It is recommended that the baseline for formal change process is the completion of each step in the lifecycle. However, as a minimum the baseline shall be declared before the presence of the potential hazards, that is, before startup.

Modification records

Records of each requested or required change shall be maintained. The change management procedure shall include the consideration of the impact of each of the required/requested changes before authorizing the implementation of the change. The implementation of the change should repeat those elements of the lifecycle appropriate to the change. The test of the resultant changes should include non-regression testing in addition to test of the change itself.

Decommissioning

The procedure for decommissioning the system shall be defined. This procedure is to include any specific requirements for the safe decommissioning of the system and, where applicable, the safe disposal or return of materials.

As with commissioning, it is likely that the decommissioning be performed in a phased manner. The decommissioning procedure shall ensure that a plan be developed that maintains the functional safety while the corresponding hazards are present. Similarly, the installation environment of the control equipment shall be maintained within its operating envelope while it is required to function.

- The decommissioning plan shall identify the sequence of removal of hazards.
- Methods shall be defined to ensure that the interaction between safety functions can be removed without initiating safety responses and still maintain safety functionality for the remaining potential hazards. This shall include the interaction between systems.
- The decommissioning procedure shall define which modules/materials are to be returned for safe disposal following decommissioning

The functional safety assessment process shall confirm the effectiveness of the achievement of functional safety for the system. The functional safety assessment, in this context, is limited to the safety-related system and will confirm that the system is designed, constructed, and installed in accordance with the safety requirements.

Each required safety function and its required safety properties shall be considered. The effects of faults and errors within the system and application programs, failure external to the system and procedural deficiencies in these safety functions are to be considered.

The assessments are to be undertaken by an audit team that shall include personnel outside of the project. At least one functional safety assessment shall be performed before the presence of the potential hazards, that is, before startup.

The achievement of functional safety requires the implementation of the safety lifecycle and ensuring that persons who are responsible for any safety lifecycle activities are competent to discharge those responsibilities.

All persons involved in any safety lifecycle activity, including management activities, shall have the appropriate training, technical knowledge, experience, and qualifications relevant to the specific duties they have to perform. The suitability of persons for their designated safety lifecycle activities shall be based on the specific competency factors relevant to the particular application and shall be recorded.

The following competence factors should be addressed when assessing and justifying the competence of persons to carry out their duties:

- Engineering experience appropriate to the application area.
- Engineering experience appropriate to the technology.
- Safety engineering experience appropriate to the technology.
- Knowledge of the legal and safety regulatory framework.
- The consequences of failure of the safety-related system.
- The safety requirements class of the safety-related systems.
- The novelty of the design, design procedures, or application.
- Previous experience and its relevance to the specific duties to be performed and the technology being employed.

In all of the above, higher risk will require increased rigor with the specification and assessment of the competence.

System recommendations

In this Section

Introduction to system recommendations

This paragraph expands on and applies the safety principles described earlier in this Manual. Many of the recommendations within this paragraph are equally applicable to other safety-related systems. However, the details of the recommendations or requirements are specific to the Trusted TMR system.

Processor performance

The introduction of the T8111 (Series B) Processor module brings both performance gains and memory usage changes over the T8110B (Series A) Processor version. These changes will benefit most users, especially when migrating from an existing Series A application, it does however require caution under the following conditions:

When a new SIS is designed, installed, and validated based on using the T8111 Processor, replacing that processor with a T8110B version will increase the SIF response time on the order of 2:1 (or greater). Care must be taken in the impact analysis to ensure that response times of SIFs have not been adversely affected.

When a new SIS is designed, installed, and validated based on using the T8111 Processor and the application size approaches 100% utilization (~960 Kb), replacing that processor with a T8110B may not work due to its slightly smaller available application memory space. Care must be taken in the impact analysis to verify that the application will load correctly into a T8110B Processor.

I/O architectures

The Trusted System has comprehensive internal diagnostics that reveal both covert and overt failures. The hardware implementation of many of the fault tolerance and fault detection mechanisms provides for rapid fault detection for most system elements. Self-test facilities used to diagnose faults within the remainder of the system are defined to provide optimum safety availability. These self-test facilities may require short periods of offline operation to introduce conditions, i.e. alarm or fault test conditions, which effectively result in the point being offline within that redundant channel. Within TMR configurations, this period of offline operation only affects the system's ability to respond under multiple fault conditions.

The Trusted TMR Processors, Interfaces, Expander Interfaces, and Expander Processors are all naturally redundant and have been designed to withstand multiple faults and support a fixed online repair configuration in adjacent slots and therefore require little further consideration. The input and output modules support a number of architecture options, the effects of the chosen architecture should be evaluated against the system and application-specific requirements.

FTA modules and other ancillaries are suitable for use as part of Trusted safety system even though they may not explicitly include a TÜV mark.

Safety-related configurations

Refer to this topic for safety-related configurations.

Table 3-1 - Central Modules

Functions/Module	IEC 61508 Certified Configuration	Conditions
Trusted TMR Processor T8110B (IRIG-B) T8110C (see Note) T8111C (see Note)	2oo3	Certified as safety-related and can be used for safety-critical applications up to SIL 3 in single module or active/standby configurations. IRIG-B functionality is interference free and cannot be used for safety functions
Peer to Peer Software board definitions dxpdi16, dxpdo16	Certified for use over single or multiple communication networks	Certified as safety-related and can be used for safety-critical communication up to SIL 3 applications.

Table 3-1 - Central Modules

Functions/Module	IEC 61508 Certified Configuration	Conditions
Peer to Peer Software board definitions dxpai16, dxpao16, dxpdi128, dxpdo128, dxpai128 & dxpao128	Certified for use over single or multiple communication networks	Certified as safety-related and can be used for safety critical communications up to SIL 3 applications provided two separate Dxpai16 & Dxpao16, Dxpdi128 & Dxpdo128, or Dxpai128 & Dxpao128 software board definition pairs are defined and used for safety values. The safety values from the duplicate software board definitions must be compared, with equivalency verified, within the receiving application.
Trusted TMR Interface 8160	Non-interfering	Certified as non-interfering to the Trusted controller but retains DIN19250/AK5 certification of the original Regent and Regent+Plus I/O system (refer to Appendix A) when used to migrate applications to the Trusted Controller in accordance with this manual, publication ICSTT-RM255 (PD-T8160), and taking account of guidance in NAMUR 126.
SC300E Bridge Module 8161	Non-interfering	Certified to SIL 3 IEC 61508 Ed 1 of the original SC300E system (refer to Appendix B) when used to migrate applications to the Trusted Controller in accordance with this manual and publication ICSTT-RM403 (PD-8161) and taking into account of guidance in NAMUR 126.
CS300 Bridge Module 8162	Non-interfering	Certified as non-interfering to the Trusted controller but retains DIN19250/AK6 certification of the original CS300 system (refer to Appendix C on page 99) when used to migrate applications to the Trusted Controller in accordance with this manual and publication ICSTT-RM404 (PD-8162), and taking account of guidance in NAMUR 126.
Trusted Communication Interface T8150 / T8151 / T8151B / T8151C	Not safety-related but interference free	Certified as non-interfering safety-related and can be used for safety-critical communication up to SIL 3 as part of the black channel in single or dual module configurations.
Trusted Expander Modules (XIM / XPM) T8310 / T8310C / T8311 / T8311C	Not safety-related but interference free 2oo3	Certified as non-interfering safety-related and can be used for safety-critical communication up to SIL 3 as part of the gray channel in single module or active/standby configurations.
Trusted Fiber TX/RX Unit T8314 / T8314C	Not safety-related but interference free 2oo3	Certified as non-interfering safety-related and can be used for safety-critical communication up to SIL 3.

Note: Module numbers ending in "C" are conformal coated versions. Conformal coated printed circuit boards in these modules are coated during manufacture. The coating meets defense and aerospace requirements and is approved to US MIL Specification MIL-1-46058C, which meets the requirement for IPC-CC-830. The coating is also UL-recognized.

Table 3-2 - Input Modules High Density I/O

Functions/Module	IEC 61508 Certified Configuration	Conditions
Trusted Digital Inputs T8403, Triplicated, 24V DC T8423, Triplicated, 120V DC T8425, Triplicated, 120V DC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42.

Table 3-2 - Input Modules High Density I/O

Functions/Module	IEC 61508 Certified Configuration	Conditions
Trusted Digital Inputs T8402, Dual, 24V DC T8402C, Dual, 24V DC	Internal 1oo2D (1oo2 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42. Time-limited operation in degraded mode
Trusted Digital Inputs T8424, Triplicated, 120V AC T8424C, Triplicated, 120V AC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42.
Trusted Analog Inputs T8431, Triplicated T8431C Triplicated T8433, Triplicated, isolated T8433C Triplicated Isolated	Internal 2oo3 (2oo3 implemented in a single module)	Within the manufactures specified safety accuracy limits. The safety state of the analog input has to be defined to 0 mA/0 V Certified up to SIL 3.
Trusted Analog Inputs T8432, Dual T8432C, Dual	Internal 1oo2D (1oo2 implemented in a single module)	Within the manufactures specified safety accuracy limits. The safety state of the analog input has to be defined to 0 mA/0 V Certified: up to SIL 3 Time-limited operation in degraded mode.

Table 3-3 - Output Modules High-Density I/O

Functions/Module	IEC 61508 Certified Configuration	Conditions
Digital Outputs T8451, Triplicated 24V DC T8451C, Triplicated 24V DC T8461, Triplicated 48V DC T8461C, Triplicated 48V DC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42. May be used in single module or active/standby configurations.
Digital Outputs T8471, Triplicated 120V DC T8471C, Triplicated 120V DC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only applications where the Proof Test frequency >> frequency of Demands and that fulfill the requirements under Energize to trip configurations on page 42. May be used in single module or active/standby configurations.
Digital Outputs T8472, Triplicated 120V AC T8472C, Triplicated 120V AC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42. May be used in single module or active/standby configurations.
Analog Outputs T8480 Analog Output 4-20 mA T8480C Analog Output 4-20 mA	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical output devices.

Table 3-4 - Multi-purpose Modules, High-Density I/O

Functions/Module	IEC 61508 Certified Configuration	Conditions

Table 3-4 - Multi-purpose Modules, High-Density I/O

Functions/Module	IEC 61508 Certified Configuration	Conditions
Speed Monitor Module T8442, Triplicated, T8442C, Triplicated Conformal,	Internal 2oo3 (2oo3 implemented in a single module)	Inputs: Within the manufactures specified safety accuracy limits. Outputs: De-energize to trip relays. Normally open or Normally closed Contacts can be used Certified up to SIL 3.
Pulse Generator T8444, Triplicated, 24V DC	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical devices.
Zone Interface T8448 Triplicated, 24V DC T8448C Triplicated, 24V DC	Internal 2oo3 (2oo3 implemented in a single module)	Outputs: De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42. May be used in single module or active/standby configurations. Inputs: De-energize to trip: certified only if the inputs are dynamically transitioned at a period not greater than the second fault occurrence time (SFOC). Energize to trip: only for applications that fulfill the requirements under Energize to trip configurations on page 42, and only for "trip amplifier" (like gas inputs) or quasi digital inputs (like fire loops). Analog measurements: certified only if the input is dynamically exercised over its full range within a period shorter than the SFOC. Non-interfering for non-safety-critical devices
Valve Monitor T8449, Triplicated, 24V DC T8449C, Triplicated, 24V DC	Internal 2oo3 (2oo3 implemented in a single module)	Inputs: Certified as non-interfering and can be used for non-safety-critical devices. Outputs: De-energize to trip: certified up to SIL 3. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42. Safety-critical valve may only be tested towards the safe position. May be used in single module or active/standby configurations.

Table 3-5 - Auxiliary Modules

Functions/Module	Conditions
Controller Chassis T8100	Certified as safety-related and can be used for safety-critical applications up to SIL 3
Expander Chassis T8300	Certified as safety-related and can be used for safety-critical applications up to SIL 3
Power Supply Rack T820X	Certified as safety-related and can be used for safety-critical applications up to SIL 3
15V DC Power Supply Unit T8220, 110 - 220V AC, Dual Input	Providing reinforced insulation according to EN 60950-1
24V DC Power Supply Unit T8225, 110 - 220V AC, Dual Input	Providing reinforced insulation according to EN 60950-1

Note: Revisions of modules are subject to change. A list of the released versions is held by TÜV or can be obtained from Rockwell Automation.

Trusted high-density I/O

The Trusted High-Density I/O modules are either inherently triplicated or dual redundant with comprehensive self-test and diagnosis facilities. Self-tests are coordinated so that a majority can be completed, even when there is a demand during the execution of the tests. Discrepancy and deviation monitoring further enhance the verification and fault detection. The TMR Processor tests internal interfaces to the controller. The culmination of these measures results in high levels of fault detection and tolerance, ultimately leading to fail-safe operation if there are multiple fault conditions. The worst case fault detection times on system memory for Trusted Modules are as follows:

Module	Worst Case	Average Detection Time
Output Modules	1.0 hours	0.5 hours
Input Modules	0.5 hours	0.25 hours
Processor modules	24 hours	12 hours [Galpat diagnostics] 1 second [operational read]

In all cases, even in the presence of a fault during this period, the system will continue to be able to respond. Under multiple fault conditions the second fault detection period within the repair time may need to be considered where the system is used in high or continuous demand safety applications.

All High-Density I/O modules include line-monitoring facilities; it is recommended that these facilities be enabled for safety-related I/O. For energize to trip I/O these facilities shall be enabled, see Energize to trip configurations on page 42.

Safety wiring principles shall be employed for field loops if it is necessary for the user to guard against short circuit faults between I/O channels (for example, to comply with NFPA 72 requirements). The Trusted modules' internal diagnostics do not detect all external short circuits between IO channels.

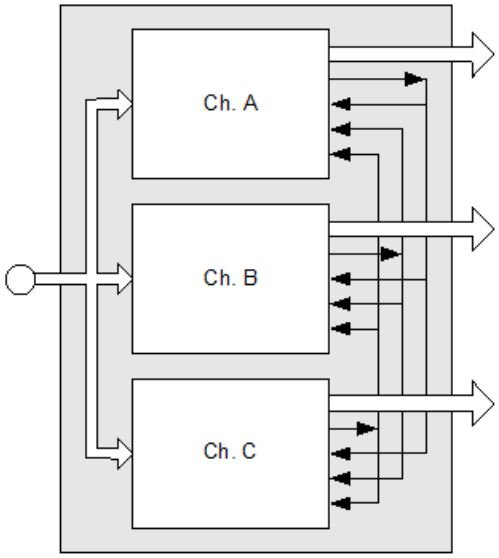


Figure 3: Single High-Density TMR I/O Module Architecture

The system supports a single High-Density TMR I/O module architecture, where it is acceptable to either stop the system or allow the signals corresponding to that module to change to either their default state, or to their active-standby configuration. The first active-standby configuration is to accommodate the active and spare modules in adjacent slot positions; the second is to use the SmartSlot configuration where a single module position may be used as the spare for a number of active modules. All configurations may be used for safety-related applications; the choice between the configurations supporting live online repair is dependent on the end-user's preference and the number of faulty modules to be repaired simultaneously.

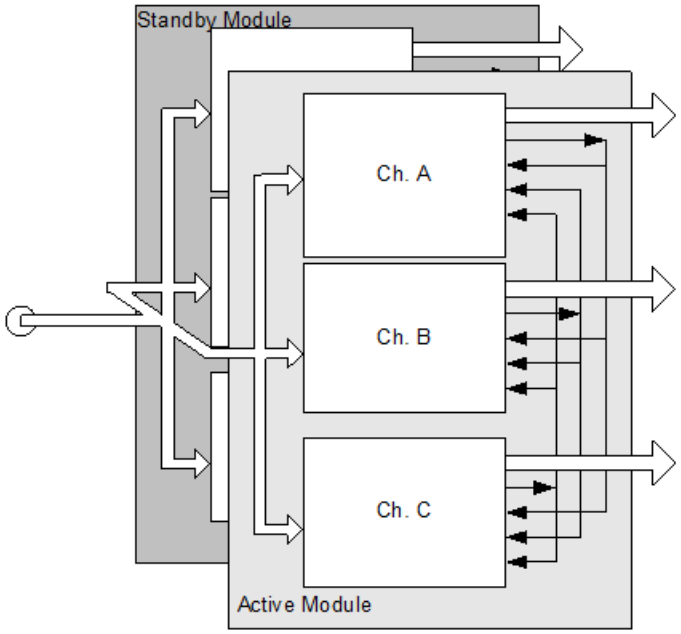


Figure 4: SmartSlot or Adjacent Slot TMR Module Configuration

The High-Density I/O modules support the system's inherent TMR architecture. To annunciate the failure, diagnostic and status information is provided within the corresponding module information available to the application programmer. Faults will also result in the generation of the corresponding front panel indication on the I/O module and the system healthy indicator and status output.

A majority fault condition on an I/O point, that is, a fault beyond its fault tolerant capability, results in a fail-safe logical state (logical 0). The input state is forced to "unknown", state 0x07 in this condition and the analog level to 2048. The module fault status and fault codes will be set accordingly, and may be optionally used for remote diagnosis purposes.

A High-Density Dual Input module operating in a degraded mode must be repaired within the MTTR that was used for calculation and validation of the SIL achieved by the safety function; or, compensating measures must be taken (proof testing) in order to maintain safe operation. The maximum duration between these proof tests (the proof test interval) depends on the specific process and must be specified individually for each application. For a specific system configuration this time can be determined through a quantitative analysis of the demand rate used in the assessment of the safety function. The ratio of the proof test rate (which is the inverse of the proof test interval) to the demand rate must equal or exceed 100. If no analysis is available, the maximum proof test interval for degraded operation shall be no greater than 72 hours for SIL 3 safety-related applications.

When a High-Density Dual Input module channel is operating in non-degraded mode, if a channel state discrepancy occurs and no module fault is detected, the channel state reported to the application will always be the lower of the two states for a digital module and the higher of the two states for an analog module.

When a High-Density Dual Input module is operating in non-degraded mode, if a channel voltage discrepancy occurs (that exceeds the configured discrepancy limits) and no module fault is detected, the channel state reported to the application will always be the safe state.

In safety-critical applications, the channel discrepancy alarms shall be monitored and alarmed to the operator.

The I/O modules use the active-standby arrangement to support bumpless online repair. The module architecture allows the faulty module to continue normal service until a replacement module is available and unlike conventional hot-standby configurations, allows for a controlled transfer even in the presence of a fault condition. The standby module may be permanently installed to reduce the repair time to an absolute minimum.

High-Density I/O modules must not be inserted into a Trusted TMR Processor partner slot. This will damage the active Trusted TMR Processor's partnering capability, and if the I/O module is subsequently removed and a standby TMR Processor is installed, then both TMR Processors will shut down and the system outputs will revert to the safe condition.

Analog input safety accuracy

When High-Density analog input modules are used, the system uses the median value. The deviations between the redundant channels' measurements are monitored to determine if they are within the safety accuracy limit, refer to the associated module's Product Description for its safety accuracy specification. When a single channel measurement exceeds the safety accuracy limit, then a discrepancy alarm is set for the input channel. Furthermore, should two or more redundant channel measurements exceed the safety accuracy limit, then the reported channel value is set to -2048 and the channel line fault status is set to True.

In safety-critical applications, the line fault status shall be monitored by the application program and used to initiate the appropriate safety function when two or more slice readings for a channel exceed the safety accuracy limit. Furthermore, the discrepancy alarms should be monitored and alarmed to the operator.

Energize to trip configurations

Certain applications may require normally open (energize to trip) input and energize to trip outputs.

Energize to trip configurations shall only be used if:

- the activation of the system is only mitigating an already existing hazard such as in fire and gas applications SIL 1 to SIL 3, or
- the activation of the system is a hazard itself and the system is used in a SIL 1 to SIL 3 application for Trusted modules and compliant application for 7000 series modules (Regent and Regent+Plus modules, see Appendix A on page 87).

Additionally the following restrictions apply:

- At least two independent power sources must be used. These power sources must provide emergency power for a safe process shutdown or a time span required by the application.

- Each power source must be provided with power integrity monitoring and safety-critical input readback into the Trusted TMR Processor, or implicit power monitoring provided by the I/O modules. Any power failure shall lead to 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 readback of the line-status signals. Any line or load failure shall lead to an alarm.
- Only modules specifically identified for the use in restricted energize to trip configurations shall be used.

If energize to trip safety-related outputs are used, line fault conditions shall be monitored by the system application and alarmed to plant operations personnel. Line monitor devices shall be installed as close to the field sensor (or actuator if required) as is practicable. Line fault status shall be monitored by the system application and alarmed to plant operations personnel.

Line monitoring may also be used in de-energize to trip safety-critical input applications but is not specifically required.

When isolation barriers are used in safety-critical applications, line monitoring thresholds shall be configured to detect barrier faults. This ensures that barrier faults do not inhibit the safety-critical function.

EN 60204 Category 0 and 1 configurations

The system is fully compliant for use with category 0 application (de-energize to trip).

Category 1 configurations require a controlled stop with power available to the machine actuators to achieve the stop and then removal of power.

The Trusted TMR System has a defined internal fail-safe state as energize-to-trip. This could result in the defined shutdown delay being shortened in some cases of I/O failure, CPU failure, or loss of power to the system.

NFPA 72 requirements

The Trusted System is certified to be used in NPFA 72 compliant fire alarm systems.

The systems should be designed and integrated in accordance with NFPA 72. In particular, the following shall be applied.

- Unless otherwise permitted, all field loops to sensors and actuators, inter-system and subsystem signal wiring, and communications links shall be line monitored for single open & short circuits.

NFPA 85 requirements

The Trusted TMR System is certified to be used in NFPA 85 compliant systems.

The systems should be integrated in accordance with NFPA 85. In particular, the following shall be applied:

- The operator shall be provided with a dedicated manual switch that shall independently and directly actuate the safety shutdown trip relay. At least one identified manual switch shall be located remotely from the boiler where it can be reached if there is an emergency.
- The burner management system shall be provided with independent logic, independent input/output systems, and independent power supplies and shall be a functionally and physically separate device from other logic systems, such as the boiler or HRSG control system.
- Momentary Closing of Fuel Values. Logic sequences or devices intended to cause a safety shutdown, once initiated, shall cause a burner or master fuel trip, as applicable, and shall require operator action before resuming operation of the affected burners. No logic sequence or device shall be permitted that allows momentary closing and subsequent inadvertent reopening of the main or ignition fuel valves.
- Documentation shall be provided to the owner and operator, indicating that all safety devices and logic meet the requirements of the application.
- System response time (that is, throughput) shall be sufficiently short to help prevent negative effects on the application.
- When a single transmitter input is used as one of the initiators of the BMS interlock system[3] consideration shall be given to the failure mode caused by drift of the analog input sense resistor, a recommended solution to this failure mode is the use of two analog input channels, where the two values are compared to provide an indication that drift has caused a discrepancy between the inputs.

NFPA 86 requirements

The Trusted TMR System is certified to be used in NFPA 86 compliant systems. The systems should be integrated in accordance with NFPA 86. In particular, the following shall be applied:

- The supplier of the application software for the programmable controller shall provide the end user, and the authority having jurisdiction, with the documentation needed to verify that all related safety devices and safety logic are functional before the programmable controller is placed in operation.
- If there is a power failure, the programmable controller (hardware and software) shall not prevent the system from reverting to a safe default condition. A safe condition shall be maintained upon the restoration of power.

[3] An example of the Interlock System is defined in figure 6.4.1.2.1 of NFPA 85.

- The control system shall have a separate manual emergency switch, independent of the programmable controller that initiates a safe shutdown.
- Any changes to hardware or software shall be documented, approved, and maintained in a file on the site.
- System operation shall be tested and verified for compliance with this standard and the original design criteria whenever the programmable controller is replaced, repaired, or updated.
- Whenever application software that contains safety logic or detection logic is modified, system operation shall be verified for compliance with this standard and the original design criteria.
- The NFPA certification is only applicable where the system is applied in accordance with the safety manual and NFPA 86 requirements.
- A programmable controller not listed for combustion safety service shall be permitted to monitor safety interlocks, or to provide burner control functions, provided that its use complies with both of the following:

  a. The programmable controller shall not interfere with or prevent the operation of the safety interlocks.

  b. Only isolated programmable controller contacts (not directly connected to a power source) shall be permitted to be wired in series with the safety interlocks to permit burner control functions.

EN 54 requirements

The Trusted TMR System is certified to be used in EN 54 compliant systems.

The systems should be integrated in accordance with EN 54. In particular, the following shall be applied:

- Where an alphanumeric display is used to display indications relating to different functional conditions these may be displayed at the same time. However for each functional condition there shall be only one window, in which all of the fields relating to that functional condition are grouped.
- Unless EN 54 section 7.12 applies, the time taken by scanning, interrogation, or other processing of signals from fire detectors, in addition to that required to take the fire alarm decision, shall not delay the indication of the fire alarm condition, or of a new zone in alarm by more than 10 s.
- The control and indicating equipment shall enter the fire alarm condition within 10 s of the activation of any manual call point
- The audible indication shall be capable of being silenced by means of a separate manual control at access level 1 or 2. This control shall only be used for silencing the audible indication, and may be the same as that used for silencing in the fault warning condition.
- The control and indicating equipment shall be capable of being reset from the fire alarm condition. This shall only be possible by means of a separate manual control at EN 54 defined access level 2. This control

shall be used only for reset and may be the same as that used for reset from the fault warning condition.

- Unless 7.11 and/or 7.12 apply, the control and indicating equipment shall action all mandatory outputs within 3 s of the indication of a fire alarm condition
- Unless 7.11 apply, the control and indicating equipment shall action all mandatory outputs within 10 s of the activation of any manual call point.
- The control and indicating equipment shall enter the fault warning condition within 100 s of the occurrence of the fault or the reception of a fault signal, or within another time as specified in this standard or in other parts of EN 54.
- Total loss of the power supply (option with requirements)

Note: If there is a loss of the main power source (as specified in EN 54-4), the control and indicating equipment may have provision to recognize and indicate the failure of the standby power source to a point where it may no longer be possible to fulfill mandatory functions of this standard. In this case at least an audible indication shall be given for a period of at least one hour.

- A system fault shall be audibly indicated. This indication may be capable of being silenced.
- The cabinet of the control and indicating equipment shall be of robust construction, consistent with the method of installation recommended in the documentation. It shall meet at least classification IP 30 of IEC 60529:2004.
- All mandatory indications shall be visible at access level 1 without prior manual intervention (for example, the need to open a door).
- If the control and indicating equipment is designed to be used with a power supply (item L of figure 1 of EN 54-1) contained in a separate cabinet, then an interface shall be provided for at least two transmission paths to the power supply, such that a short circuit or an interruption in one does not affect the other.

[EN 54 section 7.12 Co-incidence detection (option with requirements)

Following the receipt of a signal from a fire detector, and until one or more confirmatory signals are received from the same or other points, the Control Indicating Equipment may have provision to inhibit either the indication of the fire alarm condition, or the operation of outputs to

- Fire alarm devices (item C of figure 1 of EN 54-1), and/or;
- Fire alarm routing equipment (item E of figure 1 of EN 54-1), and/or;
- Fire protection equipment (item G of figure 1 of EN 54-1).

In these cases at least the following shall apply:

1. it shall be possible to select the feature at access level 3 for individual zones;
2. The inhibition of one output signal shall not affect the activation of other outputs.]

[EN 54 section 7.11, Delays to outputs (option with requirements - see also 9.4.2.c) and annex E)

The control and indicating may have provision to delay the activation of outputs to fire alarm devices (item C of figure 1 of EN 54-1) and/or to fire alarm routing equipment (item E of figure 1 of EN 54-1). In these cases at least the following shall apply:

1. The operation of delays to outputs to item C shall be selectable at access level 3 to apply to
   - Fire detectors, and/or;
   - Manual call points, and/or;
   - Signals from specific zones;
2. The operation of delays to outputs to item E shall be selectable at access level 3, to apply to
   - Fire detectors, and/or;
   - Signals from specific zones.
3. the delay times shall be configurable at access level 3, in increments not exceeding 1 minute, up to a maximum of 10 minutes;
4. it shall be possible to override the delays and immediately action delayed outputs by means of a manual operation at access level 1 and/or by means of a signal from a manual call point;
5. the delay to one output signal shall not affect the activation of other outputs.]

Sensor configurations

Sensor configuration requirements vary depending on the user needs and the process under control. The following guidance is based on the requirements defined in IEC61511.

The behavior of the SIF and associated operator responses, whether it is based on a single or multiple sensors must include the behavior of the SIF under:

- normal operation,
- sensor failure (including power failure),
- sensor bypass and
- sensor discrepancy conditions.

If the SIF behavior under the conditions listed above requires an operator response to inform maintenance, there must be an associated alarm of suitable priority to inform the operator. The reaction time associated with the sensor as well as the operator response time must be included in the calculated MTTR for the SIF.

If the SIF relies on a single sensor and the defined action is NOT to fail safe If there is a fault in the sensor (including the input channel and associated wiring, terminals etc.), then a failure alarm must be used to inform the operator. The repair of the Sensor must be carried out within the MTTR. During the repair period, additional measures of at least equal risk reduction to the SIF must be put in place to maintain the safety of the process. If the

Operator response to the failure alarm requires a direct action as part of the process (i.e. closing a valve), then the alarm must be part of the SIS and independent of the BPCS.

If the SIF is High Demand or Continuous, the total time to detect the fault and to perform any operator action shall be less than the Process Safety Time.

For sensor configurations consisting of multiple sensors, then the Systematic Capability of the device must be considered for the maximum allowed claimed Safety Integrity Level.

When Smart sensors are being used, they should be write protected to help prevent unauthorized or inadvertent modification, unless a safety review carried out for the intended application permits the use of read/write. Smart sensor diagnostics can be used to augment the SIF diagnostics, but any Process values (that is, HART PV) cannot be used for SIF implementation.

Where multiple sensors are used as part of a SIF and each sensor is powered from a different power source, appropriate protection or separation of signals must be considered to help prevent exceeding the isolation specifications of the SIS logic solver equipment.

Final element configurations

As with sensor configurations, the final element configurations will be dependent upon the user needs as well as the process under control. The following guidance is based on the requirements defined in IEC61511.

The behavior of the SIF and associated operator responses, whether it is based on a single or multiple final elements must include the behavior of the SIF under:

- normal operation,
- sensor failure (including power failure),
- sensor bypass and
- sensor discrepancy conditions.

If the SIF behavior under the conditions listed above requires an operator response to inform maintenance, there must be an associated alarm of suitable priority to inform the operator. The reaction time associated with the final element as well as the operator response time must be included in the calculated MTTR for the SIF.

If the SIF relies on a single final element and the defined action is NOT to fail safe If there is a fault in the final element (including the output channel and associated wiring, terminals etc.), then a failure alarm must be used to inform the operator. The repair of the final element must be carried out within the MTTR. During the repair period, additional measures of at least equal risk reduction to the SIF must be put in place to maintain the safety of the process. If the Operator response to the failure alarm requires a direct action as part of the process (i.e. closing a valve), then the alarm must be part of the SIS and independent of the BPCS.

If the SIF is High Demand or Continuous, the total time to detect the fault and to perform any operator action shall be less than the Process Safety Time.

For final element configurations consisting of multiple final, then the Systematic Capability of the device must be considered for the maximum allowed claimed Safety Integrity Level.

When Smart final elements are being used, they should be write protected to help prevent unauthorized or inadvertent modification, unless a safety review carried out for the intended application permits the use of read/write. Smart final element diagnostics can be used to augment the SIF diagnostics, but any Process values (that is, HART PV) cannot be used for SIF implementation.

Where multiple final elements are used as part of a SIF and each final element is powered from a different power source, appropriate protection or separation of signals must be considered to help prevent exceeding the isolation specifications of the SIS logic solver equipment.

PFD calculations

Systems that are configured to meet the needs of IEC 61508 will require the PFD for the safety instrumented functions to be calculated.

For information regarding the calculation for the Trusted TMR System and PFD numbers allocated for the Trusted TMR System refer to the TÜV Rheinland approved PFD calculation document listed in the approved version list PFH and PFDavg for Trusted TMR System, publication ICSTT-TD002.

Processor configuration Timing

This section provides information about processor configuration.

The Trusted TMR Processor supports a limited set of configuration options; the system will verify many of the configuration options, for example module locations against actual module types. The configuration options include the maximum application program scan time and sleep period between application program scans. It is important to ensure that the overall application program scan period (scan and sleep periods) be set according to the PSTE.

ISAGRAF_Config section

Sleep Period (ISA_SLEEP_PERIOD)

This parameter defines the period that the application program should “sleep” between program scans. This parameter works in conjunction with the allowed scan time defined within the System Configuration Tool of either the SIS Workstation Software or Trusted Toolset Suite. The default value for this parameter is zero. This value may be increased to allow higher levels of processing resource to be allocated to other tasks, for example, external communications. Increasing this parameter will increase the overall scan time. If this parameter is increased, it is important to ensure that this overall scan time does not result in a response time exceeding that dictated by PSTE.

The sleep period or the allowed scan time, set in the SIS Workstation Software or Trusted Toolset Suite, should be adjusted to free up processing resource for other activities. If the sleep period is set to zero and the application execution to “as fast as possible” the system will switch between the necessary activities as required. Allowing a “free” amount of resource reduces the switching, improves overall efficiency for the specific application and results in greater scan period consistency under a range of conditions, rather than a faster scan period, but variability depending on load.

Maximum Scan Period (MAX_SCAN_TIME)

This parameter defines the maximum application scan time. The default setting is 1000 ms. If the defined time is exceeded the system will automatically and immediately initiate its overall fail-safe response. This value should be set to ensure that the overall scan time does not exceed the period dictated by PSTE.

Composite Scan Time Estimation for a Trusted TMR System

The composite scan time for a Trusted TMR System represents the time required to read the input data, solve the application logic, and write the output data. This sequence is repeated cyclically for as long as the Trusted TMR System is executing an application. For details of the scan time refer to

the composite scan time calculation section of the product descriptions for the T8111 and T8110/T8110B TMR Processor modules.

Diagnostic access

The Trusted TMR Processor supports comprehensive diagnostic facilities. Some of these facilities care capable of modifying the system's operation and are therefore password-protected to provide access protection in addition to that afforded by physical access to the system.

The password is defined in the Security section of the "system.ini" file. The password is encoded and is not readily de-coded from the "system.ini" text file.

A default password is implemented automatically, however it is recommended that a specific password be defined within the "system.ini" file. It is important that this password be made available only to personnel requiring access to the additional diagnostic capabilities (typically only Rockwell Automation personnel). If this password is lost, there is no capability of accessing these functions without reconfiguring the system.

Configuration file (system.ini file) configuration

The "system.ini" file defines a number of fundamental safety configuration options. It is important to ensure that the correct file is downloaded to the system and that this file represents the correct configuration.

1. The "system.ini" file may be created using either the configuration tool or a text editor.
2. Once complete, this file should be downloaded to the system.
3. The "system.ini" file shall then be uploaded from the system and checked that it contains the required configuration options. This ensures that no faults have been introduced by the configuration tool, the PC itself, or the down/upload process.
4. Following this check, the checksum of the file (uploaded with the file) should be recorded, and used to identify specific revisions of the "system.ini" file for a system.

Trusted high-density I/O module configuration Module characteristics

This section provides information about Trusted high-density I/O module configuration.

The Trusted High-Density I/O range has facilities to allow several of its operating parameters to be adjusted; examples of these include threshold settings, indicator operation, update rates, etc. The configuration settings available for each module type are defined in its corresponding Product

Description (PD). In many applications, the parameter's default values will provide the required operation.

These parameters may be adjusted within the "system.ini" file, which shall be reviewed in a similar manner as other system configuration and programming.

Once the configuration settings for a module have been determined, the checksum for the configuration data may optionally be calculated and entered into the "system.ini" file with the appropriate command. This provides further protection against configuration setting changes if desired. The checksum can be uploaded from the module, once the settings have been verified for completeness.

SYSTEM section configuration

The Trusted High-Density I/O SYSTEM section within the "system.ini" file allows the internal bus activity, system watchdog and power failure signal and bypass timeouts to be adjusted. These may be adjusted for test and development purposes.

Internal Bus Activity (IMBTO)

The default setting (500 ms) for the internal bus activity timeout is appropriate for most applications. This timeout may be adjusted to a shorter period; the adjusted period shall be shorter than the PST_E less the overall system response time. This setting SHALL NOT be set to zero for operational systems.

System Watchdog Timeout (WDOGTO)

As with the internal bus activity timeout, it is not normally necessary to adjust this parameter. This value SHALL NOT be adjusted for safety-related applications and SHALL NOT be set to zero for operational systems.

Power Fail Timeout (PWRFAILTO)

The power fail signal timeout shall only be set to zero if the output module is required to change to its configured fail-safe state, rather than off/energize-to-trip if there is a loss of communications with, or removal of a Trusted TMR Processor.

Bypass Timeout (BYPASSTO)

The Bypass Timeout period to temporarily bypass the other timeouts defined in the system section during an Active/Standby changeover. Only in exceptional cases will it be necessary to adjust this setting. This setting SHALL NOT be adjusted for safety-related systems and SHALL NOT be set to zero for operational systems.

FORCE Section

This section allows the reported channel state to be forced directly on the associated input or output module. This feature is for testing by Rockwell Automation or an approved systems integrator only, and SHALL NOT to be used in an operational system.

SHUTDOWN Section

This section allows the user to configure individual shutdown states for each output channel. The options include de-energize, energize and hold. Safety-related, de-energize to trip outputs shall either be left to their default shutdown action configuration (de-energize to trip) or specifically configured to energize to trip. Safety-related, energize to trip outputs should be configured for the energize option. Hold is a special case that permits outputs to be held in the last state when an application is stopped or If there is a loss of IMB communications. Additional care must be taken when selecting the hold option.

FLAGS Section

This section allows the user to configure the input or output type and the form of monitoring supported for each channel. For line monitored, safety-related outputs the logical = TRUE setting SHALL NOT be used as this disables the line-monitoring facility.

LED Section

This section allows the user to configure the indicators on the front of each High-Density I/O module. LED color and flash attributes can be specified for each possible channel state (such as line fault conditions or voltage threshold ranges) Safety-related I/O SHALL NOT use steady green to indicate abnormal channel conditions.

De-energized Short Circuit Detection Section

This section allows the user to enable de-energized short circuit detection (default is disabled). Safety-related I/O that is energize to trip shall use short circuit monitoring.

Module replacement configuration

The system supports three forms of High-Density I/O module replacement:

- Hot-swap pair (companion slot)
- SmartSlot
- Live insertion and removal

In the hot-swap pair, two adjacent module positions are coupled to provide an active and standby module pair. If it is intended that the system be able to start up (including application stop and restart), on the primary module position, there is no requirement to define the secondary module position.

If it is intended to allow the system to start with only the secondary module position occupied, it is important that the module positions be included within the system.ini file. For Companion Slot modules, enter a module in the primary slot. Tick ‘Simulate’ and enter the partner chassis and slot location. Do NOT enter a module in the partner slot.

For SmartSlot pair operation, it is not possible to start up using the “spare” module position. The spare module position does not need to be in the same chassis as the primary module position.

If it is intended to perform live insertion and removal without transfer to a standby module, no specific configuration is required. If it is intended to start up a system without the primary module installed in either a SmartSlot or single module live insertion or removal configuration, the “simulate” configuration option should be set. The simulate option will allow the system to start with these modules omitted, the corresponding states and values being set to their fail-safe conditions.

1. A consistent module replacement philosophy should be used within any single system. Where mixed philosophies are used, there shall be clear indication of the repair approach applicable to each module or group of modules.
2. In hot-swap and SmartSlot configurations, the accuracy with both modules installed shall be within the plant required safety accuracy specification. If tighter tolerance is required, ensure that each sensor within a redundant configuration is allocated to independent modules and procedural measures are implemented to ensure that only a single module within this set of modules is paired at any instant.
3. If the SmartSlot module replacement is used, the system shall include provision for testing the SmartSlot linking cable. This cable shall be tested before use; the testing of this cable shall be included in the Operating and Maintenance Manual.
4. In hot-swap configurations, a secondary module that does not pair with the primary module in a reasonable amount of time (less than the SFOC) must be removed.
5. In SmartSlot configurations, a secondary module that does not pair with the primary module in a reasonable amount of time (less than the SFOC) when the SmartSlot linking cable is installed must be removed.

Input and output forcing

Locking and forcing of individual inputs and outputs from the SIS Workstation Software or Trusted Toolset Suite are supported for engineering, installation and commissioning purposes. In-service, maintenance overrides for safety-related inputs and outputs should be implemented using the application program. The SIS Workstation Software or Trusted Toolset Suite initiated locking and forcing requires:

- The TMR Processor keyswitch to be in the “Maintain“ position to make changes to the lock or force status of any point
- Access to the SIS Workstation Software or Trusted Toolset Suite lock and write commands, which are password-protected at project-level for SIS Workstation Software and multi-level for Trusted Toolset Suite.
- A list of the currently locked points is read back from the TMR system and made available within the SIS Workstation Software or Trusted Toolset Suite. For information, see Knowledgebase Document ID: IN30807- ICS Triplex 8000 Series: TN20081 some variables in ‘Unlock All Variables’ window are ‘Unknown’.

The Trusted TMR Processor inhibit LED will indicate when one or more I/O points are locked. The application program can determine how many points are currently locked by using the information available from the Trusted TMR Processor complex equipment; it is highly recommended that this is used to control an additional status display and/or for logging purposes. Refer to publications ICSTT-RM038 (PD-T8111) and ICSTT-RM251 (PD-T8110B), Complex I/O Equipment Definition section, for more information.

All input and output locks (and forces) can be removed using either a single function from the SIS Workstation Software or Trusted Toolset Suite, or from an edge triggered signal to the Trusted TMR Processor board within the application program. If locking is used, a safety-related input connected to an operator accessible switch shall be implemented to initiate the removal of the lock and force conditions.

It is important that the effects of forcing input and output points on the process and their safety impact are understood by any person using these facilities.

The system will allow the forced conditions to be maintained during normal operation. When returning to normal operation, it is recommended that all locked and forced points be returned to normal operation. It is the plant operators' responsibility to ensure that if forced conditions are present that they do not jeopardize the functional safety.

Maintenance overrides

Maintenance Overrides set inputs or outputs to a defined state that can be different from the real state during safety operation. It is used during maintenance, usually to override input or output conditions in order to perform a periodic test, calibration, or repair of a module, sensor, or actuator.

To implement a maintenance override scheme within the Trusted System correctly, the override or 'bypass' logic shall be programmed within the Application Program, with a separate set of safety-related input points or variables enabling the bypass logic.

It is important the consequences of overrides of input and output points on the process and their impact on a safety system are understood by any person using these facilities. It is the plant operators' responsibility to make sure that if there are forced conditions they do not jeopardize the functional safety of the system.

In order that maintenance overrides are carried out in a safe manner they shall be implemented and operated according to the instructions in this manual. Additionally, it is recommended they are implemented and operated according to the requirements defined in IEC 61511.

There are two basic methods now used to check safety-related peripherals connected to a Trusted TMR System:

1. Special switches connected to conventional system inputs. These inputs are used to deactivate sensors and actuators during maintenance. The maintenance condition is handled as part of the system's application program.
2. Sensors and actuators are electrically switched off during maintenance and are checked manually.

In some installations, the maintenance console may be integrated with the operator display, or maintenance may be covered by other strategies. In such installations, follow the guidance given in Communications interaction on page 67. An example maintenance override requirements checklist is given in Table 4-6.

Peer to Peer communications configuration

Trusted TMR System supports the original Peer to Peer and enhanced Peer to Peer communications, which allows safety-relevant data to pass between numbers of Trusted TMR Systems. When using this mechanism, as with any other, it is important to ensure that the overall system will respond within the required PST_E. This requirement applies to normal operation and in the presence of faults.

For safety-related applications, it is recommended that the Peer to Peer Communications use redundant networks. It should be noted that high network bandwidth usage by non-safety system equipment may cause data timeouts and hence spurious trips. Therefore separate networks for the safety data should be considered.

The Peer to Peer Input boards include the configuration of a refresh timeout. This timeout defines the maximum interval between the receipts of valid, updated data from an associated (source) system.

This timeout period shall be set that if the fault tolerant capabilities of the Peer to Peer Network, (that is, lack of fresh data is detected) the system can still respond within the required PST_E. The network propagation time must be included in the timeout period calculations, and should be reverified after each change to the network configuration.

The freshness of the received data is available to the application programmer as part of the Peer to Peer Input board input information. This status is set to 'TRUE' or '1' while updated data is received within the refresh timeout. If a timeout occurs, this status bit is set to '0'. The data received from the corresponding source system will be held in its previous state or value if there is a timeout or go to the defined fail-safe state depending on the configuration.

If "**hold last state**" is selected, it is important that the application programmer includes handling of this condition, including latching of the failure as necessary. For example, the loss of the Peer to Peer Communications link may require a specific safety reaction, or may require that the corresponding data be set to a specific state or value.

The Peer to Peer Output board includes a refresh period. This value defines the interval between transmissions of the corresponding data if no state or value changes are received from the local application program. This value shall be set to a period shorter than that of the input board, unless changes occur constantly, otherwise the corresponding input boards will time out.

The Peer to Peer master configuration includes transmit timeout values for that network. The Peer to Peer master and slave configurations include response timeout values. These values are used to determine the link status. This link status information may be used in addition to the freshness status to allow the source system, or Peer to Peer communications master, to report link status or to act if there is a link failure.

Release 3.5 and later, Peer to Peer transfers 32-bit values between nodes. The 32-bit values can be 32-bit signed or 32-bit floating point depending on the variable connected to the output board. The variable type used for a particular variable must match at both the input and output board. A single input and output board pair can use different data types on different channels provided they match on both the input and output boards.

Triguard Peer to Peer protocol

The Triguard Peer To Peer protocol, "TPTP", is a point-to-point communication protocol, consisting of query and response packets. It is used specifically for migration from Triguard to Trusted controllers.

Configuration

The configuration of the TPTP protocol serial ports, access privileges, response timeouts and queries to be transmitted is achieved using dedicated application I/O boards. Detailed guidance for the configuration of the TPTP is provided in Application Note AN-T80024.

TPTP protocol shall be configured to use dual-redundant serial links between peers. The serial links shall be provided using two separate Communication Interface modules.

Peer link usage shall be configured such that peer data latency estimated according to AN-T80024 is less than the maximum safety reaction time allocated to the application. The peer data latency shall account for transitions from dual to single link operation due to link failure.

Application requirements and constraints (Trusted and Triguard)

TPTP protocol shares the same domain of network addressable variables and associated attributes as Modbus.

Modbus Master and Slave shall not use network variable addresses that overlap those allocated for use with the TPTP protocol.

Triguard applications shall be built using the SIL 3 certified TGPROT.LIB version 3.20.

TPTP CRC checking shall not be disabled within the TGPROT_C I/O board configuration.

The TGPROT_C channel board timeout parameter shall be configured to lie between the peer data latency estimated according to AN-T80024 and the maximum safety reaction time allocated to the application.

The application shall implement redundant safety data transfer with bit-wise comparison to achieve the residual error rate PFH requirements for SIL 3 data communications according to IEC 61784-3:2010. This shall be achieved by compliance with the design rules listed under Application design rules on page 60 applicable to both Trusted and Triguard applications.

Application design rules

This topic provides information about application design rules.

1. The application peer safety data output shall include a safety data sequence number register that is incremented with each data to be sent by the application.
2. Redundant safety data shall be sent as an antivalent (bit-wise inverted) copy of the safety data.
3. The safety data and its antivalent copy may be transferred using either a single query/response packet or two separate query/response messages.
4. Non-safety data may share the same Query/Response messages as the safety data without constraint within the limits imposed by the Triguard peer protocol.
5. If a single Query/Response message is used to carry the safety-related data and its antivalent copy, then the extent of the safety-related data is constrained to lie in the range dependent upon the rate at which safety-related data is to be transferred according to Table 3-6.

Table 3-6 - Single Query/Response Safety Data Bits

Message Rate	Safety Data Bits
1 per second	780 - 4000
2 per second	822 - 4000
5 per second	882 - 4000

Where an application demands less than the minimum length according to Table 3-6 then additional register data must be added to both the safety data and its antivalent copy to comply with the minimum length constraint. The additional register data and its antivalent copy must be checked in the same way as the safety data. The additional register data may be constant.

6. If two separate Query/Response messages are used to carry the safety data and its antivalent copy, it will be necessary to ensure that the safety data does not change between the sending or receiving of the two messages. This also applies to the safety data sequence number within the application peer safety data output.
7. The transfer of safety data to Triguard nodes shall only use Triguard Peer Query Read messages. Triguard nodes shall be configured to help prevent access by Triguard Peer Query Write messages received from other peer nodes. No such restriction applies to the type of messages used to transfer safety data to Trusted nodes.
8. The peer application receiving safety data shall implement an application watchdog configured with a timeout period corresponding to the maximum safety reaction time allocated to the application.
9. The peer application receiving the safety data shall validate the safety data using a bit-wise comparison between the safety data and its

antivalent copy at the start of each application cycle. The following actions shall only be taken when the safety data and the inverse of its antivalent copy are found to match and the safety data sequence number embedded in the safety data is found to differ from that last recorded input safety data sequence number:

a. The watchdog shall be refreshed.

b. The peer safety data input shall be copied to a further set of registers representing the application peer safety data input used by the application.

c. The input safety data sequence number shall be updated to the value just received.

10. A failure of the application watchdog to be refreshed within its timeout period shall lead to the execution of the defined safe state for the application.
11. Failure of the primary TPTP link status or secondary TPTP link status shall be used to alert an operator to any degraded peer link operating status.

An application note (AN-T80024) provides guidance on implementation of the above rules and a corresponding checklist that shall be used to verify that an application has followed them.

Once migration is complete the native Trusted Peer to Peer protocol shall be used to replace Peer to Peer data exchanges (see Peer to Peer communications configuration on page 57. The application design rules above will no longer apply as this protocol is fully certified for SIL 3 communications.

Application program development

The SIS Workstation Software or Trusted Toolset Suite may be connected either directly to the serial communications ports local to the Trusted TMR Processor or via an Ethernet network.

Where Ethernet is used, the network shall not be used to connect equipment not associated with the Trusted System. PCs connected to this network shall not provide a route to access the Trusted System from other networks, that is, if they support multiple Ethernets, routing to the dedicated Trusted TMR System network shall be specifically disabled.

SIS Workstation software configuration

For project security, set access control by using a password for projects. Password definitions are limited to eight characters and can consist of letters, digits, and symbols. Enter the password to open a password-protected project.

For more information, refer to AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002.

Trusted Toolset Suite configuration

The Trusted Toolset Suite supports 16 levels of password access, level 0 being the highest access level. Each Toolset Suite function (for example, viewing, editing, compiling, downloading) may be identified for use only by users with an access level above a certain level.

User access passwords shall be implemented.

The recommended access levels are:

- 0 – Engineering supervisor
- 2 – Engineer/Application Programmer
- 4 – Maintenance Engineer
- 8 – General User

Examples of access levels are shown in Table 3-7.

Table 3-7 - Example Showing Trusted Password Access Levels

Function	Min. access level	Function	Min. access level
Global Protection	8	Debug application	8
Overwrite with archive	2	Simulate application	8
Backup on archive	8	Download/stop/start application	4
Project Description	4	Update application	4
History of modifications	8	Communications parameters	8
I/O Connection	2	Set cycle time	2
Global Variables	2	Set execution mode	2
Global & Common Defined Words	2	Change variable state	4
Create New	2	Lock/Unlock variable	4
Move program in hierarchy	2	Control SFC	4
Verify	8	Control Timer	4
Make application code	4	Set IL Breakpoint	4
Touch application	4	Set SFC Breakpoint	4
Conversion tables	2	Create graphics	8
Application runtime parameters	2	List of variables	8
Compiler options	2	List of time diagrams	8
Resource definition	2	Print project document	8
		Customize project document	4

Language selection

The SIS Workstation Software or Trusted Toolset Suite offers many programming tools to develop algorithms to meet the needs of virtually any real-time control application. The configuration and programming languages approved for use in SIL 3 safety-related application is shown in Table 3-8.

Table 3-8 - Safety-related and Non-Safety Programming Language

Safety-related	Non-Safety
Function Block (FB)	Sequential Function Chart (SFC) (Trusted Toolset Suite only)
Instruction List (IL) (Trusted Toolset Suite only)	

Table 3-8 - Safety-related and Non-Safety Programming Language

Safety-related	Non-Safety
Structured Text (ST)	
Ladder Diagrams (LD)	

- Safety-related Languages. For those languages that have been classified as 'safety-related', commonly used functions have been exhaustively tested and may be used freely. Those included within the certification testing are shown in Previously assessed functions on page 83.

  Further functions may be used subject to completion of testing commensurate with the level used for the commonly used functions.

- Non-Safety (Trusted Toolset Suite only). The languages that have been classified for non-safety-related applications only SHALL NOT be used within a safety-related system.

IL and ST include program flow control functions; these functions shall be used with caution to ensure that infinite loop or omitted logic conditions do not result. Where these constructs are used, it is recommended that full branch and data coverage tests be performed on these sections of program. It is recommended that only Boolean conditions be used for these constructs to ensure that a feasible set of tests can be applied.

Application programmer-generated function blocks may be created either on a project-specific or library basis. Where these functions are to be used for safety-related applications, they shall be subject to exhaustive testing, commensurate with that used for the commonly used functions (see Testing of new and previously untested functions on page 64). Once the function block has been subject to this level of testing it may be used as for commonly used functions.

There is provision for the Trusted System to support multiple programs within a project. A complete project may be classified as safety or non-safety-related. A safety-related project may use the safety programming languages; non-safety programming languages cannot be used. A project classified as non-safety may use any of the programming languages and the full instruction set but shall not be used to implement safety-related functions. A checklist for the selection of programming languages is given in Table 4-5.

Process control functions

Control functions that are listed in Trusted Process Control Algorithm Software Package, publication ICSTT-RM246 (PD-T8019), require the use of floating point values. This ultimately limits the integrity that can be attributed to these functions because of the introduction of an element of 'loss of

precision' and the general inability to exhaustively verify floating point capabilities.

The functions are integrated into the SIS Workstation or Trusted Toolset Suite execution environment. The overall system achieves higher levels of integrity by the use of additional online monitoring and internal state control.

The combination of the above factors indicates that the target integrity for the basic process control functions must be SIL 1. Do NOT use these functions within elements of application programs intended for SIL 3 use.

Testing of new and previously untested functions

The SIS Workstation Software or Trusted Toolset Suite provides a number of function blocks that can be combined to form a project application.

The use of these function blocks in safety certified systems is only permitted once they have been tested for correct operation. A list of the functions tested before the initial certification of a Trusted TMR System is provided in Previously assessed functions on page 83.

The new or previously untested function may be:

- a generic function block, which forms part of the SIS Workstation Software or Trusted Toolset Suite, but has not previously been subject to the level of testing defined herein, or
- project-specific function block, which is written to meet the needs of a particular feature within an application program, and may comprise a number of generic function blocks or other program functions

If a previously untested function block is needed, the function block must be tested in accordance with Application design rules on page 60, items 1 to 7.

Test method

Each function to be tested shall be placed within an application test harness using the SIS Workstation Software or Trusted Toolset Suite that exercises its capabilities. The implementation of this harness shall be such that the function block is exercised automatically, so that the test is repeatable.

As a minimum, each test harness shall comprise of all of the following:

- Function Block under test
- Alternative implementation of the function block
- Function generator
- Main and alternative comparison Pass/Fail Flag
- Test results register

Where practical, and with the exception of time, results of the test shall be automatically recorded and should not require a human to count or record dynamic data.

Alternative implementation of the function block

The test harness shall include an alternative implementation of the function being tested. This implementation shall be performed using features of the tool set that are as diverse as possible from the actual function block.

For example, an "Or Gate" can be simulated by counting the number of inputs set to a logical "1" and determining that the count is greater than or equal to 1.

Function generator

The operation of the test harness shall be automatic; a function generator shall be provided to generate the stimuli for the function under test. This function generator shall be as simple as possible and shall not contain the function under test.

Main and alternative comparison Pass/Fail flag

The results of the alternative implementation shall be compared with the results of the function under test; discrepancies shall cause a "main and alternative comparison fail flag" to be set.

Test results register

Each harness shall include registers that record the functionality of the function block. This registration should be as comprehensive as possible and should use as many predictable features as possible.

For example, a 2 input logical "Or Gate" stimulated by the two lower bits of a 16-bit counter will record 32768 logical high states if the counter is allowed to make one complete up count from 0 to 65536. The results register would count these states and present a number to the human operator. In this case, the results register should also record that no two consecutive states of the counter caused a logical "1" at the output of the Gate.

Test coverage

Where possible, all combinations of input shall be simulated.

For certain functions, such as adders and comparators, this is not practical. In these cases, the test harness shall use a significant number of test cases to prove the functions operation. The use equivalence class, boundary cases, and random numbers shall be used as the preferred method of generating these cases.

Functions containing complex algorithms or with extensive retained state or value dependence require an extensive number of test cases, and are therefore considered impractical to achieve a sufficient level of test coverage and shall be used in non-safety programs only.

Recording and filing of results

The tests shall use formally approved test procedures and the test results shall be formally recorded. The test harness, details of the test environment and test result shall be retained.

Any deviation between the results and expected results shall be examined; where this results from deficiencies in the test harness these shall be corrected and the test repeated. Should any function fail, it shall be:

- Not used within safety-related applications, or
- The conditions that result in erroneous operation shall be explicitly recorded and published. If the function is used, other functions shall

be added to the application to specifically detect the conditions leading to erroneous operation and take a fail-safe action.

To maintain system certification, any test harness used to prove that a function block should be archived as part of the test record so that the tests can be repeated at later date and if required, reviewed by TÜV.

Application development

The application program development shall follow a structured approach and follow the principles defined in Application programming on page 24. The stages defined in the following subsections shall additionally be applied for safety-related applications.

Partitioning the application

It is impractical and unnecessary to apply the same degree of rigorous development and testing to all functions within the Application where some of those functions are not safety-related.

The identification of safety functions is, in part, dependent on the specific safety philosophy. Examples of non-safety may include status indication, data reporting, and sequence of events. It is important to establish that these elements are not safety-related. For example, some safety cases rely on human intervention and therefore the correct operation of status indication.

The safety-related elements shall be implemented within separate programs to those of non-safety-related elements. Where information passes between these elements, it shall be arranged that the direction of flow is from safety relevant to non-safety relevant only.

Defensive measures

In defining the Application, the programmer must consider the potential sources of error and apply reasonable defensive programming techniques. Where values are received from other programs or external communications interfaces, the validity of the values should be checked where possible. Similarly, values received from input interfaces should be checked where possible. In many cases, it will also be possible to monitor permutations of data, inputs and plant operating modes to establish the plausibility of the information and program measures to ensure safe responses if there are implausible conditions.

Safety-related functions shall be latched when in their tripped state to help prevent intermittent field faults from removing the trip condition. The application software shall be written to ensure that safety-related functions are in their safe state during system startup.

Testable blocks

Each safety-related software block shall be 100% testable. A 100% testable block is the application logic that belongs to one safety function. Such

functions could be:

- Burner flame supervision including temperature, air/gas pressure monitoring, etc.
- Burner gas-to-air ratio control/supervision
- Parts or whole of the startup sequence of a batch reactor

The fewer the number of inputs, outputs and signal paths, the fewer the number of permutations that require testing. However, a single safety function should not be split into separate blocks; such a division is likely to lead to the introduction of errors during maintenance activities.

The interaction between the individual software blocks shall be minimized. Where interaction is necessary, it should be kept as simple as possible, for example a single shutdown initiation signal.

Each safety function shall be responsible for the control of the corresponding outputs. Sharing of outputs between functions shall not be permitted.

Individual safety-related functions

Define up to 254 programs in a single project by using the SIS Workstation Software or Trusted Toolset Suite. This facility should be exploited to enable the allocation of individual safety-related functions to separate programs. Where such programs contain independent logic paths, these should be investigated to determine if they are separate safety functions. Where they are separate, it is recommended that these be further allocated to their own program, subject to conforming to the recommendation to minimizing the coupling between programs.

Cases should be looked for that allows the creation of individual logic paths by repeating small sections of logic rather than fanning out the resultant signals.

Minimize logic depth

Where possible, the logic depth should be minimized. This helps reduce visual complexity, simplifies testing, minimizes

Where there is nested logic, it shall be possible to establish the correct operation of all intermediate logic connections.

The use of memory components, i.e. latches, within the safety function shall be minimized. Similarly, the permutation of conditions that lead to their activation shall be minimized.

Communications interaction

The Trusted TMR System provides a range of communications options to allow interaction with external systems. Where this communication is used for reporting (or out-going) communications, there are no specific safety requirements.

Data received from external equipment that either controls safety-related functions or affects their operation must be handled with caution. The Application Program shall handle the received data.

The received data should be such that it is limited to interaction which:

- Initiates safety operations, i.e. initiates shutdown sequences

- Resets signals, with the reset action only possible once the initiating conditions have been removed
- Initiate timed startup override signals which are removed automatically either on expiration of the start period or once the associated signal has stabilized in the normal operating condition
- Adjust control parameters within defined safe operational limits, i.e. lowering of trip thresholds.

Where the interaction does not fall within these categories, the effects of incorrect values and sequences of values shall be considered and measures taken to ensure that the system will respond safely if there is erroneous data. Alternatively, measures may be implemented within the application to ensure the integrity and validity of the data.

Program testing

Even with a small number of inputs, it is possible to reach a point where the number of tests becomes unreasonable. Eliminating impossible or unlikely scenarios should be used to reduce the number of logic path tests that need to be performed. The selection of what constitutes a scenario that does not require testing can be performed only after a suitable hazard analysis.

The scenarios should include possible plant conditions, sequences of plant conditions, system conditions (including partial power conditions, module removal and fault conditions).

Where it is not possible to define a representative suite of test cases, all permutations of input conditions, that is, all possible states on all possible inputs, shall be exercised. Where the logic includes memory or timing elements, additional tests shall be defined to exercise all the possible sequences of input permutations leading to their operation.

All safety-related functions shall be tested and the results of the tests recorded. The tests shall include the system scan time, fault detection time, fault reaction time and throughput delay for shutdown logic. The system scan time, including Peer to Peer Communications where appropriate, shall be less than ½ PST_E.

Functional testing coverage of all safety-related programs is considered to be 100% if:

- All inputs are exercised through their entire allowable range
- All outputs are exercised through their entire program determined range
- All logic paths are exercised
- All timers have been tested regarding their timing characteristics without changing timing parameters
- All combinatorial permutations of digital signals, with the exception of 100% tested function blocks, are tested, including fault states.
- All combinatorial permutations of analog signals, with the exception of 100% tested function blocks, are tested within the safety accuracy granularity.
- All timing properties of each safety loop have been verified

Cross reference checking

While the aim shall be to minimize the coupling and dependencies between individual programs, there will inevitably be occasions where, for example, a variable is used within two or more programs. It is important to ensure that any application program changes that affect these interactions do not jeopardize the functional safety.

The SIS Workstation Software and Trusted Toolset Suite include two cross-reference check tools. One of these verifies the source cross-references, the other the compiled code cross-references.

Once the application program baseline has been established, these tools shall be used following application modification. The identified interdependent programs shall then be retested. Whenever a program modifies a shared variable all programs that use that same variable shall be retested.

Code comparison

After each phase of modification to the application as a whole, the Trusted TMR System code comparison and runtime code version checker utilities shall be used to identify those programs that have changed. Any program identified as having undergone change, other than compiled variable addresses, shall be retested.

After an application has been tested, and before any changes are made, a reference copy of the compiled application should be made. After the application has been modified, the new application is compared to the original application by using the "TIC Difference Checker" utility. The utility will identify those programs that have changed since the original application and are subject to retest.

The "TIC Version Checker" utility is used to verify that the reference copy of the original application is the same as the application currently loaded into the Trusted TMR System.

Online modification

As with any safety-related system, it is highly recommended that online changes not be performed. Where changes have to be performed online, it is recommended that they be performed when alternative safety measures are provided or when the affected hazards cannot arise.

Certain modifications can be performed without directly affecting the system's safety function, for example the installation of additional modules. Although these modifications will not affect the system's operation until the system configuration and application program have been modified, caution shall be exercised to ensure that the modifications do not affect other safety functions.

The product allows for the online addition of modules, although these require application program modification, which dictates the stop and reload of the application. The addition of modules may be performed online to minimize the period of plant downtime. Modifications to field and power wiring to accommodate new modules shall be considered carefully.

Changes that affect the system's ability to respond safely, or may cause other plant disruption shall not be performed online unless alternate protection measures can be implemented for the duration of such modifications.

Application program

The Trusted TMR System supports two types of online updates: Normal Updates and Intelligent Updates. Specifically, an online update consists of changing the currently running application, loading those changes into the

system, then having the system "switch" to the updated application without interruption to the process that the application is controlling. Normal updates are available in all released versions of the Trusted TMR System.

With Normal Updates, the TMR System allows limited changes to be made to the application program online. These pre-defined limits restrict changes to logical operation. Modifications that exceed these predefined limits automatically preclude online modification and dictate that the application program be stopped before updating.

In addition to Normal Updates, Intelligent Updates are supported in Trusted release 3.4 and above. Both online update features enable the user to modify the application while the process is running. While both types of online updates perform essentially the same function, Intelligent Updates allow the application to be modified in a number of ways that Normal Updates would not allow.

If Intelligent Updates are to be used they must be explicitly enabled for each project, and the Intelligent Update Manager must have knowledge of the specific version of the application that is currently running in the controller. Each time an application is compiled, the Intelligent Update Manager uses its knowledge of the application running in the controller to create an Intelligent Update recipe. This recipe contains a signature of the application running in the target, and information on how to perform specific mapping for variables and function block instance data. It is the recipe that allows the value of variables and function block instance data to be preserved across an online update.

IMPORTANT Before using Intelligent Update, read and understand the Intelligent Online Updates section of the AADvance-Trusted SIS Workstation Software User Guide, publication ICSTT-UM002, or the Trusted Toolset Suite product description, publication ICSTT-RM249 (PD-T8082).

The existing application program must be archived before any changes to the application are carried out.

Where it is necessary to perform online modifications, caution shall be taken to ensure that unsafe responses are not generated. Particular consideration shall be given to the effects during the transition between the existing and the new programs and configurations. This is particularly important where a number of interacting systems provide the required safety functions.

Before any revised application program is downloaded to an online system:

- All changes shall be tested using the application simulator
- The cross-reference checkers (see Cross reference checking on page 69) shall be used and programs using data from modified programs shall be retested.
- The source code compare utility (see Code comparison on page 69) shall be used; any programs identified as having other than compiled variable addresses shall be retested.

Once testing has been successfully completed, the application program may be downloaded to the Trusted TMR Processor. The download and application update may only be performed with the Trusted TMR Processor keyswitch in the **Maintain** position.

System configuration

All modifications to the system configuration ("system.ini" file) shall be subject to the same considerations as specified earlier in this manual. The configuration file may be up- or downloaded to the system when the Trusted TMR Processor keyswitch is in the **Maintain** position. High-Density I/O configuration changes then require that the application program be stopped and restarted to bring the changes online.

Modification to the system configuration normally entails the addition or deletion of input and output points. If these points previously did not exist within the application program, it will be necessary to take the system offline to perform the changes.

Basic system parameters, including the number of chassis, chassis mapping, communications settings etc., require that the Trusted TMR Processor be removed and reinstalled, or the power cycled to the controller chassis to implement the configuration changes.

The existing system configuration ("system.ini") must be archived before any changes to the system configuration are carried out.

Where changes to the system configuration are anticipated it is necessary to include the “spare” module positions and chassis within the existing "system.ini" file.

Environmental requirements

The system installation environment presents a potential source of common cause failure. It is necessary to ensure that the equipment is suitable for the intended environment. Refer to the Trusted Environmental Specification, ICSTT-TD003. Alternatively, methods of maintaining the equipment's environmental conditions within its capabilities should be provided. This is applicable to all systems; the remainder of this section however gives the specific environmental recommendations for a Trusted TMR System.

Climatic conditions

The recommended and maximum climatic conditions for the equipment are shown in Table 3-9. These conditions apply for representative and typical system configurations. Where high equipment densities are accommodated within a system or large quantities of high-power equipment are closely packed, it is necessary to consider the localized heat generation and its impact on the overall system operating environmental conditions.

Table 3-9 defines the climatic conditions for the modules within a system as a whole. It is possible to achieve a system capable of operation in a wider range of climatic conditions using detailed analysis of the characteristics of the system and resultant conditions for the equipment mounted within the system.

The following should be noted:

1. The operating temperature is the temperature measured at a point not more than 50 mm from the plane of the airflow entry point of the equipment as per IEC 61131-2. The overall system shall normally be mounted in a cabinet which when the doors are closed will affect the temperature in proximity to the equipment elevating it relative to the ambient outside the cabinet.
2. It is highly recommended that the operating temperature of the system be monitored, and an alarm created (with defined operator response) if the system exceeds the maximum operating temperature limit.

   Note: The alarm level needs to take account of the time taken to respond to ensure that the intended temperature limit is not exceeded.

3. It is highly recommended that during system design the target site temperature is checked and during commissioning the temperature elevations within a particular system are monitored, documented, and considered (if used) in the operating temperature maximum alarm limit.
4. Trusted is designed to operate in a Pollution Degree 2 or better environment (IEC 61010-1); the enclosure type and design shall take this into account.

It may be possible to artificially (for example, using anti condensation heaters or similar) maintain an ambient equipment temperature above 0 °C when the temperature outside the system cabinet falls below 0 °C.

It should be noted that the operating temperature for the equipment within any electronic system has a significant impact on the potential operating life of that equipment. High operating temperature and rates of temperature change significantly reduce the operational life of any electronic device; therefore, measures should be taken to ensuring that the operating environment remains within the recommended range. Similarly, it is highly recommended that the periods that the equipment is exposed to conditions outside the recommended range be minimized.

Table 3-9 - Climatic Condition Requirements

Parameter	Comment	Recommended		Limit	
		Min	Max	Min	Max
Operating Temperature (dry)	With forced airflow	+10 °C	+30 °C	0 °C	+60 °C
		+50 °F	+86 °F	+32 °F	+140 °F
Storage Temperature (dry)		+10 °C	+30 °C	-25 °C	+70 °C
		+50 °F	+86 °F	-13 °F	+158 °F
Operating Humidity	Noncondensing			10% RH	95% RH
Storage Humidity	Noncondensing			10% RH	95% RH
Temperature change			±0.5 °C/min		See Note
			±1 ºF/min		

Note: Although there is no defined maximum, it is important to avoid changes of humidity and temperature that could produce condensation. The effects of condensation on any type of electrical equipment can result in equipment failures or improper operation.

Electromagnetic Compatibility (EMC)

The Trusted TMR System is designed and tested to be resistant to usual levels of conducted and radiated electromagnetic interference and electrostatic discharge. The levels of electrical environmental noise depend on the design of the equipment installation, wiring, other installed equipment, and how near it is to the TMR equipment.

You must make sure that the Trusted TMR System complies with the client's requirements and with applicable national or regional standards:

- For installations in the European Economic Area, the CE mark requirements for EMC are a legal minimum for electromagnetic emissions.
- For installations in the United Kingdom, the UKCA mark requirements for EMC are a legal minimum for electromagnetic emissions.
- For installations in Republic of Korea, the KCC mark statement for EMC:

A 급 기기 (업무용 방송통신기기): 이 기기는 업무용(A 급)으로 전자파적합등록을 한

기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서

사용하는 것을 목적으로 합니다.

Translation: Class A device (Broadcasting Communication Device for Office Use): This device obtained EMC registration for office use (Class A), and may be used in places other than home. Sellers and/or users need to take note of this.

- For installations in other locations, you must determine if the local electromagnetic interference (EMI) levels are higher than those shown in the Trusted Environmental Specification, ICSTT-TD003.

Physical Installation Design

This topic provides information about physical installation design.

Enclosure

The Trusted Controller Chassis must be installed in an EMC-rated enclosure utilizing EMC gaskets on all doors and internal swing frames. The Trusted TMR System makes high levels of radiated emissions and it will get EMC emissions compliance only when care is taken to make sure that none of these signals leak out of the enclosure.

If the side panels of the enclosure are removed, or the doors are opened (for example, during maintenance work), the immunity of the controller chassis to EMC interference is unchanged, but the emissions radiated from the installation to its environment will be higher.

IMPORTANT The side panels of the enclosure must be installed and the doors must be kept closed to let the system comply with the usual EMC environmental constraints for emissions.

If the expected EMI levels are higher than those shown in the Trusted Environmental Specification, ICSTT-TD003, you must apply applicable protection measures.

Preparing and Earthing the Controller Chassis

Install module blanking panels (shields) on all empty module positions in the Trusted Controller chassis. This will reduce the strength of unwanted electromagnetic emissions during system commissioning and maintenance work when the enclosure doors are open.

The chassis must be connected to the EMC enclosure using a cable no smaller than 4 mm2 area and no longer than 200 mm.

Enclosure Internal Wiring

Cable pigtails that provide a functional earth connection between Trusted I/O modules and their field termination assemblies must be connected directly to the Trusted Controller chassis at the module end, and to the EMC enclosure at the field termination assembly end.

Cable Entries

Each cable that passes through the boundary of the enclosure (the boundary means the sides, floor and top) must be shielded (screened) or pass through an EMC filter unit bonded directly to the EMC enclosure. This includes AC mains power cables, field wiring, and serial and Ethernet communications cables.

Cable shields must remain intact up to the boundary of the enclosure, and must be connected to earth at the boundary of the enclosure:

- Shielded cables must use a gland or a shielded cable connector at the location where they enter the enclosure. The gland or shielded connector chosen must provide the shortest possible path between the cable shield and the enclosure wall.
- Communications cables should use shielded twisted pairs.
- Each power input (field power and system power) must have an inline EMC filter bonded directly to the EMC enclosure. The filters must be rated appropriately for the load.
- Do not use pigtails to make earth connections for cable shields. These can act like miniature antennas and make EMC emissions worse.

System Power Requirements

The system's power supplies and distribution, if incorrectly designed, present a potential common cause failure. It is therefore necessary to:

- Establish the power philosophy, specific earthing philosophy3, required voltage and power requirements, and the separation requirements where items of equipment are separately supplied, for example, system internal supplies and field loop supplies.
- Define the architecture of the Power Supply Units (PSU), for example, 100% redundancy, dual N +1 redundancy, etc. and ensure that each power source is of adequate capability.
- Ensure that the PSUs are compatible with the power feeds provided. Alternatively, measures should be implemented to ensure that the PSU power feeds remain within the PSU specifications.
- In high demand energize to trip and continuous demand mode of operation additional protection will need to be in place to inherently limit each processor power supply to a maximum 32V.
- Define the power distribution requirements, together with the protective philosophy for each distribution, for example, current limited at source or protective devices. Where protective devices are

used, it is important to establish that sufficient current be available to ensure their protective action and that the protective device can break the maximum prospective fault current.

- Ensure that the power distribution media is sized to accommodate the maximum prospective fault currents and tolerable voltage losses. This is specifically important where floating supplies are employed and other power sources may result in high prospective fault currents if there are multiple earth-fault conditions.

The system modules require two 24V DC power feeds, with a common return path, i.e. the 24V return is common between the power feeds.

Where other than Trusted power supplies are used, they shall conform to the electrical requirements defined in EN 61010-2-201 in addition to the electrical requirements and tests for EL1 defined in EN 62368-1, where the EL1 (formerly referred to as SELV/PELV) upper limit is <= 60V DC.

DC Output Module Field Power Reverse Polarity Protection

Trusted DC output modules require the use of external reverse polarity protection devices to ensure conformance to IEC 61131 part 2 and to help prevent damage to the output module if field power wiring is inadvertently reversed. Since the reverse polarity protection devices are intended to prevent against wiring faults, it is required that these devices are independent of the power supply. When selecting a reverse polarity protection device, ensure that the reverse polarity protection device's voltage and current ratings are adequate to meet the field voltage and maximum field current of the protected DC output modules.

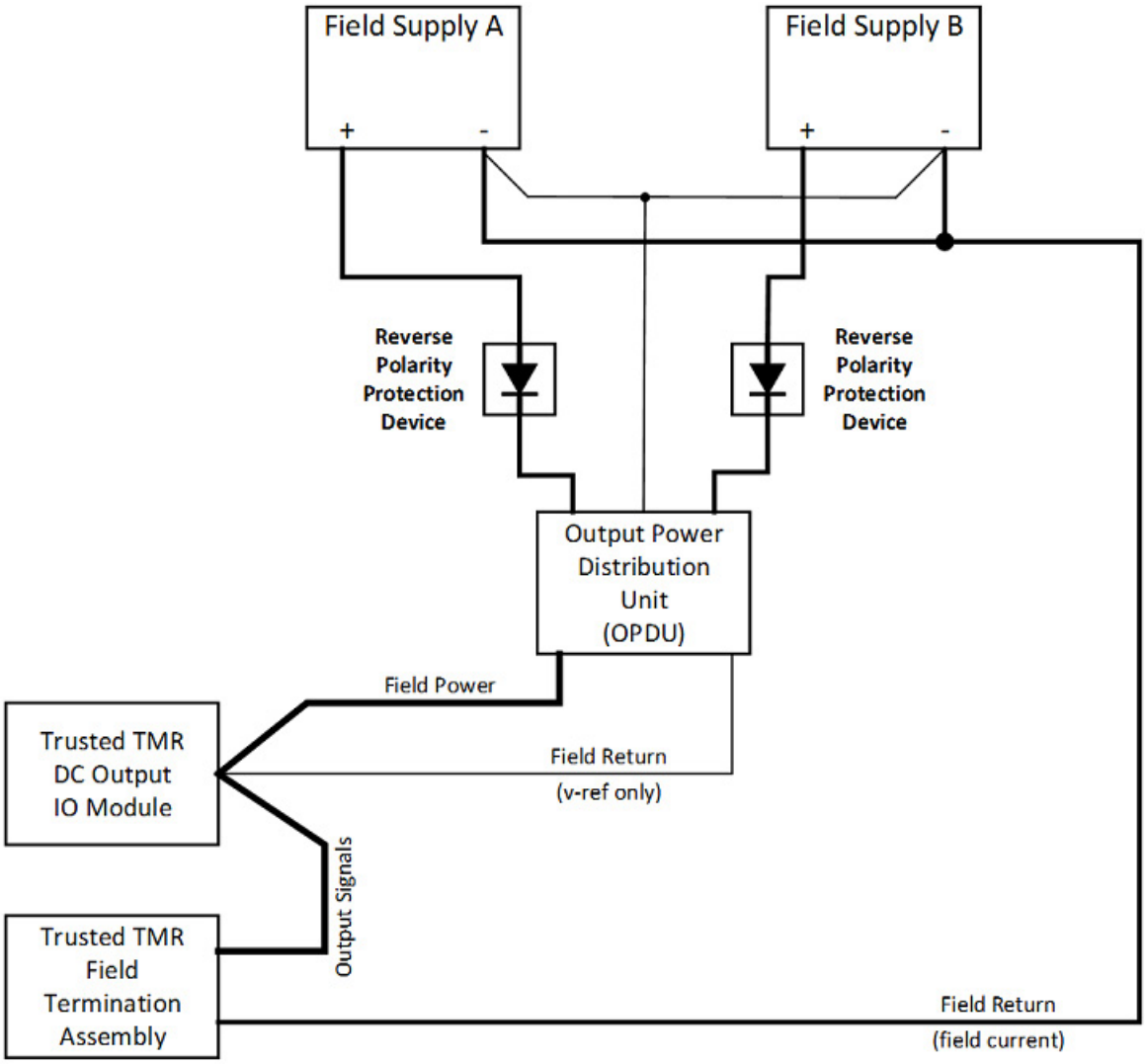


Figure 5: Example - DC Output Module Field Power Reverse Polarity Protection

Electrostatic handling precautions

The following handling precautions shall be observed:

1. Personnel should earth themselves before handling modules.
2. Modules should not be handled by their connectors.
3. Do not remove modules from their packaging until required for use.

Example checklists

This section provides a number of example checklists, these are provided as an aid for competent engineers. In general each checklist item should result in "yes", where this is not the case a justification should be produced.

Example pre-engineering checklists

The checklists provided within this section are applicable to the requirements. It should be recognized that the requirements will undergo refinement, particularly, in the early stages of a project. The information provided initially may be 'outline'; in this case, these checklists should be used to help identify where omission has occurred or where further refinement is necessary.

Table 4-1 - Example Scope Definition Checklist

Description	Reference	Yes/No
Has a summary description of the intended application been provided?	Scope definition on page 22	
Is the intended installation environment defined? If so: Does this include both normal and possible abnormal conditions? Does this include geographical distribution requirements?	Scope definition on page 22 and Environmental requirements on page 72	
Has a list of all the third-party equipment interfaces been provided and are definitions of both the protocol and the data to be interchanged established?	Scope definition on page 22	
Are all of the plant interfaces defined, including the signal qualities and characteristics?	Scope definition on page 22	
Have any special or abnormal conditions that exceed the normal equipment capabilities been highlighted to enable special measure to be implemented?	Scope definition on page 22	
Is the presented information adequate to support the necessary level of understanding of the plant/Equipment Under Control (EUC) and its environment?	Scope definition on page 22	

Table 4-2 - Example Functional Requirements Checklist

Description	Reference	Yes/No
Is the definition of each of the required functions complete?	Functional requirements on page 22	
Are the interfaces, signals, and data associated with each function clearly identified?	Functional requirements on page 22	
Where a 'tag referencing' scheme is used for these signals, has a summary description of the naming convention been provided to facilitate an understanding of the role of the signal?	Functional requirements on page 22	
Have the performance requirements for each function, or collective functions, been defined?	Functional requirements on page 22	
Have the operating modes of the EUC, process, or plant been clearly defined?	Functional requirements on page 22	
Have the functions required to operate in each plant operating mode been identified?	Functional requirements on page 22	
Have the transitions between each plant operating mode been defined? Have the functions necessary to effect these transitions been established?	Functional requirements on page 22	

Table 4-3 - Example Safety Requirements Checklist

Description	Reference	Yes/No
Have all of the functional requirements been allocated a required safety requirements class?	Safety requirements on page 23	
Has the safety-related timing for each safety-related function, including process safety time (PST) and fault tolerance period, been established?	Safety requirements on page 23	
Have the safety requirements been approved?	Safety requirements on page 23	
Are there clear definitions of the external interfaces involved in each of the safety-related functions? (These may already be defined in the functional requirements).	Safety requirements on page 23	
Is there now sufficient information to understand how the plant should be controlled safely in each of its intended operating modes?	Safety requirements on page 23	

Example engineering checklists

This topic provides example engineering checklists.

Table 4-4 - Example I/O Architecture Checklist

Description	Reference	Yes/No
Has the PSTE been established?	Process Safety Time (PST) on page 15	
What is the PSTE?	Process Safety Time (PST) on page 15	
Has the fault detection time for the system been established?	Trusted high-density I/O on page 38	
What is the fault detection time?	Trusted high-density I/O on page 38	
Where the fault detection time is greater than the PSTE, does the safety-related I/O configuration provide a fail-safe configuration? For example, a fault tolerant architecture or used for a low demand application. If not, the system topology shall be discussed with the client to ensure that the system implementation is safe.	Process Safety Time (PST) on page 15	
If a probability of failure on demand has been specified, has this been met?	Process Safety Time (PST) on page 15	
Do the selected architectures provide solutions where there is no single power source or distribution point of failure that could lead the system to fail to function safely when required?	System Power Requirements on page 76	
For each of the I/O signal types, do the I/O modules provide the correct characteristics and behavior for the intended sensor or actuator (including minimum and maximum load requirements)? If not, have additional interfacing elements been included to ensure that the effective signal is compatible with the selected module type?	Energize to trip configurations on page 42	
Are the selected I/O module types compatible with the required I/O architecture?	Safety-related configurations on page 34	
Is the safety-accuracy adequate for the application? If active and standby modules are to be installed simultaneous, has allowance been included for the effect on the accuracy?	Analog input safety accuracy on page 42	
Has the allocation of signals to I/O modules and channels considered each of the signals' function? Ensure that potential module and power group failures result in either continued safety function or fail-safe operation.	Safety-related configurations on page 34	
Do safety-related inputs and outputs use only those configurations identified as safety-related	Safety-related configurations on page 34	
Are there any safety-related, normally energize to trip outputs? If so have redundant power sources, power failure warning and line monitoring been provided?	Energize to trip configurations on page 42	
Have sensor fault conditions been taken into account?	Final element configurations on page 48	
Have actuator fault conditions been taken into account?	Final element configurations on page 48	
Have field power supplies conforming to the electrical requirements defined in EN 61010-2-201 in addition to the electrical requirements and tests for EL1 (formerly referred to as SELV/PELV) defined in EN 62368-1 been used?	System Power Requirements on page 76	

Table 4-5 - Example Language Selection Checklist

Description	Reference	Yes/No
Has application programming for safety-related sections been limited to the FB, IL, ST & LD programming languages? Note: Instruction list (IL) language is obsoleted in the SIS Workstation Software.	Language selection on page 62	
Are any functions not in the previously tested libraries required? If so has provision been made to adequately test these functions?	Testing of new and previously untested functions on page 64	
Ensure that the programming language classified as non-safety (SFC) is NOT used for safety-related projects	Language selection on page 62	

Table 4-6 - Example Maintenance Override Requirements checklist

Description	Reference	Yes/No
Are the effects of overriding fully understood, particularly where the override action will affect independent parts of an application?	Maintenance overrides on page 56	
Has a method of enabling, or more importantly removing, the overrides for the system as whole, or individual subsystems, been provided?	Maintenance overrides on page 56	
Have programming or procedural measures been defined to ensure that no more than a single override may be applied to a given safety-related process unit?	Maintenance overrides on page 56	
Have indication of the presence of override conditions and recording their application and removal been defined?	Maintenance overrides on page 56	
Is there an alternative method of removing an override?	Maintenance overrides on page 56	
Are there programming or procedural measures to limit the period of override?	Maintenance overrides on page 56	

Table 4-7 - Example High-Density Module Configuration Checklist

Description	Reference	Yes/No
For each of the I/O signal types, do the I/O module settings provide the correct characteristics and behavior for the intended sensor or actuator?	Module characteristics on page 51	
Have the thresholds been verified with both increasing and decreasing field signal levels and with margins to allow for the accuracy and calibration to ensure that they do not result in overlapping bands?	Module characteristics on page 51	
Is consistent use made of front panel indicators? Ensure that "green" is not used for abnormal conditions.	Module characteristics on page 51	
Have the update rates been set such that they are acceptable for fault annunciation requirements and that the rates result in the system's response within the PSTE.	Module characteristics on page 51	
Have the settings been defined according to a field device type setting, and minimal use has been made of channel-specific settings?	Module characteristics on page 51	
For any non-standard configuration settings, have tests been defined and executed to 100% test the required operation?	Module characteristics on page 51	

Table 4-8 - Example Trusted TMR Processor Configurations Checklist

Description	Reference	Yes/No
If Peer to Peer communications is used, are the timeouts set to ensure a response time less than that required by PSTE?	Peer to Peer communications configuration on page 57	
Has the diagnostic access password been set?	Diagnostic access on page 51	
Has the security been set up on the SIS Workstation Software or Trusted Toolset Suite?	Diagnostic access on page 51	
Has the Engineering supervisor password been set? (For Trusted Toolset Suite only)	Configuration on page 59	
Has the Engineer/ Application programmer password been set? (For Trusted Toolset Suite only)	Configuration on page 59	
Has the Maintenance engineer password been set? (For Trusted Toolset Suite only)	Configuration on page 59	
Has the General user password been set? (For Trusted Toolset Suite only)	Configuration on page 59	

Table 4-9 — Example Testing Checklist

Description	Reference	Yes/No
Have all of the functions used been fully tested?	Language selection on page 62 and Testing of new and previously untested functions on page 64	
Has the program been fully tested? The code checker can be used to highlight which programs have changed during modification.	Code comparison on page 69	
Record the application scan time (read from the SIS Workstation Software or Trusted Toolset Suite display)	Program testing on page 68	
Record the system throughput time (output SOE – input SOE)	Program testing on page 68	
Record the system throughput time where Peer to Peer communications is required (output SOE – input SOE)	Program testing on page 68	
Are the scan and response times in accordance with the PST_E requirements (< ½ PST_E)?	Program testing on page 68	
Have the climatic conditions been verified to be suitable?	Climatic conditions on page 73	

Previously assessed functions

The following list shows those function blocks that have been proven safe to use in certified systems.

Function	Description
Boolean	
(>=1)	Logical OR (2 to 16 inputs)
(&)	Logical AND (2 to 16 inputs)
( )	Inverted Line (Boolean inversion)
(=1)	Exclusive OR
(RS)	Reset dominant Latch
(SR)	Set dominant latch
(ftrig)	Falling edge detection
(rtrig)	Rising edge detection
Timers	
(TON)	Timer delay off
(TOF)	Timer delay off
Counting	
(CTU)	Counter
Comparison Tests	
(>=)	Greater than or Equal to
(<=)	Less than or Equal to
(=)	Equal to
(>)	Greater than
Arithmetic	
(+)	Add (2 to 16 inputs)
Logic	
(And Mask.)	And Mask
Signal Generation	
(sig_gen)	Function Generator
Data Manipulation	
(sel)	Binary selector (Selects one of 2 integer variables)
(MOD)	Modulo
Register Control	
(SHR)	Shift Right
Data Conversion	
(Boo)	Converts any variable to a Boolean
(Ana)	Converts any variable to an Integer
(Tmr)	Converts a variable for use by a timer

Function	Description

System security

Serial networks are closed and local, and have limited protocol functionality. They are therefore immune to any attack except local deliberate sabotage. Trusted TMR Systems, however, with their Engineering Workstations and DCS, are Ethernet networks that tend to be part of a larger corporate network, which opens up limitless possibilities for accidental or malicious infection or attack.

The following mitigative steps shall be considered when assessing the security risks identified in the security assessment:

- The Trusted TMR System should not be on a network with open access to the internet. Refer to publication SECURE-RM001 for recommendations on network firewall.
- The Firewall must be active on the Engineering Workstation, preventing access to the relevant Ethernet ports on each communication interface and antivirus software must be installed and up to date.
- The Engineering Workstation, containing the SIS Workstation Software or Trusted Toolset Suite, should be password-protected. If it is a laptop, it should be kept locked as it is the key to the application
- The Ethernet Telnet access should be kept closed ("tcp diag" off) until required.

WARNING:
Use the Trusted System Configuration Tool and set a new password (it is recommended to change the default password for a more secure one). This password will give access to the privileged diagnostic console 'su' command to grant access to more invasive commands (ie: ability to execute NIO CLI commands).

- If the Trusted Toolset Suite uses a USB or parallel dongle, this should be kept securely. Without it, the Toolset will not run at Trusted Toolset Suite version 3.51 and above. At Trusted Toolset Suite version 3.46, the application compilation will not complete.
- Keep the maintenance lead securely stored because it can be used for both configuration and diagnostics.
- Ensure that the full compiled application and the system configuration are securely backed up. The configuration can be recovered from the Trusted TMR Processor but the application cannot and a full copy of the application is needed for modifications.
- The application should be password-protected.

- Trusted is quite resistant to radio interference due to its voting structure. However, sensible use of site radios is advised; do not use radios inside or near an open panel. The panel doors form part of the RFI protection; the plastic module cases provide no protection.
- The panel doors should be closed and locked. Key operated locks are more secure than tool operated locks. Terminals, plugs, fuses, and relays can all be dislodged, so are best kept secure.
- The Trusted TMR Processor keyswitch should be turned to the "**Run**" position and removed. This helps prevent download of system configurations or online changes through the SIS Workstation Software or Trusted Toolset Suite.
- The module ejectors should remain closed. The ejector tool can be kept with the TMR Processor key. This makes it more difficult to remove modules.
- Removable media (USB storage devices, CDs etc.) should be virus checked before use within the system.

Regent and Regent+Plus I/O

The Regent and Regent+Plus (Low Density) I/O modules provide internal TMR interfacing. Other elements of individual modules may be non-redundant (depending on module type) to support 'slice redundancy' in redundant module configurations. To optimize the system's safety availability, the self-test functions are timed to take only a small part of the system resources.

In non-redundant configurations, it is important that the resulting test interval be sufficiently short to ensure the system's ability to respond within the process safety time. For these configurations, the test interval (TI) is given by:

$TI = (172 * IOU * T_{scan}) + 2$

Where:

- TI = test interval in seconds
- IOU = number of Low Density I/O chassis
- T_{scan} = system scan time in seconds

Note: Regent and Regent+Plus I/O Low Density modules are certified as non-interfering to the Trusted TMR Controller but retain the DIN19250/AK5 certification of the original Regent and Regent+Plus I/O system.

The Regent+Plus User's Guide provides additional information on the configuration and use of Low Density I/O, including I/O module-specific restrictions that must be followed.

Effect of Input Architectures

If the four basic low density input configurations and the effect of the fault detection time are considered, then:

1. For a simplex input configuration, the logic signal into the application will remain at the state before detection until the fault detection time has expired, and will then take up the logic '0' condition. This is not fault tolerant and only becomes fail-safe after the fault detection period or test interval. If the sum of the TI, and 2× T_{scan} is not less than PST_E, then an alternative I/O architecture shall be chosen. If the demand rate is low, this can be acceptable for shutdown functions.
2. In (1002) configurations, the system remains active during the fault detection time but will trip when the fault detection time expired.

3. In 2002 configurations, the input remains static during the fault detection period, but returns to operation when the fault detection period expires. This is fault tolerant but the system is inactive during the fault detection time. As before, if the sum of the TI, and 2× T_{scan} is not less than PST_E, then an alternative I/O architecture shall be chosen. In this configuration, the input modules shall be in separate chassis.
4. When a (2003) configuration is used the system remains operational at all times and tolerates the failure.

Effect of Output Architectures

If the three basic low density output configurations and the effect of the fault detection time are considered, then:

1. For a simplex output configuration, the output may be indeterminate if there is a failure. Additional outputs may be used to provide a fail-safe mechanism on an output group basis. The output will remain indeterminate until the fault detection time has expired, with the additional output fail-safe the output group will then take up the fail-safe (logic '0') condition. This is not fault tolerant and only becomes fail-safe after the fault detection period or test interval. If the sum of the TI, and 2× T_{scan} is not less than PST_E, then an alternative I/O architecture shall be chosen.
2. Guarded output modules provide a one-out-of-two (1002) structure within a single module. A single fault may result in an indeterminate condition on a redundant output channel, leading to either immediate fail-safe action, or action by the other channel on demand. A faulty output will be detected within the fault detection period, and shall be replaced within the second fault occurrence period to ensure continued functional safety. This provides a fail-safe output structure and may be used within safety-related configurations.
3. Dual guarded outputs, this structure uses two guarded output modules in parallel, i.e. a quad output structure. This structure is both fault-tolerant and fail-safe. As with other dual structures, a failed output shall be replaced within the second fault occurrence period to maintain continued safe operation.

Table A-1 Input Module, Low Density I/O

Modules	Certified Configuration Risk Class AK5	Conditions
Digital Inputs T7401, 24V DC T7402, 48V DC T7404, 110V AC T7408, 120V DC	1oo2 or 2oo3 or 1oo3	De-energize to trip: certified only if the inputs are dynamically transitioned at a period not greater than the SFOC. 1oo3 configuration means that the three input signals cannot be voted. Any mismatch of the signals leads to an alarm annunciation.
Monitored Inputs T7411, 24V DC T7411F, 24V DC T7418F, 120V DC	1oo2 or 2oo3	Certified for de-energize to trip and energize to trip: certified only if the inputs are dynamically transitioned at a period not greater than the SFOC. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42.
T7419, fire detector, 16 point line monitored	MooN	

Table A-1 Input Module, Low Density I/O

Modules	Certified Configuration Risk Class AK5	Conditions
Analog Inputs T7420A, standard T7420AF, fast response	2oo3 with mid value select or dual with high/low select	Certified only if the inputs are dynamically ranged over full scale at a period not greater than the SFOC.
Other Inputs T7431A, thermocouple	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical input devices.
Input and Output Multiplexer T7491	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical input devices.

Table A-2 Output Modules, Low Density I/O

Modules	Certified Configuration Risk Class AK5	Conditions
Guarded Digital Outputs T7461A, 24V DC T7462A 48V DC T7485 L/H, 120V AC	Fail-safe single module (1oo1) or Fault tolerant dual modules (2oo2)	De-energize to trip: certified. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42, and only if the outputs are dynamically transitioned 0->1->0 or 1->0->1 at a period not greater than the SFOC.
Monitored Guarded Outputs T7481, 24V DC T7484, 110V AC T7488, 120V DC	Fail-safe single module (1oo1) or Fault tolerant dual modules (2oo2)	De-energize to trip: certified. Energize to trip: certified only for applications that fulfill the requirements under Energize to trip configurations on page 42.
Other Outputs T7441A, 24V DC T7444, 110V AC T7446L/H, relay T7454, 110V AC, isolated T7464, 110V AC, guarded T7470A, Analog T7480A, Analog, guarded	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical output devices.
Input and Output Multiplexer T7491	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical output devices.

DX and TX Low Density module types in Safety applications

When using DX (Dual) and TX (Triple) Low Density I/O redundant voting configurations certain defensive measures are needed; refer to publication ICSTT-RM255 (PD-T8160) for detailed configuration options for each module type. These structures provide discrepancy and error information but do not take into account of SFOC. If these structures are used in a safety function, it is required that the logical state of each channel be defaulted to a safe state within the logic. For DX modules, this time must be less than the systems process safety time. For TX modules, this must be less than the SFOC.

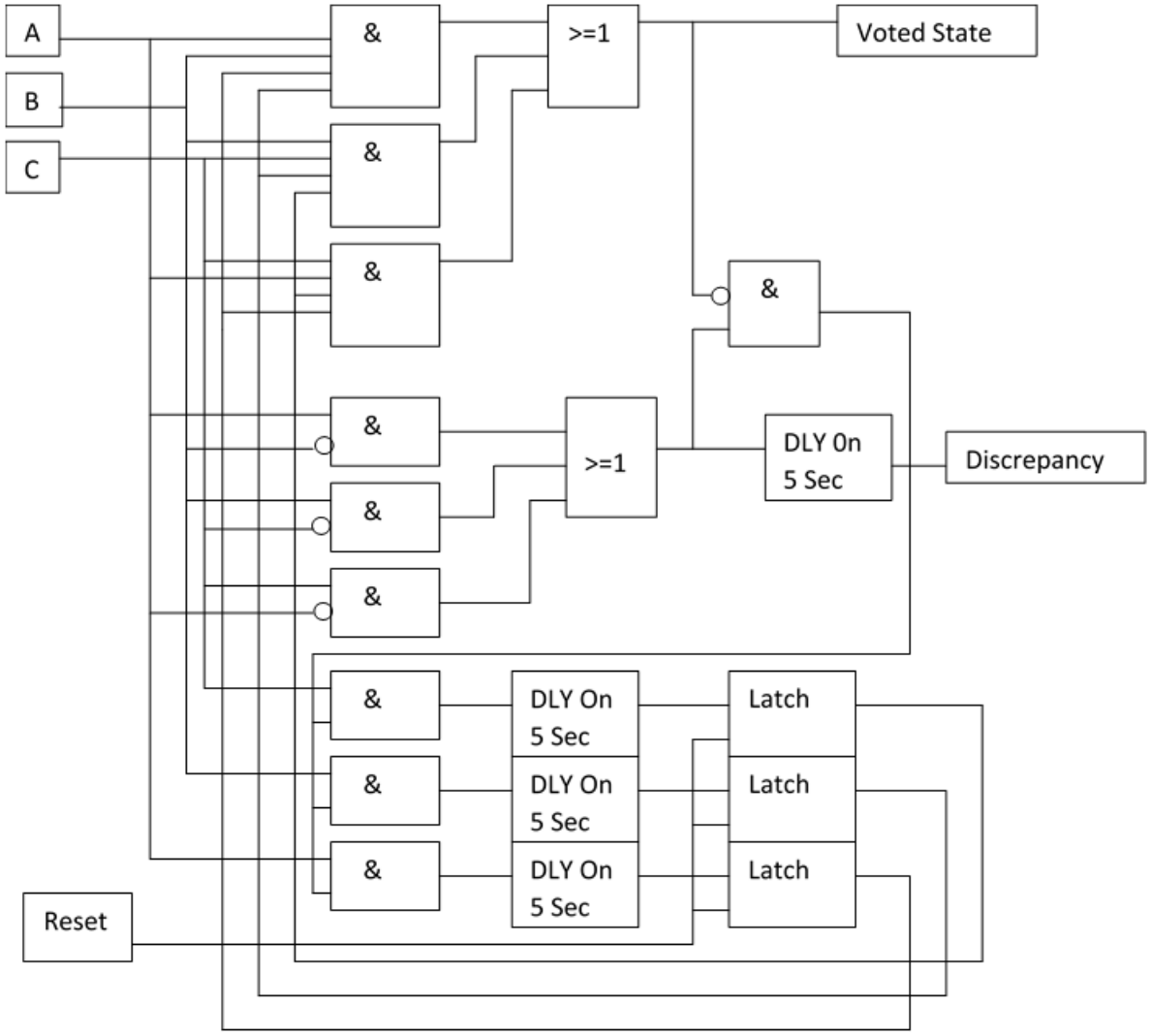


Figure 6: 2003 voting logic with discrepancy reporting

In safety-related applications it is recommended where 2003 fault tolerance is required, three SX (Simplex) modules should be used, and the 2003 vote performed in the application program. Within the application, the vote must detect discrepancies on a per channel basis and cause the discrepant channel to default to a safe state. In the event that an input fails to the energized state and is declared as discrepant it must be forced to a safe state within the voter logic. Should a second input go to the energized state, and not be confirmed by the third within the defined time period, that input will also be forced to a

safe state thus preventing energizing of the logic until a reset is operated. Below is a function that performs this logic. There are many implementations that can be used but the functionality should be retained.

The sample application logic above uses a 5 second discrepancy timeout period. The actual timeout period used should be based on the process safety time, and must not exceed the SFOC.

In safety-related systems the logical state from DX type modules must be forced to the safe condition by the application program if the error bit for that channel is set to a "1". This action can be delayed to help prevent unwanted control actions but the total time of the logical delay, the MSEC delay set within the module and the system throughput must not exceed the "Process Safety Time" for the application.

In this configuration, the error bit must be latched by the application and manually reset after the discrepancy has been removed.

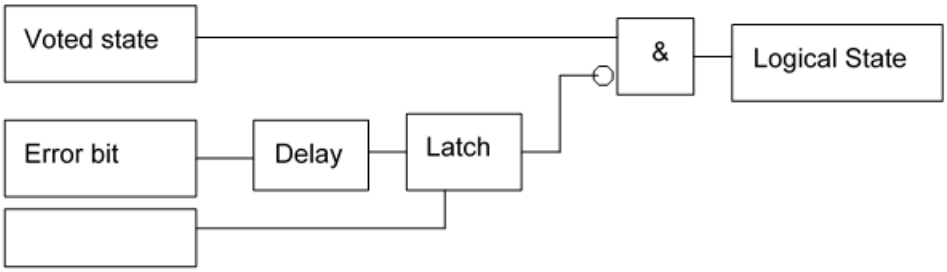


Figure 7: Discrepancy error bit latch and manual reset logic

Triguard

For guidance on how to upgrade a Triguard SC300E system to a hybrid Trusted/SC300E system, see application note AN-T80015.

Triguard I/O

The Triguard SC300E I/O modules provide internal TMR interfacing. Other elements of individual modules may be non-redundant (depending on module type) to support 'slice redundancy' in redundant module configurations. To optimize the system's safety availability, the self-test functions are timed to take only a small part of the system resources.

The test interval (TI) to ensure the system's ability to respond to latent errors within the system PST is given by:

$$TI = 20 \times IOU \times I/O$$

Where:

- TI = test interval in seconds
- IOU = number of Triguard I/O chassis
- I/O = number of I/O modules in a chassis

Effect of input and output states

This section provides information about the effect of input and output states.

Effect of input states

If the three basic Triguard input states and the effect of the fault detection time are considered, then:

1. For a simplex input configuration (used in non-SIL applications), the logic signal into the application will remain at the state before detection. This is not fault tolerant and does not test the simplex elements. The module is however interference-free.
2. In one-out-of-three, second critical fault (1003) situations, the system remains active until the fault is detected during normal data or status reads by the MP and accessed by the application. The application then carries out a controlled plant shutdown if it is a critical input.
3. In two-out-of-three (2003) the system remains operational at all times and tolerates the single failure.

Effect of output states

If the single basic state and the effect of the fault detection time are considered, then:

1. Output modules provide a two-out-of-three (2003) structure within a single module with one slice fault. A faulty output will be detected

within the fault detection period, and shall be replaced within the second fault occurrence timeout period to ensure continued functional safety.

Table B-1 Central Modules

Modules	TÜV Certified Configuration	Conditions
Triguard Interface, 8161 SC300E Bridge Module	Simplex (2oo3 implemented in a set of three modules)	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.
Local Chassis Interface, MBB	Simplex (2oo3 implemented in a set of three modules)	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.
Remote Slave Interface, MRB01XS	Simplex (2oo3 implemented in a set of three modules)	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.
Remote Master Interface MRB04XM	Simplex (2oo3 implemented in a set of three modules)	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.

Table B-2 Input Module, Triguard I/O

Modules	TÜV Certified Configuration	Conditions
Digital Inputs MDI32BIS, TMR, 24V DC MDI32GIS, TMR, 48V DC MDI32FIS, TMR, 120V DC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip: certified to SIL 3 IEC 61508 Ed 1 of the original SC300E system. Energize to trip: certified only for applications that fulfill the requirements under section 3.2.4.
Digital Inputs MDI64BNS, Simplex, 24V DC	Simplex 1oo1	De-energize to trip. Certified as non-interfering and can be used for non-safety-critical input devices.
Analog Inputs MAI32(L/M)AD, TMR 0-5/10 V MAI32(N/P)AD, TMR 0-20/40 mA	Internal 2oo3 (2oo3 implemented in a single module)	Within the manufactures specified safety accuracy limits. The safety state of the analog input has to be defined to 0 mA/0 V Certified to SIL 3 IEC 61508 Ed 1 of the original SC300E system.

Table B-3 Table Output Modules, Triguard I/O

Modules	TÜV Certified Configuration	Conditions
Digital Outputs MDO32BNS, TMR, 24V DC MDO16GNS, TMR, 48V DC MDO16FNS, TMR, 120V DC MDO16CNS, TMR, 120V AC	Internal 2oo3 (2oo3 implemented in a single module)	De-energize to trip): certified to SIL 3 IEC 61508 Ed 1 of the original SC300E system. Energize to trip): certified only for applications that fulfill the requirements under section 3.2.4. May be used in single module or active/standby configurations.
Analog Output MAO04NND, TMR, 0-22 mA	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical devices.

Table B-4 Triguard Multi-purpose Modules

Modules	TÜV Certified Configuration	Conditions
Analog Output / Pulse Input MHB44IND, TMR, 4-20 mA, 1 Hz-35 KHz	Not safety-related but interference free	Certified as non-interfering and can be used for non-safety-critical devices.

Table B-5 Auxiliary Chassis and PSUs

Modules	Conditions
Controller Chassis 8100	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.
Primary, Secondary and Remote Triguard Chassis	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.
Power Supplies PAC, PDC	Certified as safety-related and can be used for safety-critical applications to SIL 3 IEC 61508 Ed 1.

Safety-related inputs and outputs

The Safety Loops, Cause and Effect Charts or other design data will define which loops are to be considered as Safety Loops. All inputs and outputs associated with Safety Loops must follow the design guidelines laid out in this section.

- All Modules must be configured for 3-2-0 fail-safe operation.
- All output modules associated with Safety Loops must be configured with adjacent hot repair partner slots. The hot repair partners for output modules must not be fitted during normal operation.
- If the process time constraint is less than 30 seconds, or only single sensors are provided for process measurement, then all input modules associated with safety loops must also be configured with adjacent hot repair partner slots.

Inputs

Safety inputs to a Safety System will be either De-energize to trip inputs or analog inputs.

Digital inputs

De-energize to trip inputs (usually termed fail-safe) will be used for all safety digital inputs. The number of safety monitoring signals required for each safety parameter will depend primarily on the safety integrity level (safety classification) required to be achieved, the 100% proof test cycle required and the level of diagnostics available from the field device.

All safety digital inputs will be wired to a Digital Input Termination Card. Where the safety integrity level requires that more than one field sensor monitoring a safety parameter, each of these sensors should be, where practical, wired to separate Termination Cards. The Simplex part of the termination card (for example, fuses) must be considered for reliability analysis as part of the field loop.

The Termination Card will be connected to the Triguard SC300E Input Module via a standard system cable that connects to the socket on the appropriate Hot Repair Adapter Card or chassis slot.

Through the hot repair adapter card, where required, and the chassis backplane connector the input signal is connected to the configured digital input slot position where a Digital Input Module would be located.

All the chassis slots and, where required, its hot repair partner slots configured for the Digital Input Module must also have the polarization keys fitted and configured for this type of module as specified in the Module and Chassis Users Manuals.

Where the safety integrity level requires that separate sensors are used to monitor the same safety parameters they should be configured to separate Digital Input Modules where practical.

Analog inputs

Analog transmitters are used to monitor safety parameters and inherently provide an increased level of diagnostics with respect to a simple fail-safe digital input. Analog signals always provide values within a set operating range. For safety-related transmitters this should be 4-20 mA or 1-5 volts allowing for fault indication below say 3 mA (0.75 V) and 20 mA (5 V). If overrange detection is required, a 0-10 V input module must be used. All monitored faults from the analog signals must be used by the application software to produce fail-safe results (for example, failed transmitter demands a shutdown).

The number of analog transmitters used to monitor a safety parameter will be dependent on the system integrity level (safety classification) requirement of the loop, the 100% proof test cycle of the loop and the level of diagnostics available from the transmitter.

The field analog signal is wired to the Analog Input Termination Card. Where the safety integrity levels require that more than one transmitter is used to monitor a safety parameter, then the additional analog input signals should be wired to separate Termination Cards where practical. The Simplex circuitry on the termination card must be considered for reliability as part of the transmitter loop (for example, fuses and monitoring resistors where fitted). Refer to Figure B-1.

The signal is connected from the termination card to the Triguard SC300E input module via a standard system cable, which connects to the socket on the appropriate Hot Repair Adapter Card or chassis connector.

Through the Hot Repair Adapter Card, where required, and the chassis backplane connector the input signal is connected to the appropriate configured analog input module slot position, where an appropriate Analog Input Module would be located.

All the chassis slot and, where required, their hot repair partner slots configured for the Analog module must also have the polarization keys fitted and configured for this type of module as specified in the Module and Chassis User Manuals.

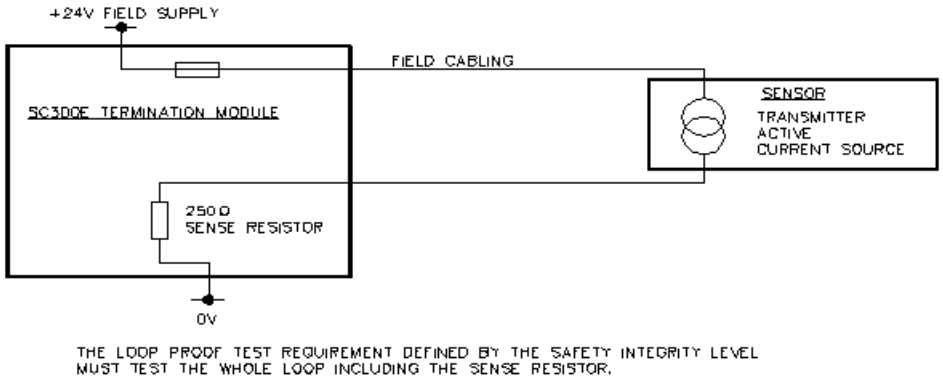


Figure 8: Current to Voltage Conversion

Where separate transmitters are used to monitor the same safety parameters to meet increased integrity levels these should be configured to separate Analog Input Modules where practical.

Switch inputs with end of line and series line-monitoring resisters fitted may be connected as analog inputs. These line-monitored inputs provide increased diagnostic information to the safety system giving discrete analog values (step changes) for open circuit, switch open, switch closed, and short circuit conditions.

Fail-safe analog processing

For each analog input variable received by the system, three values are generated, one from each channel. Under normal operation (transparent to the application) a standard mid-value selection algorithm is used, selecting the middle value (assuming all three values are within the health window) to be passed to the application. It is this mid-value that the user operates on within the application, all three processing channels now using this selected mid-value.

When one of the three analog channel values presented to the TMR Processors falls outside of the health window, the TMR Processors flag it as bad by converting it to a negative number. If now the two remaining values diverge by more than the health window, these are also flagged as bad by converting them to negative numbers. The effect is to present to the application a negative value when two or more channels are bad.

The application, by use of either an analog processing module or simple comparators, can provide a bad/safe discrete value for each analog value.

When large numbers of analog inputs are to be processed, a function should be used to monitor faults within the analog loops effectively.

This configuration provides for each analog variable an array of discrete values for channel faults, open and short circuit faults, as well as defining a global fault bit and the test parameters. Both open and short circuit faults values should be configured.

Outputs

This section provides information about outputs.

De-energize to trip outputs

All safety-related outputs will be from the Digital Output Module. Each module must be configured with a hot repair partner slot to allow bumpless hot repair to be accomplished.

The Output Module provides a fully tested six-element switch voting circuit for each individual output.

Where the safety integrity level (safety classification) requirements of a safety loop require two or more final elements to be available for shutdown purpose, then each final element should be driven from a separate Digital Output Module and Termination Card, where practical.

The shutdown signal is connected from the Output Module through the chassis backplane, the hot repair adapter card, and the system cable to the Termination Card where the field wiring is connected.

The simplex part of the termination module (for example, fuses) must be considered as part of the field loop for reliability analysis.

Multiple input/output safety configuration

Where the safety integrity level requires multiple sensors and final elements from a safety loop, then these configurations will be as follows.

Dual sensors

These will be voted by the application logic in a 1oo2 manner such that either sensor providing an alarm status requires a shutdown.

Where the sensor diagnostics provide fault status then the safety loop may revert to a 1oo1 voting on the good sensor for the time constraint of the sensor's safety loop. At the termination of this time constraint, the loop will demand a shutdown.

A single remaining sensor going into fault will demand an immediate shutdown.

Triplicated sensors

These will be voted on a 2oo3 basis by the application logic; however, once a sensor has been voted as bad, the voting logic will revert to a 1oo2 vote on the remaining two sensors following the strategy determined for dual sensors.

Dual final elements

These are to be configured in a 1oo2 manner such that either output requires a shutdown.

Hot repair adapters

Wherever dual slot hot repair facilities are required, the hot repair adapter boards must be fitted on the chassis backplane.

CS300

Migrating a CS300 Controller

The following definitions are related to CS300 hardware and are used in only this appendix of this manual.

Abbreviations

- ICCB - Integrated computer control board (the legacy CS300 processor board)
- PI - Process Interface
- PIM - Process Interface Module
- TM - Termination Module

Overview

You can migrate the I/O of an existing CS300 controller to a Trusted TMR System. The migration process lets you retain the hardware and wiring of the existing I/O, and take advantage of the benefits of a Trusted TMR System.

This appendix defines how to safely migrate an existing CS300-based system to a Trusted TMR System for a Safety Instrument Function while retaining the DIN19250/AK6 certification of the original system. The migration of a CS300 controller described here is suitable for low demand applications.

Note: These instructions apply to inputs and outputs used for Safety Instrumented Functions. Where I/O points are used for only monitoring, or only redundant indication, these instructions do not necessarily apply. For guidance on how to migrate a CS300 system for non-safety applications, refer to application note AN-T80014.

The migrated system uses a T8100 Trusted Chassis and its T8110B Trusted TMR Processor module running an updated application, together with three 8162 CS300 Bridge Modules (installed in the original CS300 primary rack) and associated cabling. The migrated system retains the original CS300 racks, I/O modules, and field wiring, but the CS386 integrated computer control boards (ICCBs) are removed and the original application is no longer used.

The hardware changes are summarized as follows. The three ICCBs are removed, and three 8162 CS300 Bridge Modules are fitted in their place. A small PCB is fitted to rear of the CS300 rack, and the rack is connected to the Trusted Chassis by a ready-made cable assembly. The original field wiring remains unchanged. It is recommended that the Trusted chassis is installed close to the original CS300 primary rack. This will make operation and maintenance easier.

The software changes are more complex. In particular:

1. The existing application must be recreated to run on the Trusted TMR System.
2. The new application has to retain the safety integrity of the original system. The DIN19250/AK6 standard of the original controller was the predecessor to the SIL 3 rating of IEC 61508, and while the Trusted TMR System is certified to SIL 3, the original I/O will remain DIN19250/AK6.
3. The new application needs to include diagnostic functions to replicate diagnostic functionality that was built into the original application.
4. The new application must monitor the state of the TM118-TWD watchdog module. If the watchdog module times out, the affected outputs must be latched into the tripped state. See TM118-TWD watchdog module on page 109.

Associated documents

This section provides information about associated documents.

Specifications

AN-T80014: Application Note, Trusted / CS300 Migration Process. Rockwell Automation.

BASS 0257: CS300 Safety System Application Guidelines. Rockwell Automation.

Publication ICSTT-RM404 (PD-8162): CS300 Bridge Module

TÜV Certification

The 8162 CS300 Bridge Module is certified as non-interfering to the Trusted TMR System and can be used to migrate existing applications. It is not intended to be used in new safety systems.

The Autotest management function blocks are approved by TÜV Rheinland for use in safety applications.

You can download a copy of the TÜV certificate from:

http://fs-products.tuvasi.com

List of modules for safety-related applications

A legacy CS300 system is often made up by a large variety of components. The list that follows shows the components of hardware that can be used with the Trusted migration in a safety-related application.

Table C-1 List of CS300 Modules Suitable for Safety-Related Applications

Item	Description	Part No. / Revision	Remarks
1	PI-316 extension chassis (6 series)	001-1053	
	... PI-651 bus interface card (qty 3)	099-1037	
	... process interface module (PIM) chassis	031-0531	
2	PI-317 extension chassis (7 series)	001-1054	
	... PI-751 bus interface card (qty 3)	099-1037	
	... PIM chassis	031-0531	
3	Ext. chassis interface board	001-1024-00	
	... assembled PCB	099-1037-03	
4	PI-331/C triplicated power supply 24V DC	001-1011-00	
	... chassis assembly	031-1003-01	
	... modules 24V DC	031-1000-01	

Table C-1 List of CS300 Modules Suitable for Safety-Related Applications

Item	Description	Part No. / Revision	Remarks
	... cooling fan unit	031-1001-01	
4	PI-110/C PI-M cooling module	001-1010-02	
5	PM108 D/C power supply digital termination (24V DC)	001-1039-00	
	... chassis	031-1005-02	
	... power supply module	031-1004-01	
6	TM118-TWD triplicated watchdog timer	001-1032-00	
7	PI-716 digital input board	099-1045	AK6 certified 3 2 0 and 3 2 1
8	PI-726 digital output board	099-1078	
9	PI-727 digital output board	099-1043	AK6 certified 3 2 1
10	PI-732 analog input board (5V unipolar)	099-1042	
11	PI-616 digital input board	099-1124	AK6 certified 3 2 0 and 3 2 1
12	PI-626 digital output board	099-0084	
13	PI-627 digital output board	099-0074	AK6 certified 3 2 1
14	PI-632 analog input board (5 V unipolar)	099-1105	
15	TM-117-RME termination panel digital output monitor (24V DC)	099-1094-00	Only use in dual tested configurations
16	TM-118-D digital termination panel (24V DC)	099-1003	Only use in dual tested configurations
17	TM117-SME digital output testing	099-1097/8/9	
18	TM117-DC digital input	099-1000	
19	TM118-DH digital input	099-1157	
20	TM119-DH digital input	099-1152	

Note: The PI-641 and PI-741 analog output modules and their associated termination panels are also supported by the migration, but for only non-safety applications. Therefore, there is no function blocks associated with these modules.

Requirements for the Trusted TMR system

The Trusted TMR System requires at least a controller assembly and a power system, and possibly an expander system as well. The controller assembly has a T8100 Trusted Controller Chassis to house the essential modules:

- One T8111 or T8110 Trusted TMR Processor.
- One T8311 Trusted Expander Interface modules to provide the interface between the controller chassis and the CS300 chassis.
- One T8151B Trusted Communication Interface for the Ethernet interface to the engineering workstation and, if present, other Trusted systems or third-party equipment. (A T8151C conformal coated version can also be used).
- One T8153 Trusted Communications Interface Adapter, to allow the physical connections to the T8151B Trusted Communication Interface.

The T8100 Trusted Controller Chassis must be installed in a rack with doors and side panels, and the doors must be kept closed during usual operation. This lets the 8162 Bridge Module achieve compliance with its EMC specifications with no degradation in performance. The front door can have a window so that the LEDs are visible. The CS300 equipment must be inside the cabinet and earthed correctly (see Physical Installation Design on page 75). A

complete list of all Trusted items needed for the migration is given in Table C-2.

Table C-2 Trusted Items Needed for the Migration

Item	Description	Remarks
1	T8100 Trusted Controller Chassis	
2	T8111 or T8110B Trusted TMR Processor	
3	8162 CS300 Bridge Module (qty. 3)	
4	TC 324-02 CS300 interface cable connector card	
5	TC 322-02 CS300/SC300E interface cable assembly	
6	T8311 Trusted Expander Interface Module	
7	T8312 Trusted Expander Interface Adaptor	
8	T8151B Trusted Communication Interface or T8151C Trusted Communications Interface (Conformal coated module)	

System architecture features

The three 8162 CS300 Bridge Modules enable the connection between the Trusted TMR System and the legacy CS300 I/O, as shown in this figure:

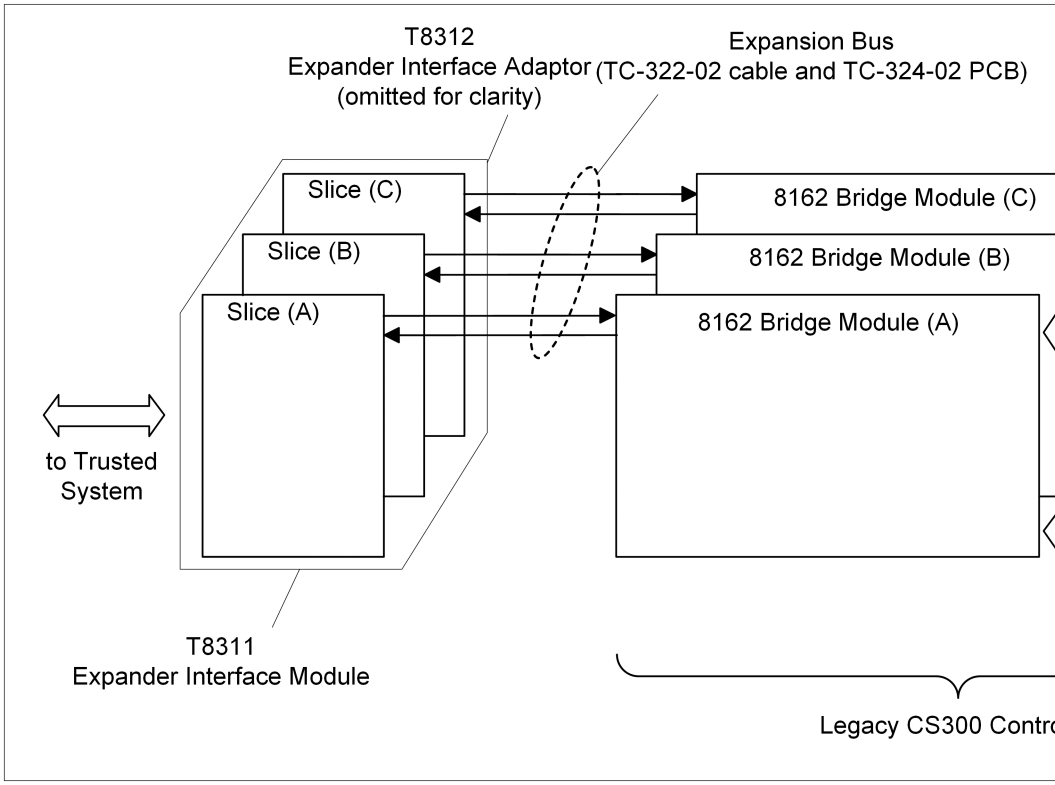


Figure 9: System Architecture features using 8162 Bridge Modules

The system communications must use approved cabling and accessories. In particular:

- The Trusted TMR System carries a T8312 Expander Interface Adaptor and the CS300 rack carries a TC-324-02 PCB.

- There is one TC-322-02 cable assembly. This carries the data between the two items of equipment using a triple, bidirectional communication link.
- Cable assemblies are available up to 15 m long, and the system will support a cable up to 50 m long.

The migrated system will support the pre-existing configuration of the CS300 I/O modules. Communications that existed from the legacy CS300 system to workstations, printers, and distributed control systems must be provided through the T8151 Communications Interface module.

PI-664/PI-774 serial communication boards (if fitted) must be removed.

The system checks output module signals by test routines within the migrated application or by using output line monitoring units. Inputs are checked by a 2003 comparison or (for digital inputs) with the addition of test routines in the application.

The migration supports all of the PI-316 extension racks present in the original system. The existing cabling between the extension racks remains unchanged.

The 8162 CS300 bridge module

The system is designed to use three identical 8162 CS300 Bridge Modules. The data from the three modules is 2003 voted and discrepancy checked by the T8110 Trusted TMR Processor module.

A faulted CS300 Bridge Module should be replaced as soon as practical, and must be replaced within 24 hours. The system requires two unfaulted Bridge Modules at all times, and so if a second CS300 Bridge Module is faulted before the first faulted module is renewed, the system will shut down.

Each of the CS300 Bridge Modules must be powered from the existing PI-331 triple redundant power supply units (PSUs) which support the main CS300 I/O chassis.

Note: Each CS300 Bridge Module consumes less power (and creates less heat) than the original ICCB that it replaces.

The CS300 chassis carries three sets of four backplane jumpers, these are located behind the slots in the chassis for the three CS300 Bridge Modules, as shown in Figure 10: CS300 Backplane Address Jumpers. These jumpers set up the address of the chassis. It is highly recommended that these jumpers are set to represent Trusted address '2'. The jumpers in each set of four are labeled 0, 1, 2 and 3. Fit a jumper link to jumper 1 only (in positions A, B and C) to configure address 2'.

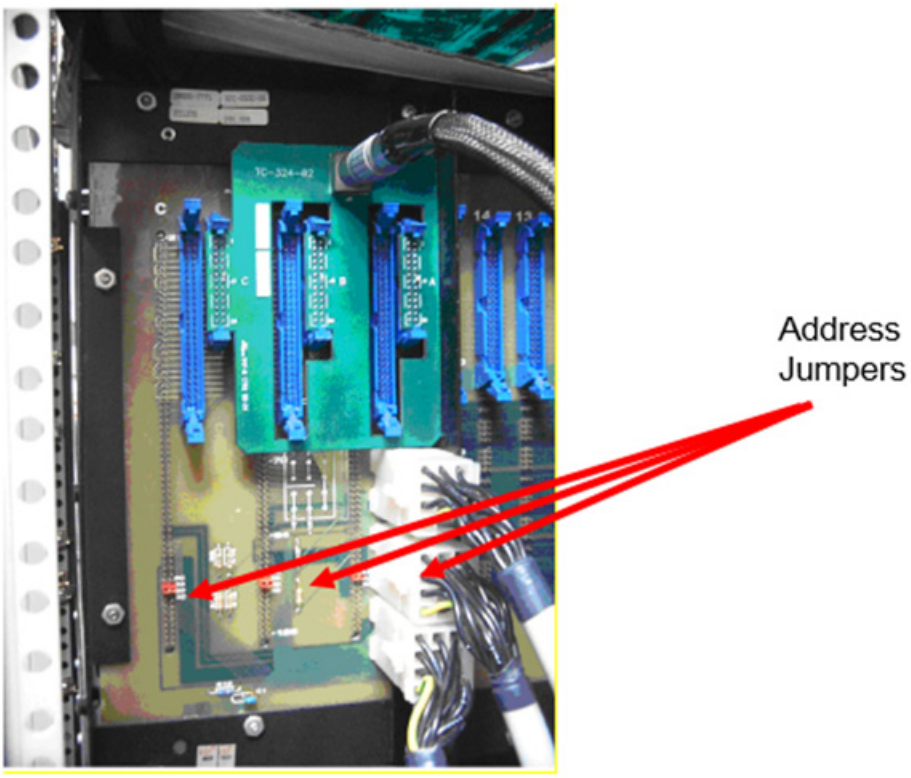


Figure 10: CS300 Backplane Address Jumpers

The Trusted chassis is designated Chassis 1. The original primary rack of the CS300 controller that was designated Chassis 1 is now logical Chassis 2, Chassis 2 (if present) is now logical Chassis 3, and so on. All communications to workstations and DCS systems are through the Trusted communication interfaces.

For more details about the CS300 Bridge Module, refer to ICSTT-RM404 (PD-8162)

CS300 equipment power supplies

Any power supply used with the 8162 CS300 Bridge Module shall conform to IEC 61131 Part 2 (EN 61010-1 or EN 60950-1), where the SELV/PELV upper limit is <= 60V DC.

Note: The power supply monitors its output voltage and temperature. When either is outside their specified limits, then a fault is declared and is reported by a power supply front panel indicator. The CS300 Bridge Module also monitors the power output and will detect an over voltage and declare a fault.

PI-616/PI-716 digital input board

When the PI-616/PI-716 digital input board is used for safety-related applications, it must be configured for 3-2-0 degradation and arranged in one of the tested configurations shown in *Figure 11: Wiring for CS300 simplex digital input module* and *Figure 12: Wiring for CS300 duplex digital input modules*.

PI-632/PI-732 analog input board

The analog input board does not have integrated calibration drift monitoring or a calibration maintenance alarm. This must be implemented in the migrated application. The board must be configured for 3-2-0 degradation and used as shown in *Figure 13: Wiring for CS300 analog inputs*.

When the safety system's availability is analyzed, then the isolated analog input amplifier fitted to the termination panel must be considered in the same way as the input field sensors.

The analog input cards must have their calibration checked during the normal plant maintenance cycle. The analog calibration check must be completed, at a minimum, one time every year.

The Trusted TMR Processor constantly monitors the analog data input from the CS300 slices. When a discrepancy greater than 1% is detected between two slices, a fault is declared.

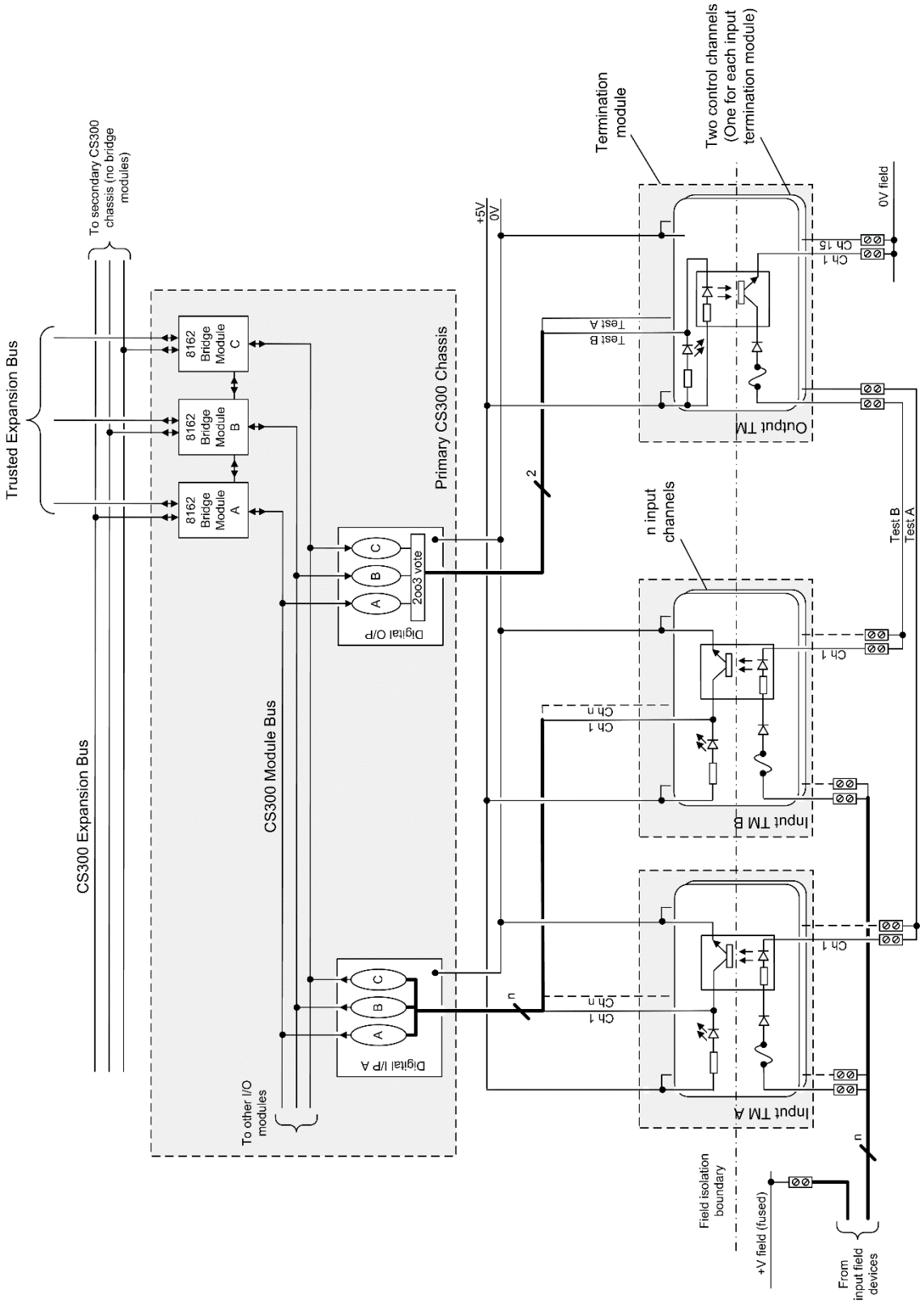


Figure 11: Wiring for CS300 simplex digital input module

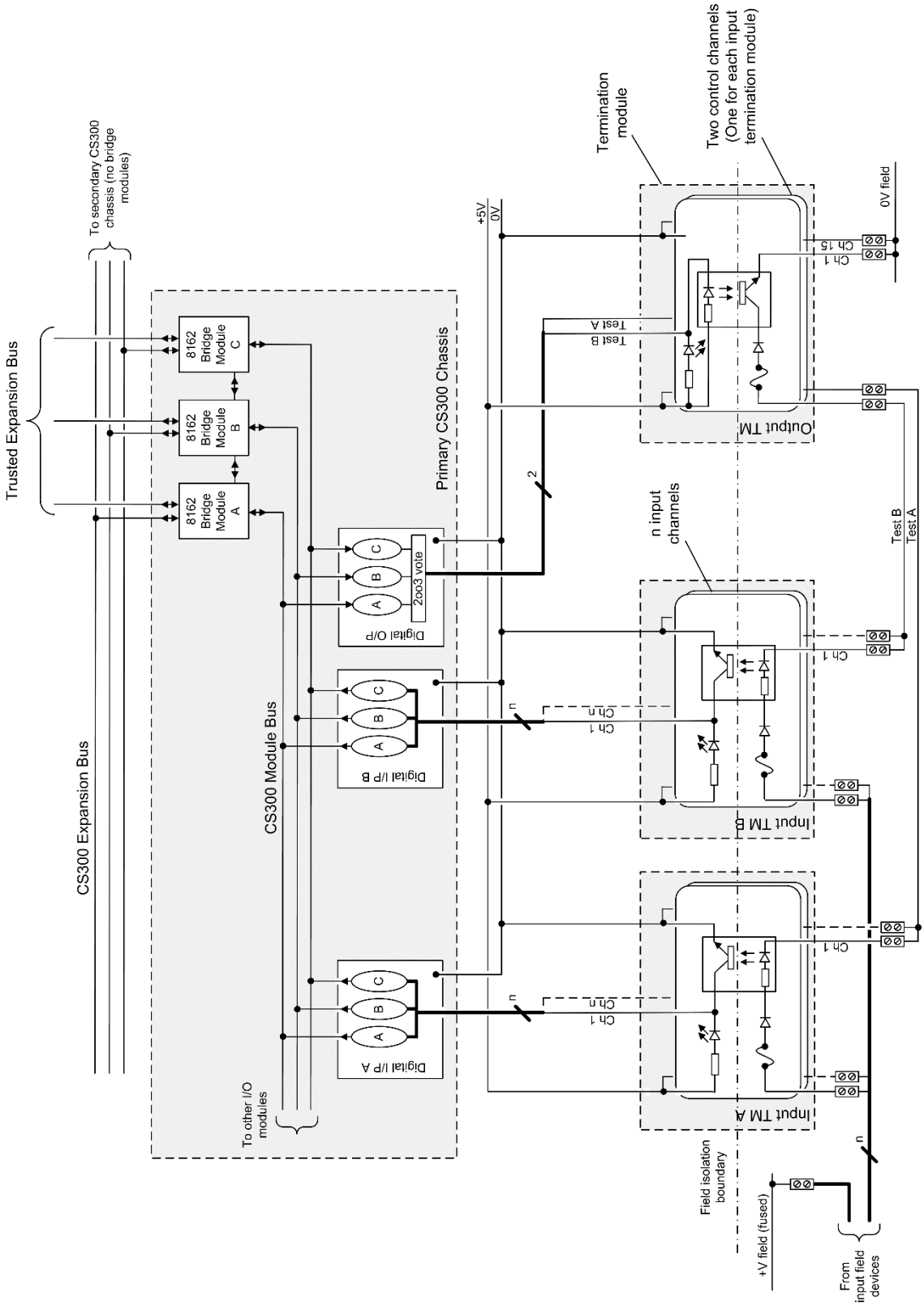


Figure 12: Wiring for CS300 duplex digital input modules

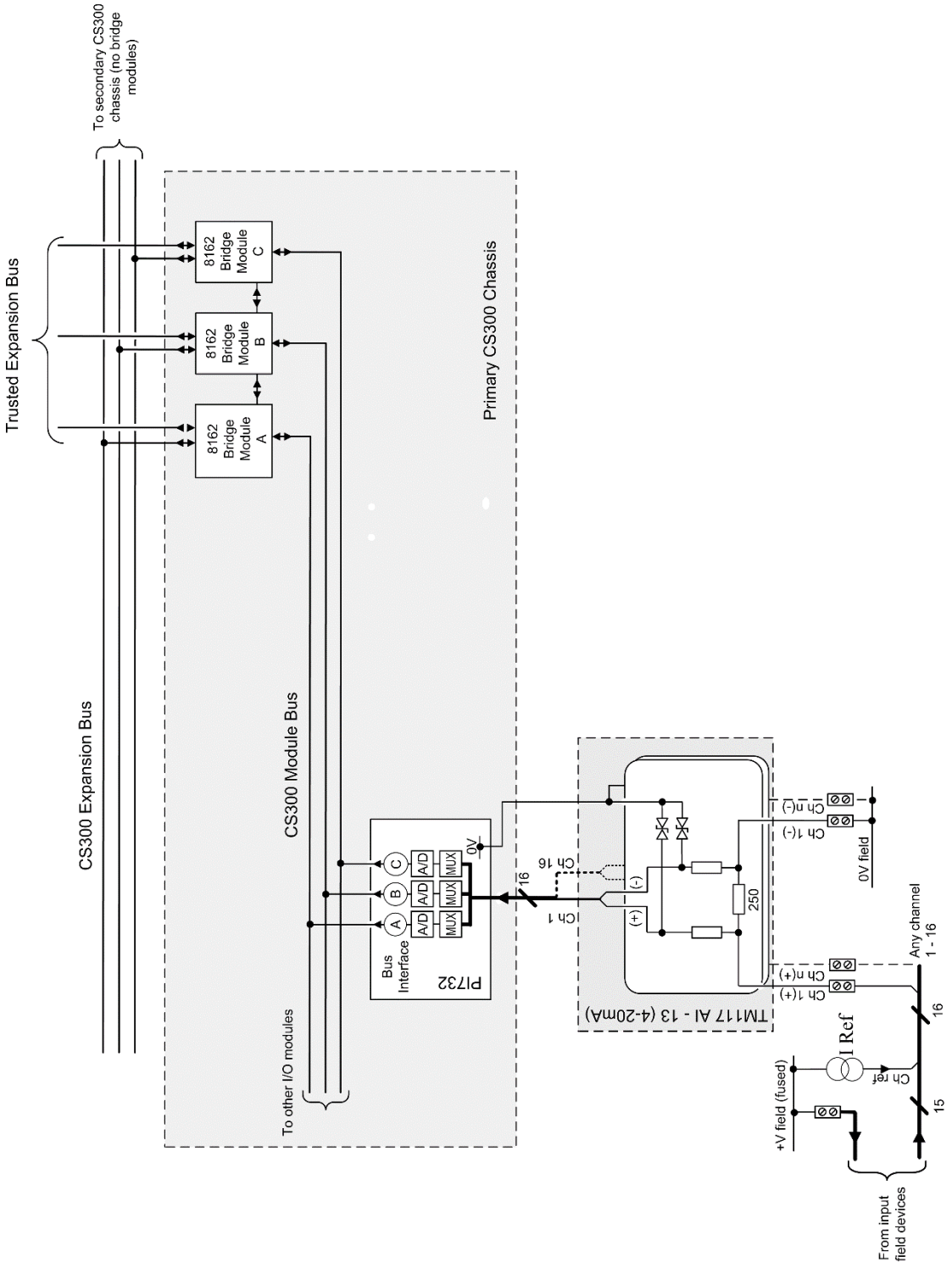


Figure 13: Wiring for CS300 analog inputs

PI-626/PI-726 digital output board

The PI-626/PI-726 voted digital output board receives inputs from each of the 8162 CS300 Bridge Modules, votes on the inputs, and produces one voted output per channel.

When the digital output board is used for safety-related applications, it must be arranged as shown in *Figure 14: Wiring for CS300 digital outputs*.

PI-627/727 digital output board

The PI-627/727 voted digital output board provides 32 voted output lines.

When the digital output board is used for safety-related applications, it must be configured for 3-2-0 degradation and arranged as shown in *Figure 14: Wiring for CS300 digital outputs*. The output board 3-2-1 function is not validated.

TM118-TWD watchdog module

The migrated system must use the TM118-TWD watchdog module to put digital outputs into a known safe state if the application stops, for example if more than one 8162 CS300 Bridge Module fails.

The migrated system must pulse the outputs to the TM118-TWD watchdog module at intervals of no more than five seconds. An interval of one second is recommended.

The five second period between system failure and the watchdog module trip must be accounted for in the overall process safety time. Refer to the information in Process Safety Time (PST) on page 15 for details about PST.

The watchdog may be patted as fast as the application scan rate will allow an output to be toggled; i.e. two application scan periods.

Note: The use of three separate digital output modules for the three signals is recommended. Refer to *Figure 14: Wiring for CS300 digital outputs*.

The state of the watchdog must be monitored and, if the watchdog goes to the tripped state, all outputs associated with the watchdog must be latched to the tripped condition until a manual reset is applied.

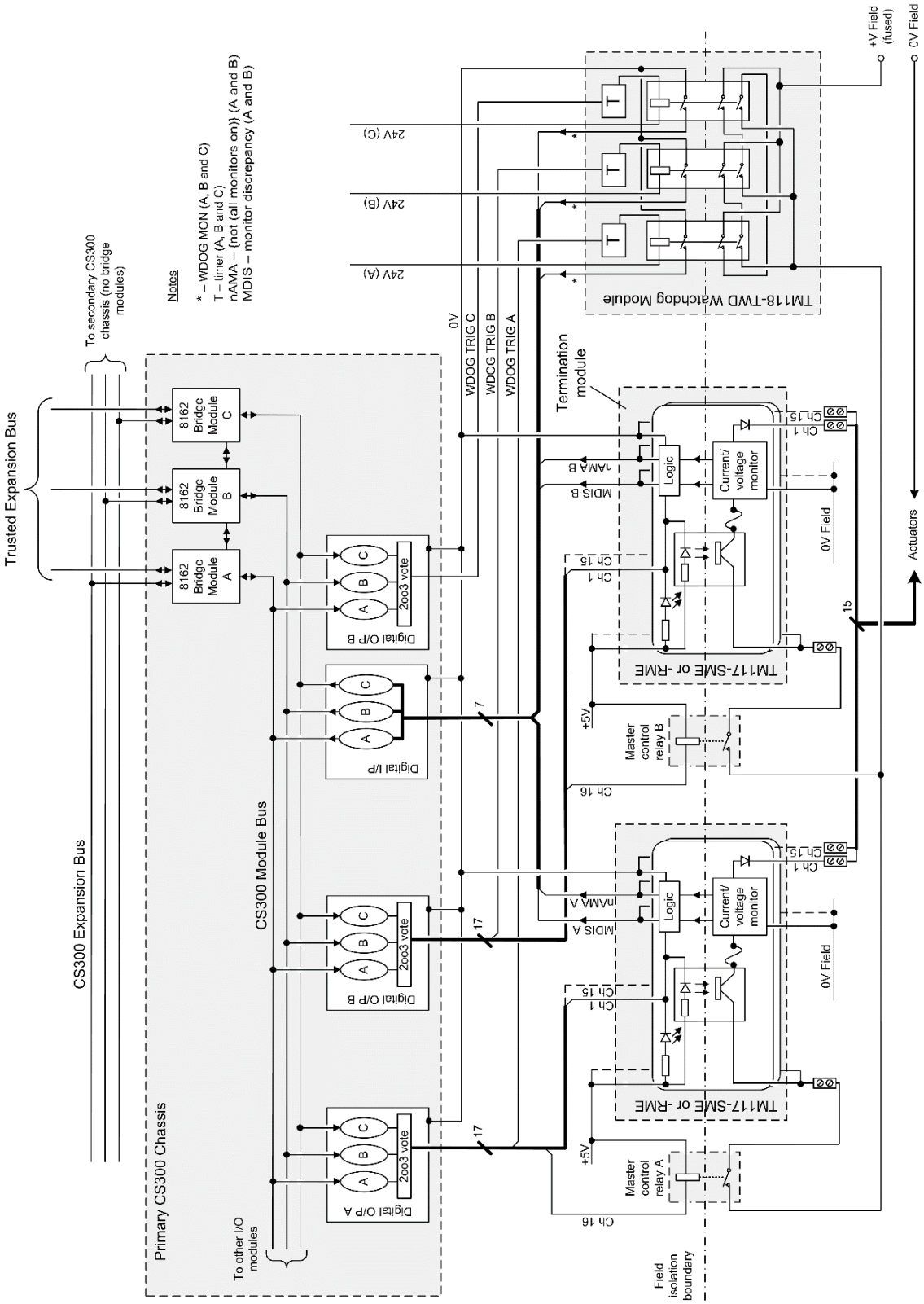


Figure 14: Wiring for CS300 digital outputs

Site planning and installation design

This section provides information about site planning and installation design.

Operational environment

Make sure that the intended operational environment meets the published specifications for the Trusted TMR System, including the 8162 CS300 Bridge Module.

The temperature of the CS300 equipment enclosure must be monitored by at least two temperature sensors and an alarm created if the panel exceeds the designed maximum operating temperature. If appropriate, forced air cooling can be applied to lower the usual operating temperature.

Installation design

The installation of the CS300 equipment and the TC 322-02 Trusted Expansion Interface Cable must comply with all of the installation requirements for Trusted. Refer to Physical Installation Design on page 75.

Planning the migration

IEC 61508-1:2010, and includes the following tasks:

- The migration activities must be planned to make sure that the functional safety for the legacy CS300 safety-related system is appropriate, both during and after the migration. This objective applies to the equipment under control as well as to the CS300 and Trusted TMR Systems.
- The migration must be preceded by a request for modification or retrofit under the local procedures for the management of functional safety.
- A migration plan must be created, approved, and implemented.
- The plan must begin by finding the boundary of the equipment under control and the control system, and then specifying the scope of the hazard and risk analysis (for example, process hazards and environmental hazards).
- The migration plan will then follow the safety lifecycle.

The success of the migration will be measured by the achievement of the required functional safety for the safety-related systems, both during and after the modification and retrofit phase, and by chronological documentation of the operation, repair, and maintenance of the safety-related systems.

The CS300 system must be taken offline to perform the migration. Before doing this, the process must be safely shut down and the plant brought to a safe/neutral state.

Replicating the application

This section provides information about replicating the application.

Prerequisites

Obtain the ‘as operational’ data for the existing system. This will usually consist of the ‘as built’ drawings, updated to include the details of all subsequent on-site modifications and upgrades.

Make sure that you have application backups that are representative of the running system. In particular, the system configuration files and application logic in the backups must be identical to the files in use in the original system at the time of the upgrade.

Choosing application logic

The Trusted TMR System supports Ladder Logic, and because CS300 only supports this language you must use Ladder Logic for the new application. This will minimize the changes and training requirements for existing users.

Detecting and handling faults

The processor in the Trusted TMR System provides comprehensive diagnostic coverage for the detection of faults up to and including the 8162 CS300 Bridge Modules.

In the legacy system, the diagnostic coverage of the CS300 I/O modules and their termination modules relied on the use of special configurations of modules, and the execution of line tests that were built into the ICCBs. The tests tried to stimulate the input and output paths while looking for faults, and used this method to find and isolate faulted hardware modules. The migrated application must include suitable function blocks that replicate these line tests. The function blocks are supplied by Rockwell Automation. The migrated application can then mimic the behavior of the original.

The system uses standard CS300 digital output channels to 'pat' (refresh) the watchdog timer in the TM118-TWD watchdog module. Outputs that are used for safety instrumented functions are programmed to go to a safe state when the watchdog times out. This mechanism caters for those faults, such as the failure of two Bridge Modules, which cause a loss of control of output modules.

Using the Autotest Management Function Block

The original ICCBs had dedicated instructions to do the self-test of the CS300 I/O modules and termination modules. In the migrated system, the behavior of these instructions must be recreated by the migrated application.

The SIS Workstation Software or Trusted Toolset Suite includes a set of ready-made function blocks that you must use to test all of the CS300 inputs and outputs used for safety instrumented functions. These function blocks are collectively known as the Autotest Management Function Blocks. 'Auto' means 'self', and so 'Autotest' describes a series of self-tests. The function blocks run their tests at defined times, each day. The tests help to make sure that, if a demand occurs, the system can respond to the demand.

This section explains how to use the function blocks in the migrated application.

You must include the Autotest functions in the migrated application – they are not a routine built into the controller.

Function block library

The function blocks are supplied as a library that accompanies the installation of the 8162 CS300 Bridge Module. This is typically an install disc supplied with the Trusted Toolset Suite and is included in the SIS Workstation Software.

The migrated application must use the library for all safety-related I/O points, for the following reasons:

- The library gives a constant style of implementation of the Autotest functions across different systems. This is easier to validate than project-specific implementations.
- The library performs the Autotests correctly.
- The library reduces application complexity.

Hardware arrangements

The Autotest of the I/O works at the application level and uses dedicated input and output ports to stimulate and monitor I/O behavior. The Autotest functions work with the arrangements of additional input and output ports shown in figures C2 through C5. These input and output ports are standard I/O, and appear to the application in the same way as the I/O being tested. The logic convention applied at the application interface uses logic '1' to show the energized field state.

Quick reference guide

There are seven function blocks, as shown in Table C-3.

Table C-3 Function Blocks

Term	Meaning or origin	Remarks
ITSTM	input test manager	controls the scheduling of diagnostic tests for digital input modules, including sequencing the test relays A and B for the termination assemblies
DIPT	digital input (point test)	tests digital inputs: decodes the DIM output from the ITSTM and decides if a fault exists (one DIPT for each digital input channel)
OTSTM	output test manager	controls the scheduling and sequencing of diagnostic tests for digital output modules
RMET	RME test	tests each of the two slices of a dual digital output (one RMET for each digital output module)
LFLT	line fault line test	looks for failures in field wiring for an analog input
PACK16[4]	pack 16 bits	packs 16 Boolean variables to one integer
UNPACK16	unpack 16 bits	unpacks one integer to 16 Boolean variables

Table C-4 Summary of Function Block Parameters

Term	Meaning or origin	Type	Remarks
AB	abort test	Boolean	abort all tests that are running
AMOA	all monitors on A	Boolean	output from termination assembly A to RMET
AMOB	all monitors on B	Boolean	output from termination assembly B to RMET

[4] PACK16 has only one output, and is strictly a function, not a function block.The parameters of the function blocks are summarized in Table C-4. Some parameters are used by more than one function block, for example to send data from one block to another. Also, many configuration parameters for ITSTM and OTSTM are the same.

Table C-4 Summary of Function Block Parameters

Term	Meaning or origin	Type	Remarks
BITn	binary digit (n)	Boolean	inputs 1 to 16 to PACK; and outputs 1 to 16 from UNPACK
COUNT	counter	analog	quantity of completed test cycles
CMD	command	analog	encoded outputs from application to RMET
DIC	digital input configuration	Boolean	configures the ITSTM to test simplex or dual-input modules
DIM	digital input mode	analog	coded output from ITSTM to DIPT
DOM	digital output mode	analog	coded output from OTSTM to RMET
FLTA	fault A	Boolean	output from DIPT or RMET, meaning channel fault on slice A
FLTB	fault B	Boolean	output from DIPT or RMET, meaning channel fault on slice B
FRQ	frequency	analog	the frequency of scheduled tests
HR	hour (current time)	analog	the hour part of the current time of day, usually taken from the real-time clock of the Trusted TMR controller
IP	process input	analog	output from termination assembly for an analog input to LFLT
IPA	input A	Boolean	output from termination assembly for digital input slice to DIPT
IPB	input B	Boolean	output from termination assembly for digital input slice to DIPT
IPV	input verification	Boolean	output from DIPT
LF	line fault	Boolean	output from LFLT to application
MDA	monitor discrepancy A	Boolean	output from termination assembly A to RMET
MDB	monitor discrepancy B	Boolean	output from termination assembly B to RMET
MTS	manual test start	Boolean	input used to start a test sequence
OC	open circuit	Boolean	output from LFLT to application
OCTHR	open circuit threshold	analog	input configuration parameter to LFLT
OPA	output A	analog	coded output from RMET to control relay A, see also PCK16
OPB	output B	analog	coded output from RMET to control relay B, see also PCK16
PCK16	packing of 16 bits	analog	coded output from RMET to UNPACK16
PACK16	packing of 16 bits	analog	coded output from PACK16 to RMET
RAT	request Autotest	Boolean	output from DIPT to application
RST	reset	Boolean	input, resets the latched Autotest faults
SC	short circuit	Boolean	output from LFLT to application
SCTHR	short circuit threshold	analog	parameter to configure high threshold of LFLT
STM	start time	analog	the hour of the time of day when the first test starts
TA	test active	Boolean	shows when any test sequence is active
TRA	test relay A	Boolean	output, controls the Autotest relay A
TRB	test relay B	Boolean	output, controls the Autotest relay B

Choosing and using function blocks

This section provides information about choosing and using function blocks.

General instructions

This section provides information about general instructions.

1. The function blocks are supplied by Rockwell Automation. You must use the function blocks as supplied as they are not accessible and cannot be changed.
2. The migrated application must annunciate fault detection status. This will enable faulty hardware to be replaced within the mean time to repair used for the module PFD calculation.
3. The function blocks do not find some invalid configuration parameters, such as some enumerations out of range. You must make sure that your application sends satisfactory configuration data to the function blocks.
4. After the state of an output changes, the Trusted TMR controller must wait for a suitable settling time before reading the input associated with monitoring the same output. To do this, the migrated application must use triggered application cycles with an interval equal to or greater than the required settling time.
5. You must disable the Trusted latent fault detection (LFD) feature for outputs connected through the CS300 equipment. This will help prevent spurious Trusted fault reports.
6. You must do an analysis of the safety instrumented functions to find out how frequently Autotests must run. Then configure the function blocks to do the tests when they are necessary.
7. The migrated application must have a mechanism to schedule the test sequences at a user-definable time of day and rate.
8. When the function blocks find a fault, they latch (hold) it. The migrated application must have a mechanism to let the user reset the records of latched faults after a fault is removed. The mechanism can reset faults individually, or reset multiple faults with one action.
9. The replacement of CS300 I/O modules must be done only when the test sequences are not running. The migrated application must provide a suitable indication so that maintenance operators know when they can replace a module.
10. Verify the impact of termination module diagnostic tests upon process safety time. The period required to complete a diagnostic test shall be less than or equal to four Trusted TMR processor application cycles.

Testing digital inputs

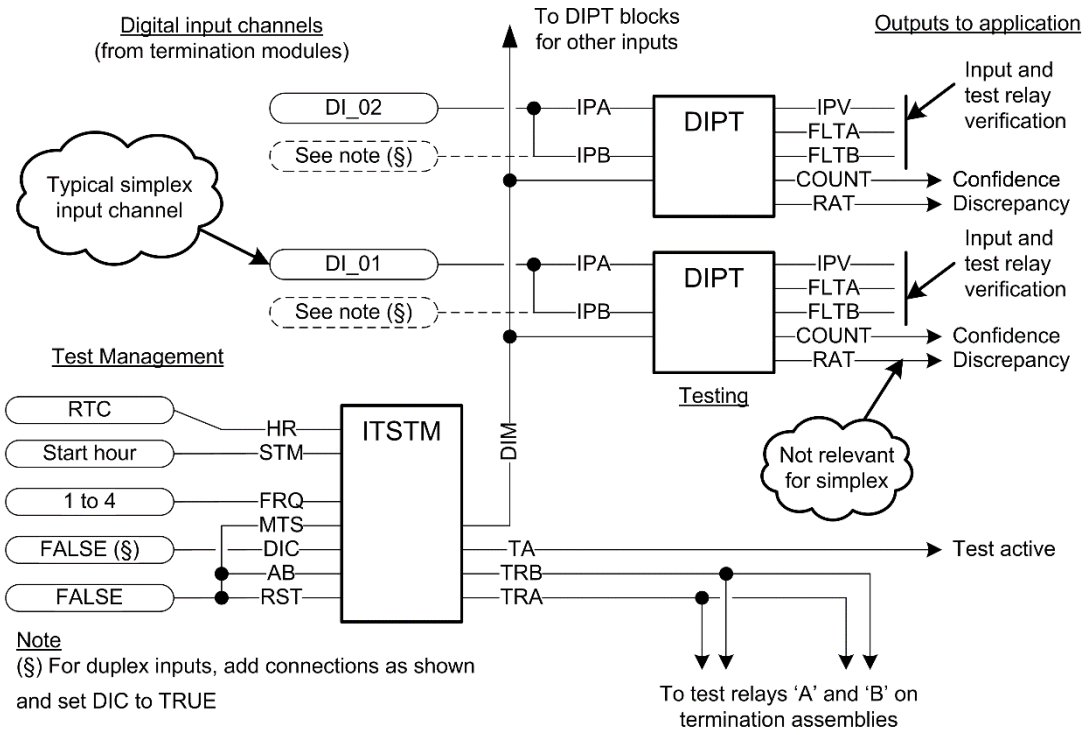


Figure 15: Testing Wiring for digital inputs

If a safety integrated function (SIF) relies on one or more CS300 digital inputs, you must use the function blocks to do tests on the inputs for stuck on / stuck off conditions. You will use at least one ITSTM function block, to schedule the tests for the inputs, and several DIPT function blocks – one DIPT for each digital input as shown in Figure C-7.

The DIPT does tests on simplex input channels or duplex input channels, but not both at the same time. If it is necessary to do tests on simplex and duplex input channels in the same system, you must use at least two sets of DIPT function blocks – one for simplex (as illustrated above) and one for duplex (as shown by the dotted lines above).

The ITSTM supports one method of operation (simplex or duplex) and one test schedule and so, if all the input channels are simplex or duplex (but not a mixture of the two), and it is applicable to do tests on all of the inputs at the same time, the application can use only one ITSTM to manage all of the tests. In other circumstances, do the following:

- If it is necessary to do tests on different inputs at different times, you have to use multiple ITSTMs.
- If there is a mixture of simplex and duplex input channels, you have to use multiple ITSTMs.
- When you use multiple ITSTMs, divide the DIPTs into groups and connect each group to its own ITSTM. Then configure each ITSM to the applicable schedule.

The DIPT has a RAT (request Autotest) output, which it sets to TRUE if the inputs of a duplex module have been inconsistent for more than one application cycle. When this happens, a test is necessary to find out which half of the duplex input has a fault. The application must respond to the RAT output by starting a test of the input modules to find a solution to the discrepancy.

Note: During a test, the DIPT input verification (IPV) output will freeze. An Autotest will not cause a trip.

Testing analog inputs

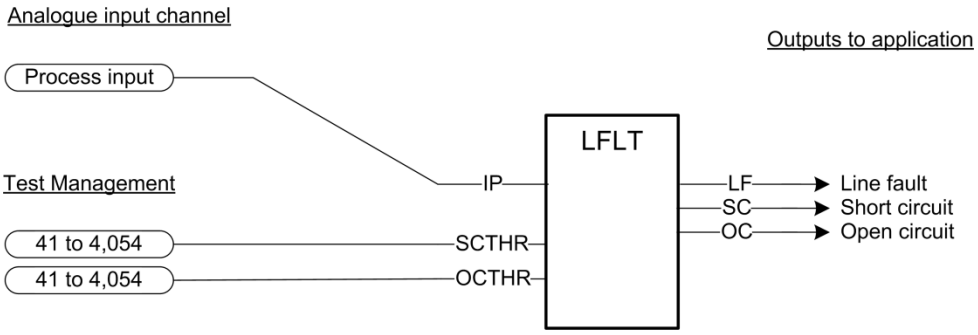


Figure 16: Testing Circuit for analog inputs

If a safety instrumented function (SIF) relies on one or more CS300 analog inputs, you must use the function blocks to do tests on the inputs for open circuit and short circuit conditions. You will use one LFLT for each analog input. The LFLT uses the unscaled process input value taken directly from its PI-732 channel as shown in *Figure 16: Testing Circuit for analog inputs*.

The LFLT tests are not scheduled. The LFLT constantly monitors its analog input channel (IP) for a deviation that takes the value above the short circuit threshold or below the open circuit threshold.

- The Trusted TMR Processor constantly monitors the analog data input from the CS300 slices. When a discrepancy greater than 1% is detected between two slices, a fault is declared. The migrated application must report the fault to the operator so that the defective module can be replaced within the mean time to repair used in the PFD calculation for the module.
- An analog input is valid when the values from the three slices are closer than a count of 41 – this represents 1% of the maximum count, 4,095. The analog input cannot distinguish between values greater than 4,095 or less than 0, and so the usable range for inputs is from 41 to 4,054.
- The lower (open circuit) threshold (OCTHR) and the higher (short circuit) threshold (SCTHR) must be in the range 41 to 4054 inclusive. If the application sets either threshold to a value outside this range, the LFLT uses its limit value (41 or 4,054) not the requested value.

- These limits apply to all analog input modules and all configurations of termination module.

The application must use calibration drift monitoring for analog inputs:

- One of the 16 channels on each analog input card must be wired to a known calibration source and a diagnostic ladder used to monitor for drift and to provide the alarm.
- The calibration reference must be chosen to reflect the highest level for which the input module is intended to read.
- The calibration reference channel must also be monitored through an LFLT function block.

Testing digital outputs

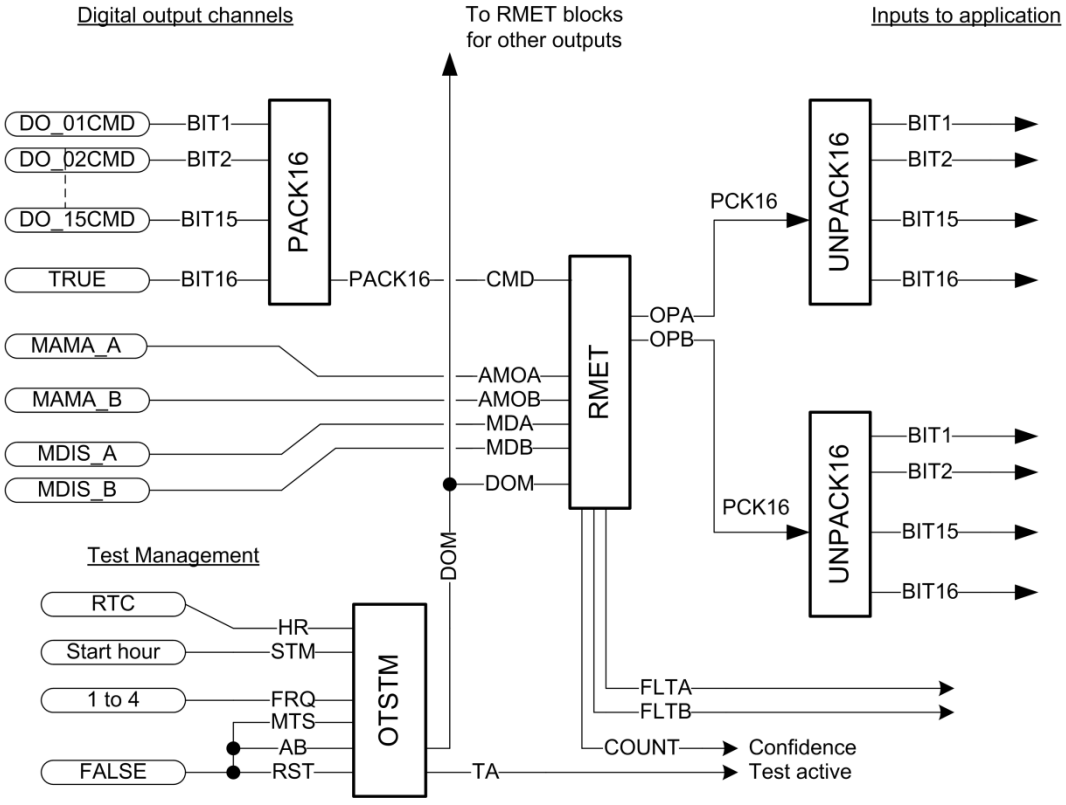


Figure 17: Testing Circuits for digital outputs

If a safety integrated function (SIF) relies on one or more CS300 digital outputs, you must use the function blocks to do tests on the outputs for stuck on / stuck off conditions. You will use at least one OTSTM function block, to schedule the tests for the outputs, and one or more RMET function blocks – one RMET for each output module as shown in *Figure 17: Testing Circuits for digital outputs*.

You must disable the Trusted latent fault detection (LFD) feature for outputs connected through the CS300 equipment. This will help prevent spurious Trusted fault reports.

A digital output used for a SIF always uses two (duplex) digital output modules. The function blocks look for discrepancies between the outputs from the two modules.

Although the Digital Output module has 32 channels, its associated TM117-RME/SME termination module has only 16 channels. The 16th channel (bit 16 in the illustration) represents the master control relay for each slice and must be set true leaving 15 channels available as field outputs.

Output testing must occur only when all 15 channels in the group are commanded on.

The LED indication on TM117-RME/SME shows the commanded state and not the physical state.

The rules for Structured Text put a limit on the quantity of inputs and outputs on a function block. This limit would stop one function block receiving or transmitting all 16 channels as well as its control parameters. To help prevent this problem, the solution uses two more function blocks, PACK16 and UNPACK16, to put the 16 output channels into one integer. This lets one RMET examine all 16 output channels of a digital output module.

The OTSTM supports one test schedule, so it is sufficient to use one OTSTM if it is applicable to do a test on all of the digital outputs at the same time. If it is necessary to do tests on different outputs at different times, you have to use multiple OTSTMs. Divide the output modules into groups and connect each group to its own OTSTM, and set up each OTSM to the applicable schedule.

Scheduling, running, and aborting tests

You can configure each ITSTM and OTSTM to do its tests 1, 2, 3 or 4 times in a 24 hours period. To do this, set STM to the hour of the time of day for the first test, and FRQ to the quantity of tests required (1 to 4). Also connect HR to the hour part of a real-time clock – this is usually the built-in real-time clock in the Trusted TMR System.

When the application tests digital inputs (using the DIPT function block) the application will react to changes in digital inputs up to eight cycles later than usual. When the application tests digital outputs, the RMET function block does not introduce delays into changes made to output states.

The application must include a mechanism to make sure that the function blocks are being executed. To do this, the application must inspect the COUNT outputs from the ITSTM and OTSTM.

You can also start a test manually from the application. To do this, set manual test start (MTS) to TRUE (positive logic convention). If there is no scheduled test running, the manual test starts straight away. If there is a test running when you set MTS to TRUE, there will be a delay of one full application cycle between the end of the scheduled test and the start of the manual test.

The AB (abort) command is a mechanism to stop tests that are running. The application can use the AB command to stop a time-consuming test that is running. The controller always actions a shutdown demand, even when a test is running.

Responding to outputs from function blocks

The application must react to the outputs of the function blocks in an applicable way. The response will include one or more of the following:

- If the DIPT issues a RAT (request Autotest), the application must start a test of the input modules to find out which half of the duplex input has a fault. To do this, connect the RAT output of the DIPT function block to the MTS input of the ITSM function block.
- If the ITSTM or OTSTM gives an FLT (fault) output, the application must annunciate the fault so that repair action can be taken. If necessary, the application must also start an applicable action to protect the safety system.

There are more details of responses in Parameter Specifications on page 122.

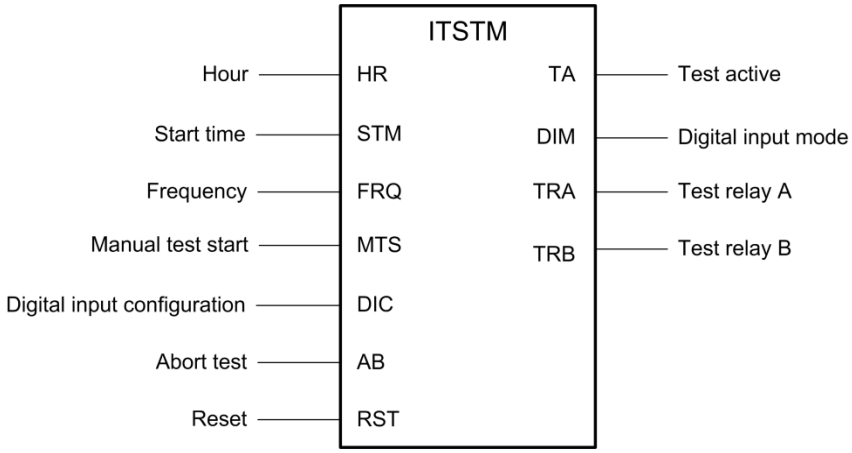
Commissioning a system and repairing faults

The ITSTM and OTSTM each have an MTS (manual test start) command. The MTS is useful during commissioning, to make sure that a test is fully operational, and after repairing a fault, to make sure that the repair is satisfactory. You can use the AB (abort) command to stop a manual test immediately, to finish the verification.

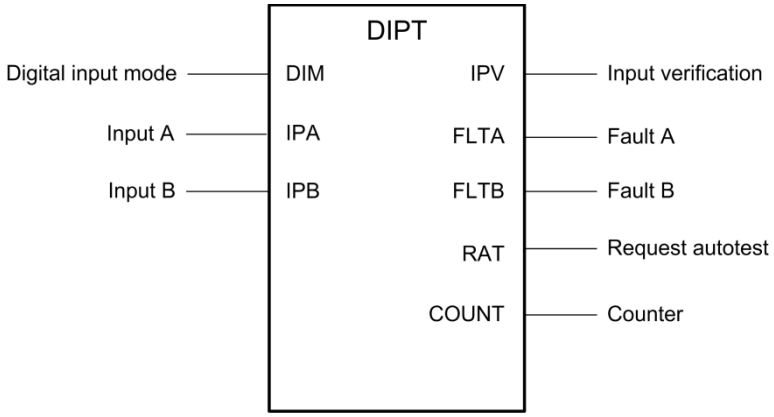
Function block specifications

This section provides information about function block specifications.

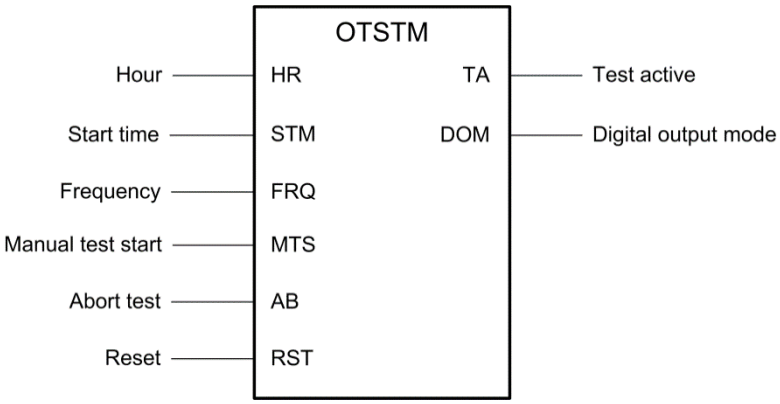
ITSTM – Input Test Manager



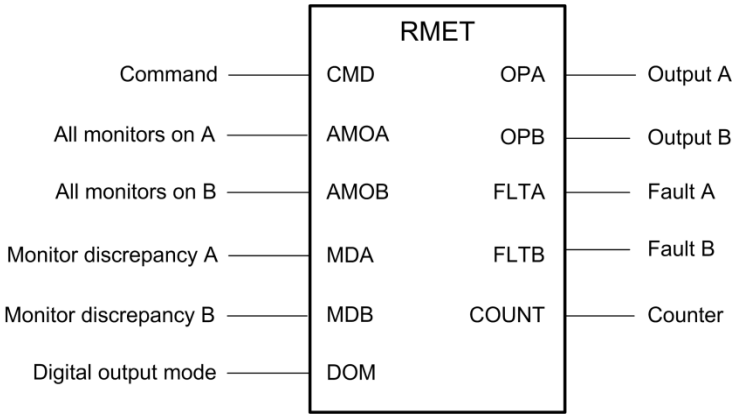
DIPT – Digital Input Point Test



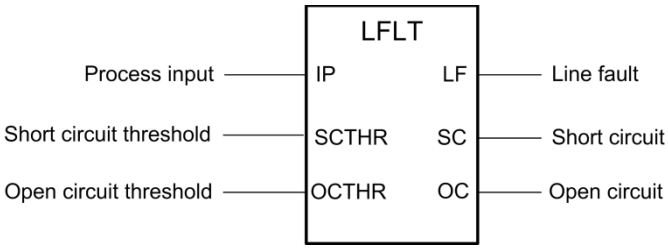
OTSTM - Output Test Manager



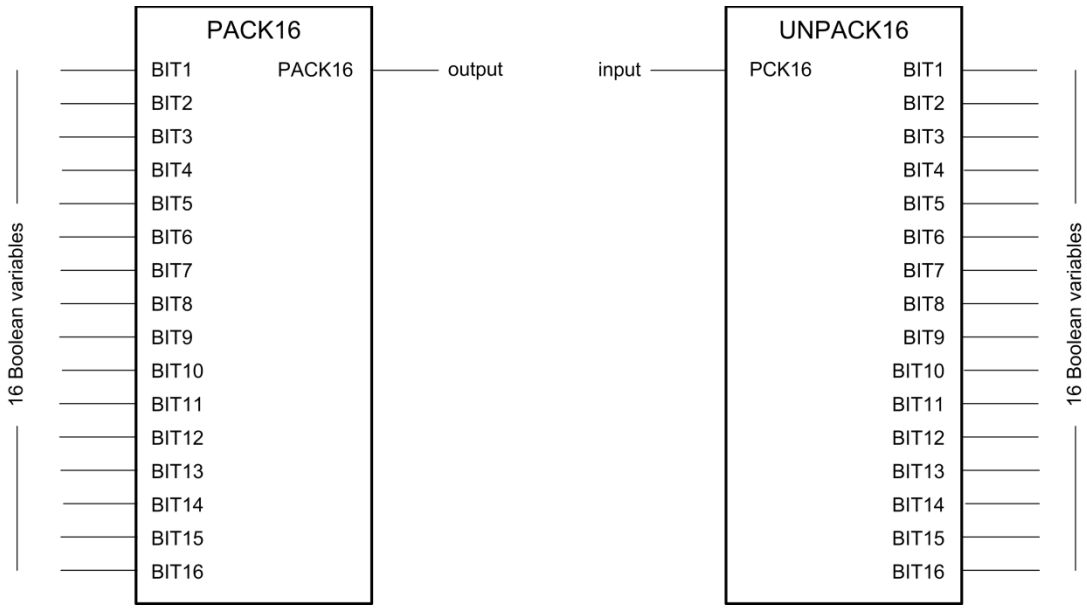
RMET – RME Test



LFLT - Line Fault Line Test



PACK16 and UNPACK16 – Pack and Unpack 16 bits



Parameter Specifications

This section provides information about parameter specifications.

AB, abort

Purpose	The AB (abort) control input lets the user application cancel the execution of an on-going sequence of tests.
Data type	Boolean
Direction	From user application to ITSTM From user application to OTSTM
Values	TRUE FALSE Default: FALSE
Notes	The AB input is edge triggered. On a rising edge, any test in progress is aborted.

AMOA / AMOB, all module outputs A / B

Purpose	The AMO (all monitors on) inputs to the RMET are used by the test procedure in the RMET.
Data type	Boolean
Direction	From user application to RMET
Values	TRUE: all the channels on the slice are on FALSE: one or more channels on the slice are off
Notes	Connect AMOA and AMOB to the A and B slices of the TM117-RME/SME monitored output termination module.

COUNT, counter

Purpose	The COUNT outputs from the RMET and DIPT are records of the quantity of completed tests done by their function blocks. COUNT is set to zero on an RST (reset) command.
Data type	analog
Direction	From RMET to user application From DIPT to user application
Values	0 to 65,535
Notes	The COUNT outputs are confidence outputs. The application can examine them to make sure that tests are actually being done.

CMD, command

Purpose	The CMD input to the RMET represents the commanded output states from the application. It is not for direct use by the user application.
Data type	analog
Direction	From PACK16 to RMET
Values	0 to 65,535 (bit-packed integer)

DIC, digital input configuration

Purpose	The DIC control input lets the user application configure the ITSTM to work with simplex and duplex digital input modules
Data type	Boolean
Direction	From application to ITSTM
Values	TRUE - dual DI module FALSE - single DI module
Notes	The application must set DIC to the applicable value

DIM, digital input mode

Purpose	The DIM (digital input mode) is an encoded output from the ITSTM to each DIPT. It is not for direct use by the user application.
Data type	analog
Direction	From ITSTM to each DIPT
Values	not specified

DOM, digital output mode

Purpose	The DOM (digital output mode) is an encoded output from the OTSTM to each RMET. It is not for direct use by the user application.
Data type	analog
Direction	From OTSTM to each RMET
Values	not specified

FLTA / FLTB, fault A / B

Purpose	The FLT (fault) outputs let the DIPT and RMET tell the application when there is a fault on slice A or slice B of a duplex input (DIPT) or output (RMET) channel
Data type	Boolean
Direction	From ITSTM to user application From OTSTM to user application
Values	TRUE – there is a fault on the applicable slice Otherwise FALSE
Notes	The FLT outputs from the DIPT are latched until a reset command is received from the related ITSTM.

FRQ, frequency

Purpose	The FRQ (frequency) input sets the quantity of times the ITSTM or OTSTM will start its test sequences in a time of 24 hours.
Data type	analog
Direction	From application to ITSTM or OTSTM
Values	1, 2, 3 or 4
Notes	A value less that 1 is treated as 1, and a value larger than 4 is treated as 4.

HR, hour

Purpose	The HR (hour) parameter is used by the ITSTM and OTSTM to control their scheduled testing.
Data type	analog
Direction	From controller RTC to ITSTM and OTSTM
Values	0 to 23
Notes	The HR input is usually connected to the Trusted TMR controller's real-time clock.

IP, process input

Purpose	The IP (process input) parameter carries the value from a PI-732 analog input channel as a raw unscaled integer
Data type	analog
Direction	From application to LFLT
Values	0 to 65,535

IPA / IPB, input A / B

Purpose	The IPA and IPB parameters carry the measured input for the channel for their slices.
Data type	Boolean
Direction	From application to DIPT
Values	TRUE – input channel high FALSE – input channel low
Notes	For a simplex input module, connect IPB to the same point as IPA.

IPV, input verification

Purpose	The IPV (input verification) output represents the field input of the channel.
Data type	Boolean
Direction	From DIPT to application
Values	TRUE – input channel (voted) high FALSE – input channel (voted) low
Notes	IPV is the voted input state to be used by the application.

LF, line fault

Purpose	The LF (line fault) output is a logical OR of the SC and OC outputs from the LFLT
Data type	Boolean
Direction	From LFLT to application

LF, line fault

Purpose	The LF (line fault) output is a logical OR of the SC and OC outputs from the LFLT
Values	TRUE - either SC or OC (or both) is TRUE FALSE – SC and OC are FALSE

MDA / MDB, monitor discrepancy

Purpose	The MDA and MDB (monitor discrepancy) parameters show when there is a discrepancy.
Data type	Boolean
Direction	From application to RMET
Values	FALSE – a discrepancy exists between the commanded and actual states of one of more output channels in a TM117-RME/SME termination module Otherwise TRUE
Notes	Connect MDA and MDB to the A and B slices of the TM117-RME/SME monitored output termination assembly.

MTS, manual test start

Purpose	The MTS (manual test start) input starts a test sequence if there is no test already in progress.
Data type	Boolean
Direction	From application to ITSTM or OTSTM
Values	TRUE FALSE
Notes	Make sure that the application returns MTS to FALSE promptly. This input parameter is level sensitive, and will cause repetitive testing (and relay chatter) if it is held TRUE.

OC, open circuit

Purpose	The OC (open circuit) output tells the application when the value of the process input is less than the OCTHR
Data type	Boolean
Direction	From LFLT to application
Values	TRUE – the process input is less than the OCTHR Otherwise FALSE

OCTHR, open circuit threshold

Purpose	The OCTHR (open circuit threshold) determines the low (or open circuit) threshold for the analog input tested by the LFLT
Data type	analog
Direction	From application to LFLT
Values	41 to 4,054

OPA / OPB, output A / B

Purpose	The OPA and OPB outputs control each of two TM117-RME/SME monitored output termination module output slices. OPA and OPB are not for direct use by the user application.
Data type	analog
Direction	From RMET to UNPACK16
Values	0 to 65,535 (bit-packed integer)

PACK16, a packing of 16 bits

Purpose	PACK16 carries 15 digital output channels and a test channel. It is not for direct use by the user application.
Data type	analog
Direction	PACK16 to RMET
Values	0 to 65,535 (bit-packed integer)

PCK16, a packing of 16 bits

Purpose	PACK16 carries 15 digital output channels and a test channel. It is not for direct use by the user application.
Data type	analog
Direction	RMET to UNPACK16
Values	0 to 65,535 (bit-packed integer)

RAT, request Autotest

Purpose	The RAT (request Autotest) output tells the application when there is a discrepancy between duplex digital inputs.
Data type	Boolean
Direction	From DIPT to application
Values	TRUE – the inputs to a duplex input module have been inconsistent for more than one application cycle when a test is not in progress Otherwise FALSE
Notes	The application must respond to RAT by using it to start a test of the input modules to find out which half of the duplex input is faulty, and find a solution to the discrepancy.

RST, reset

Purpose	The RST (reset) parameter removes all latched fault states in its ITSTM or OTSTM.
Data type	Boolean
Direction	From application to ITSTM From application to OTSTM
Values	TRUE FALSE Default: FALSE
Notes	This input is edge triggered. On a rising edge, the latched fault states are reset.

SC, short circuit

Purpose	The SC (short circuit) output tells the application when the value of the process input is larger than the SCTHR
Data type	Boolean
Direction	From LFLT to application
Values	TRUE – the process input is larger than the SCTHR Otherwise FALSE

SCTHR, short circuit threshold

Purpose	The SCTHR (short circuit threshold) determines the high threshold for the analog input tested by the LFLT
Data type	analog
Direction	From application to LFLT
Values	41 to 4,054

STM, start time

Purpose	The STM (start time) parameter sets the hour value of the time of day when the ITSTM or OTSTM will start its first test sequence of the day.
Data type	analog
Direction	From application to ITSTM or OTSTM
Values	0 to 23
Notes	A value outside the range 0 to 23 is taken to be 12

TA, test active

Purpose	The TA (test active) output lets an ITSTM or OTSTM tell the application when it is managing an active test.
Data type	Boolean
Direction	From ITSTM or OTSTM to application
Values	TRUE – a test is active Otherwise FALSE

TRA / TRB, test relay A / B

Purpose	The TR (test relay) outputs let the ITSTM control the two test relays 'A' and 'B' for the input termination assemblies
Data type	Boolean
Direction	From ITSTM to application
Values	FALSE – test of applicable slice is active Otherwise TRUE

Connecting Fire & Gas and Emergency Shutdown Systems

If the legacy CS300 system is for a fire and gas detection and protection application and it provides hardwired shutdown command signals to a complementary Emergency ShutDown (ESD) system, these signals must be configured as standard ESD outputs using dual TM-117-RME termination panels and follow a 3-2-0 output configuration:

- If one 8162 CS300 Bridge Module fails, the F&G detection system will continue to run.
- If two 8162 CS300 Bridge Modules fail, the fire and gas detection system will stop running, and the outputs from the system to the ESD system will go to their default states when the relevant watchdog timers time out. It is necessary to set up these default states and the watchdog timers so that, if two 8162 CS300 Bridge Modules should fail, the operating plant is correctly and safely shutdown.

Retaining the CD901 diagnostic panel

The CD901 diagnostic panel provides an LED display of system status and common alarms. In the legacy CS300 system, it formed a first line indication of system faults.

Although the SIS Workstation Software or Trusted Toolset Suite provides an indication of system faults, it may be worthwhile to retain the diagnostic panel to reduce the amount of operator retraining needed for the migrated system. If the panel is retained, provide suitable support for it in the migrated application.

TM117-DMX Matrix Driver Interface Module

The TM117-DMX matrix LED driver interface module is used for fault annunciation in some CS300 systems.

If the migrated system retains the TM117-DMX module, the system must use the external serial ports on the Trusted TMR Processor to drive the module. The migrated application will use an I/O board interface (implemented by the I/O driver software of the Trusted TMR Processor) to control the serial ports.

Making printouts of alarm and diagnostic data

The legacy CS300 controller firmware can create and print reports and events. The Trusted TMR System has no equivalent facility (and indeed has no printer output) but it does have two event logs.

- The T8110 TMR Processor maintains and holds an event log, which automatically records all system faults and actions. This log includes module faults and swaps, program downloads, and presses of the Reset button.
- The system also has a Sequence of Events (SOE) log that records changes to Boolean variables. This log includes timestamps (recorded to a precision of milliseconds), but these are not absolutely accurate due to the disconnection between the Trusted application and the CS300 I/O in the migrated system.

To make printouts of alarm and diagnostic data, open the appropriate logs files in a word processor or other text editor, and print them.

Preparing for entry into service

The application must be 100% tested against the functionality of the original application before the migrated system is placed into service.

Maintaining the migrated system

Maintenance schedule

This section provides information about maintaining the migrated system.

The requirements for the manual test intervals for the Trusted modules (including the 8162 CS300 Bridge Module) are written in PFH and PFDavg Data for Trusted TMR System, publication ICSTT-TD002. In addition, the following minimum requirements apply:

- The maintenance schedule for the migrated system must include a test of the TM118-TWD watchdog module at least one time every year.

Completion

After the migration is completed, return the ICCB modules and other unused CS300 parts to Rockwell Automation. Do not dispose of these items locally.

Hazardous area and electrical safety information

This section provides hazardous area and electrical safety information.

Product information

This section provides details about Trusted 8000 Series: Processor, Digital/Analogue I/O & Ancillaries Product Information.

ATTENTION: Refer to Trusted 8000 Series: Processor, Digital/Analogue I/O & Ancillaries Product Information, publication ICSTT-PC002
(Doc No 554455) before you install, configure, operate or maintain Trusted 8000 Series products. 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.

Trusted processor relay connections (applicable to T8110 only)

The following relay connections applicable to T8110B legacy Trusted TMR Processor module only. The T8111 processor has replaced the mechanical relays with solid-state devices.

The Trusted Processor relay option is available for reporting the fault and failed status of the Processor subsystem. These relays are not intended for use in a Safety Function.

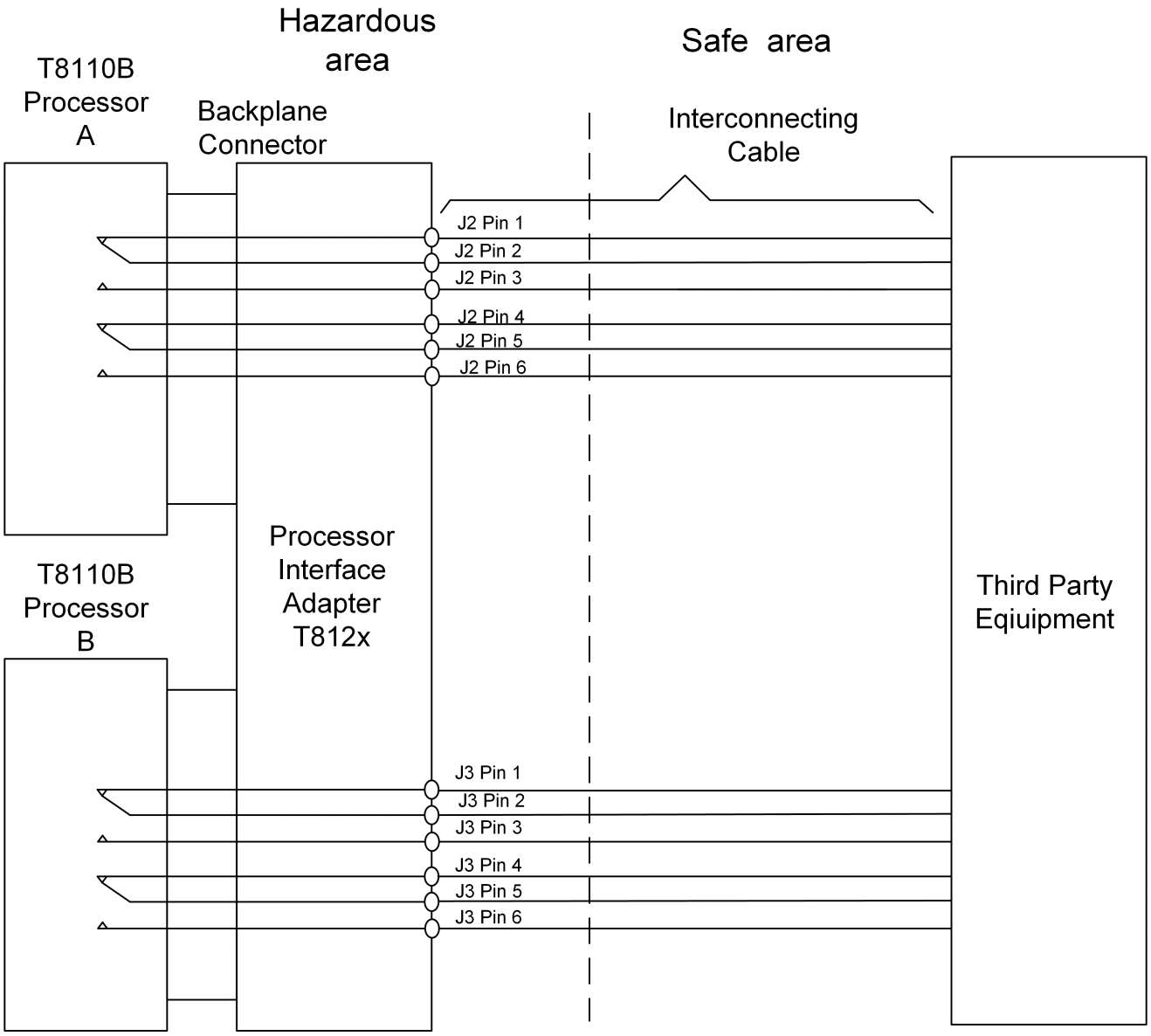


Figure 18: T8110B TMR Processor Relay Contact

Wiring Requirements

The following wiring requirements apply:

- The wiring must be installed by a competent person
- Relay contact must not be connected in parallel.
- Non-incendive field wiring circuits must be in accordance with the National Electric Code (NEC), NFPA70, Article 501.
- The non-incendive field wiring circuit concept allows interconnection of non-incendive field wiring apparatus using any of the wiring methods permitted for unclassified locations when certain parametric conditions are met.
- Capacity: Ca ≥ Ci + Ccable
- Inductivity: La ≥ Li _ Lcable
- The maximum cable length to be determined as follows:

a. Max cable length < (La-Li)/Lcable and

b. Max cable length < (Ca – Ci)/Ccable

The lower value of a) and b) is to apply.

- Lcable l: inductance per unit length of use cable
- Ccable c: capacitance per unit length of used cable.

Maximum third-party load and cable parameters:

- Ccable = 0.05 µF
- Lcable = 0.5 mH
- Um = 30V DC

Class I Div 2 Group A,B,C.D

Class I Zone 2 Group IIC

- Ci = 0.05 µF
- Li = 0.5 mH
- Um = 30V DC
- Ii = 75 mA

Glossary

Actuators

Devices that cause an action (electrical, mechanical, pneumatic, etc.) to occur when required within a plant component.

Architecture

Organizational structure of a computing system that describes the functional relationship between board level, device level and system level components.

ASCII

The American Standard Code for Information Interchange. Uses seven bits to represent 128 characters. Both upper and lower case letters, numbers, special symbols and a wide range of control codes are included.

Availability

The probability that a system will be able to perform its designated function when required for use – normally expressed as a percentage.

Asynchronous

A data communications term describing the method by which signals between computers are timed. Although the number of characters to be sent per second is undefined, the rate at which a character's bits are sent is predetermined. Each character is preceded by a start bit and terminated by a stop bit.

Backplane

A printed circuit board that provides connecting busses between the Processor and I/O modules.

Buffer

A type of memory in which information is stored temporarily during transfer from one device to another, or one process to another. Normally used to accommodate the difference in the rate or time at which the devices can handle the data.

Bus

A group of conductors that carry related data. Micro-based systems have an Address Bus, Data Bus, and a Control Bus.

Companion Slot

A spare empty slot to the right of the slot occupied by the 'active' module. The slots are inter-connected to enable the 'active' module to be replaced in the empty slot as necessary.

Communications Interface

An intelligent communications module that interfaces between a TMR Controller and an Engineering Workstation, third-party equipment or other TMR Controllers.

Controller

A Controller is the heart of any Rockwell Automation microprocessor-based system. It performs central processing of user application logic and controls the actions of input and output hardware, as well as peripheral hardware such as printers and Visual Display Units.

Discrepancy

A discrepancy exists if one or more of the elements disagree.

DRAM

Dynamic Random Access Memory. A type of volatile read/write memory where the data is stored as a short-life capacitive charge.

Element

A set of input conditioning, application processing, and output conditioning.

Engineering Workstation

Comprising rugged PC platform fitted with the SIS Workstation Software or Trusted Toolset Suite.

EPROM

Erasable Programmable Read Only Memory. A non-volatile storage medium that is electronically programmed. Strong ultra-violet light might erase the EPROM device.

EUC

Equipment Under Control. Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

Fail-Safe

The capability to go to a predetermined safe state if there is a specific malfunction.

Fault Tolerance

Built-in capability of a system to provide continued correct execution of its assigned function in the presence of a limited number of hardware and software faults.

Field Devices

Equipment connected to the field side of the I/O terminals. Such equipment includes field wiring, sensors, final control elements, and those operator interface devices hard-wired to I/O terminals.

Firmware

Special purpose memory units containing software embedded in protected memory required for the operation of programmable electronics.

Fixed Frame

An empty fixed metal surround, designed to contain 483 mm (19 ”) standard equipment.

FBD

Functional Block Diagram. A graphical IEC 61131 language for building complex procedures by taking existing Functional Blocks from the IEC 61131 library and wiring them together on the screen.

Gray Channel

A non-safety-critical communication line between two modules that are regarded as safety-critical. Communications sent across a “gray channel” are viewed as subject to errors induced by that channel, which must be detected and compensated be the safety-related receiver.

GUI

Graphical User Interface

Hot Swap

Alternative term for Companion Slot

IEC 61508

IEC 61508 is an international standard that covers functional safety, encompassing electrical, electronic and programmable electronic systems; hardware and software aspects.

IEC 61511

IEC 61511 is an international standard that covers functional safety and Safety Instrumented Systems for the process industry, encompassing electrical, electronic, and programmable electronic systems, hardware and software aspects.

IL

Instruction List. A low-level IEC 61131 language, similar to the simple textual PLC’s language.

Industrial Processor

High performance processor for use in non-safety-related applications that can be used in a simplex or dual-redundant configuration.

Input Module

Interface that converts input signals from external devices into signals that the control system can use.

I/O

Input/Output conditioning circuits (as distinct from the central processing).

I/O Driver

Essential software to allow the SIS Workstation Software or Trusted Toolset Suite to configure and program unique types of Trusted TMR System I/O interfaces.

LD

Ladder Diagram. An IEC 61131 language composed of contact symbols representing logical equations and simple actions. The main function of the ladder diagram is to control outputs based on input conditions.

HMI

Human Machine Interface. The Graphical User Interface of the Operator Workstation for making adjustments in the process, and monitoring keys, knobs, switches etc.

Modbus

An industry standard communications protocol developed by Modicon. Used to communicate with external devices such as distributed control systems (DCSs) or operator interfaces.

Module

An electronic (generally pluggable) subsystem.

MORSE

Method for Object Reuse in Safety-critical Environments. Programming and configuration software tool for the Fast Flex range of remote I/O.

Mean Time To Restoration (MTTR)

In accordance with IEC 61508 and IEC61511:

The expected time to restore functionality, taking into account time to detect the fault, time spent before the repair, the repair time, and the time taken to restore operation.

Output Module

Interface that converts output signals from the Trusted TMR Processor into signals that can actuate external devices.

Peer to Peer Communications

Allows two or more TMR Systems to communicate with each other.

PCM

PCI Mezzanine Card

Pollution Degree

An environment in accordance with IEC 61010-1:

Pollution Degree 1: No pollution or only dry pollution occurs. The pollution has no influence.

Pollution Degree 2: Only non-conductive pollution occurs except that occasionally a temporary conductivity caused by condensation is to be expected.

Pollution Degree 3: Conductive pollution occurs or dry non-conductive pollution occurs that becomes conductive due to condensation, which is to be expected.

Pollution Degree 4: Continuous conductivity occurs due to conductive dust, rain or other wet conditions.

Protocol

A set of rules governing data flow in a communication system. The protocol governs such matters as the way a message is addressed and routed, how often it is sent, how to recover from transmission errors and how much information is to be sent.

PSU

Power Supply Unit.

RAM

Random Access Memory. A volatile (unless battery backed) form of read/write memory. The time to access different locations is the same. It may be static (SRAM - data held in a flip-flop) or dynamic (DRAM – data held as a capacitive charge).

Real Time

A method of data processing in which the data is acted upon immediately instead of being accumulated and processed in batches.

Redundancy

The employment of two or more devices, each performing the same function, in order to improve reliability.

RISC

Reduced Instruction Set Computer

RS 232C, RS 422, RS 485

Standard interfaces introduced by the Energy Industries Association covering the electrical connection between data communication equipment. RS-232C is the most commonly used interface. However, RS-422 allows for high transmission rates over greatly increased distances.

RTU

Remote Telemetry Unit

Safety

Where IEC 61508 certification is a requirement, the Safety Chapter prescribes how to use the TMR system in a safety-related application.

SFC

Sequential Function Chart. A IEC 61131 language that divides the process cycle into a number of well-defined steps separated by transitions.

SIL

Safety Integrity Level. One of four possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.

SIS Workstation

AADvance®-Trusted® Safety Instrumented System Workstation Software.

Software used for configuring and programming the Trusted TMR System.

Slot

A slot is the term given to the physical allocation of a module within a 483 mm (19-inch) frame.

SmartSlot

Spare module slot position wired, and configured to enable any one of a number of modules of the same type to be 'hot' replaced as necessary (see Companion Slot).

SOE

Sequence of Events

Software (Application Software)

Software specific to the user application. Generally, it contains logic sequences, permissives, limits, expressions, etc. that control the appropriate input, output, calculations and decisions necessary to meet system safety functional requirements.

SRAM

Static Random Access Memory. A type of random access memory where the data is held in a flip flop storage device.

ST

Structured Text. A high-level IEC 61131 structured language with a syntax similar to Pascal. Used mainly to implement complex procedures that cannot be expressed easily with graphical languages.

Swing frame

An empty hinged metal surround, designed to contain 483 mm (19-inch) standard equipment.

Synchronous

A data-communication term describing the method by which signals between computers are timed. In synchronous communications, a pre-arranged number of bits is expected to be sent across a line per second. To synchronize the sending and receiving machines, a clocking signal is sent on the same line by the transmitting computer. There are no start or stop bits in synchronous communications.

TMR

Triple Modular Redundancy.

TMR Interface

An interface between the Trusted TMR Processor modules and six U format Trusted I/O Modules (Low Density I/O)

8000 Series

Family name for the certified range of Trusted products for use in a wide range of controls applications including safety, continuous process, supervisory control/data acquisition, and integrated control and safety.

TMR Processor

The Trusted processor for use in safety-related applications of the 8000 series system. Handles application program execution, diagnostics and reporting functions. The Trusted TMR Processor uses three high-performance RISC processors based on patented TMR architecture arranged in a lock-step configuration.

Trusted Toolset Suite

Software used to configure and program the Trusted TMR System.

TÜV Certification

Independent third-party certification against a defined range of International standards.

Voting System

Redundant system (for example, M out of N, 1002, 2003 etc.) which requires at least M of the N channels to be in agreement before the system can take action.

Watchdog

Watchdog circuitry provides dynamic and/or static monitoring of Trusted TMR Processor operation and is used to annunciate a processor or related failures.

Recommended proof test methods

This appendix identifies specific cases where the diagnostic coverage can only be achieved by performing specific proof tests.

1oo2 24V DC digital inputs

This test is required for all 24V DC DI channels (T8802, T8805 when used with the T8402) used for Safety-Related Inputs used where the Proof Test frequency >> frequency of Demands.

The purpose of this test is to verify that the channel sense resistor, located on the FTA has not failed, either open circuit or short circuit by verifying that the channel is reporting the correct state, therefore does not constitute a potential undetected dangerous failure.

The method described here is the recommended method to verify that neither a stuck off or stuck on condition can exist for the 1oo2 60 channel DI. It is assumed that this methodology will be incorporated into a Proof Test procedure that includes other elements of Proof Testing and general proof test requirements as defined in IEC61511.

There are two methods that can be used:

Method 1 – For Normally Energized (De-energize to Action) inputs without line monitoring.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Disconnect the field device at an appropriate termination point and verify that the state transitions from TRUE to FALSE.

Step 3 – Return the field device into service, verify that the state correctly transitioned back from FALSE to TRUE before removing the Lock/Force.

Method 2 – For Normally De-energized (Energize to Action) inputs with line monitoring.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Activate the field device (by closing the input switch, by simulation or otherwise) and verify that the state transitions from FALSE to TRUE.

Step 3 – Return the field device into service, verify that the state correctly transitioned back from TRUE to FALSE before removing the Lock/Force.

4-20mA analog inputs (non-isolated)

This test is required for all AI channels (T8830, T8831, T8842 when used with the T8431 and T8832, T8835 when used with the T8432) used for Safety-Related Inputs used where the Proof Test frequency >> frequency of Demands.

The purpose of this test is to verify that the channel sense resistor has not drifted beyond a reasonable accuracy by verifying that the channel is reporting values within its expected accuracy, therefore does not constitute a potential undetected dangerous failure.

The Proof Test method is based on +/- 0.5% (FSD) accuracy, the actual measurement accuracy of the AI channel is within this specification (+/-0.2%), and if tighter tolerances are required then this process can be modified appropriately.

The methods described here are the recommended methods to verify AI channel accuracy, it is assumed that this methodology will be incorporated into a Proof Test procedure that includes other elements of Proof Testing and general proof test requirements as defined in IEC61511.

There are two methods that can be used:

Method 1 – Apply a calibrated current source to the specific channel, with the field device disconnected.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Disconnect the field device at an appropriate termination point and connect a calibrated current simulation device in its place.

Step 3 – Follow the general calibration check procedure.

Step 4 – Return the field device into service, verify that it is operating correctly before removing the Lock/Force.

Method 2 – Use the field device to provide the current source, measuring the current with a suitably calibrated current meter.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Disconnect the field device at an appropriate termination point and connect a calibrated current meter in series to measure the field device current.

Step 3 – Follow the general calibration check procedure.

Step 4 – Return the field device into service, verify that it is operating correctly before removing the Lock/Force.

Calibration check procedure:

Step A - Set the current to the AI channel 4 mA, verify that the input value is in the range -25 to +25 counts.

Step B - Set the current to the AI channel 12 mA, verify that the input value is in the range 2023 to 2073 counts.

Step C - Set the current to the AI channel 20 mA, verify that the input value is in the range 4071 to 4121 counts.

Step D – Return to Specific Method.

4-20 mA analog inputs (isolated)

This test is required for all AI channels (T8833 when used with the T8433) used for Safety-Related Inputs used where the Proof Test frequency >> frequency of Demands.

The purpose of this test is to verify that the channel sense resistor has not drifted beyond a reasonable accuracy by verifying that the channel is reporting values within its expected accuracy, therefore does not constitute a potential undetected dangerous failure.

The Proof Test method is based on +/- 0.61% (FSD) accuracy, the calibration accuracy of the AI channel (not including the accuracy of the channel sense resistor) is within this specification (+/-0.15%), and if tighter tolerances are required then this process can be modified appropriately

The methods described here are the recommended methods to verify AI channel accuracy, it is assumed that this methodology will be incorporated into a Proof Test procedure that includes other elements of Proof Testing and general proof test requirements as defined in IEC61511.

There are two methods that can be used:

Method 1 – Apply a calibrated current source to the specific channel, with the field device disconnected.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Disconnect the field device at an appropriate termination point and connect a calibrated current simulation device in its place.

Step 3 – Follow the general calibration check procedure.

Step 4 – Return the field device into service, verify that it is operating correctly before removing the Lock/Force.

Method 2 – Use the field device to provide the current source, measuring the current with a suitably calibrated current meter.

Step 1 - If performing this test on a live system, Lock (using the SIS Workstation Software or Trusted Toolset Suite) or Bypass (using specific application method applied) the selected channel. If not, proceed to Step 2.

Step 2 - Disconnect the field device at an appropriate termination point and connect a calibrated current meter in series to measure the field device current.

Step 3 – Follow the general calibration check procedure.

Step 4 – Return the field device into service, verify that it is operating correctly before removing the Lock/Force.

Calibration check procedure:

Step A - Set the current to the AI channel 4 mA, verify that the input value is in the range -41 to +41 counts.

Step B - Set the current to the AI channel 12 mA, verify that the input value is in the range 2007 to 2089 counts.

Step C - Set the current to the AI channel 20 mA, verify that the input value is in the range 4055 to 4137 counts.

Step D – Return to Specific Method.

24V DC digital outputs

This test is required for all 24V DC DO modules or DC powered NO Contact where Normally De-energized (Energize to Trip) channels (T8850 when used with the T8451, T8461, or T8891 when used with the T8842) are used for Safety-Related Outputs used where the Proof Test frequency >> frequency of Demands.

The purpose of this test is to verify that the diodes used for OR'ing the two Field Power sources are not Open circuit, therefore does not constitute a potential undetected dangerous failure.

The method described here is the recommended method to verify that neither of the diodes used to OR the 24V DC field supply to a specific T8850 FTA, or the DC supply feeding NO Contact outputs is open circuit. It is assumed that this methodology will be incorporated into a Proof Test procedure that

includes other elements of Proof Testing and general proof test requirements as defined in IEC61511.

Method:

Step 1 - If performing this test on a live system, it may be necessary to employ a method external to the Trusted logic solver to mechanically or electrically force any Normally Energized (De Energize to Trip) outputs associated with final elements on the FTA under test into their normal operating state. If not, proceed to Step 2.

Step 2 – Turn off the 'A' field supply at an appropriate isolation or termination point and verify that the diode related to 'B' supply is correctly providing 24V DC to each power group on the FTA under test.

NOTE: Although strictly NOT required from a Proof Test perspective, a secondary test can be performed while the 'A' Power source is turned off (disconnected) to verify that the diode associated with the 'A' supply is not 'Short Circuit'. With 1k ohm resistor connected in series with the meter, measure the current (in mA) from the supply side of the diode to 0V and the current should be << 24 mA if the diode is correctly preventing backfeed of the 'B' supply (there will be a small leakage current, so it may not be 0 mA).

Step 3 – Return the 'A' field supply into service.

Step 4 – Turn off the 'B' field supply at an appropriate isolation or termination point and verify that the diode related to 'A' supply is correctly providing 24V DC to each power group on the FTA under test.

Note: Although strictly NOT required from a Proof Test perspective, a secondary test can be performed while the 'B' Power source is turned off (disconnected) to verify that the diode associated with the 'B' supply is not 'Short Circuit'. With 1k ohm resistor connected in series with the meter, measure the current (in mA) from the supply side of the diode to 0V and the current should be << 24 mA if the diode is correctly preventing backfeed of the 'A' supply (there will be a small leakage current, so it may not be 0 mA).

Step 5 – Return the 'A' field supply into service.

Step 6 – If required under Step 1, return any Normally Energized final element forces/bypasses back into normal service.

120V AC digital outputs

This test is required for all 120V AC DO modules that Normally De Energized (Energize to Trip) channels (T8871 when used with the T8472) used for Safety-Related Outputs used where the Proof Test frequency >> frequency of Demands.

The purpose of this test is to verify that the varistors (V1/V2) are not Short Circuit, therefore do not constitute a potential undetected dangerous failure.

The method described here is the recommended method to verify that neither of the varistors, which are across the output, have failed Short Circuit. It is assumed that this methodology will be incorporated into a Proof Test

procedure that includes other elements of Proof Testing and general proof test requirements as defined in IEC61511.

Method:

Step 1 - If performing this test on a live system, it will be necessary to disconnect the final element associated with the channel under test, this is to help prevent a spurious action occurring due to the Proof test. If not, proceed to Step 2.

Step 2 – Disconnect the switched output to final element, but with the 120V AC supply remaining connected and energized, verify that the output being tested reports a STATE value of 3 (No Load). Energize the output channel and verify that the channel STATE remains at STATE 3 (No Load), if the output, when energized reports either a STATE 4 (Output Energized) or a STATE 5 (Field Short Circuit) then the output channel likely has a failed varistor, so the FTA will need to be replaced.

Step 4 – De-energize the output, then reconnect the final element field connection and verify that the output is reporting a STATE 2 (Output De-energized).

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.

ICSTT-RM459K-EN-P, November 2023 (T8094 Issue 40)

Change
Updated Peer-to-Peer usage conditions
Updated Power Supply Requirements precautionary note
Updated Power Supply Requirements in Table 4.4 checklist
Added reference for Network Firewall and precautionary Warning statement for changing default system password
Deleted Expansion Channels Communications Path proof test

ICSTT-RM459J-EN-P, October 2021 (T8094 Issue 39)

Change
Changed "European Standard" to "standard" in *EN 54 requirements*
UKCA update - *Electromagnetic Compatibility (EMC)*
Updated Proof Test method accuracy in *4-20 mA analog inputs (isolated)*

ICSTT-RM459I-EN-P, March 2021 (T8094 Issue 38)

Change
Updated publication template
Updated *Safety management*, *Safety system validation*, *Operation and maintenance plan*, *Safety-related configurations*, *Trusted high-density I/O*, and *Climatic conditions* sections.

Issue 37, December 2019

Change
Added AADvance-Trusted SIS Workstation Software and T8111 information to several sections.
Added Process Control Functions section.

Issue 36, July 2019

Change
Updated for T8425.
Updated section F.1.5 120V AC Digital Outputs.

Issue 35, May 2019

Change
Replaced Appendix D.1 content with Attention statement that includes a reference to the product information publication.

Issue 34, December 2018

Change
Added section F.1.6 Expansion Chassis Communication Path.

Issue 33, October 2018

Change
Address fault tolerance requirement NFPA 85 clause 4.11.3
Added section 3.14.5 DC Output Module Field Power Reverse Polarity Protection.
Updated section 3.2.2 with information on application of safety wiring principles for field loops.
Updated references to figures and tables in sections 1.3.4, 2.3.1, 2.3.2, 2.3.3, 3.12.2, C.1.4, and C.2.7.
Changed paragraph style of text for Figure 4 in section 3.2.2.
Added Rockwell Automation publication number.
Added registered trademarks statement.

Issue 31, June 2017

Change
Update to EMC guidance – not released

Issue 30, May 2017

Change
Updated to include Triguard® peer to peer support

Issue 29, March 2016

Change
Update for Trusted Release 3.6.1

Issue 28, July 2015

Change
Update for Trusted Release 3.6.

Issue 27, June 2013

Change
Update for TÜV Rheinland certification of CS300 migration (Appendix C and section 3.13)
Change of company name in text to Rockwell Automation

Issue 26

Change
Not released.
Draft A – 21 May 2013
Draft B – 23 May 2013

Issue 25, May 2013

Change
Instructions for use of "Autotest" management function blocks added in Appendix C.
Additions and corrections to Appendix C for certification.

Issue 24, January 2013

Change
Details of CS300 migration added in Appendix C.

Issue 23, November 2012

Change
Obsolete – withdrawn.

Issue 22, November 2012

Change
Update for certification of release 3.5.3.

Issue 21, October 2009

Change
Relevant sections revised due to updated standards; NFPA 72:2007, NFPA 85:2007, NFPA 86:2007.; ICS Triplex Technology replaced with ICST Triplex

Issue 20, February 2009

Change

Issue 20, February 2009

Change
Company logo; master\slave replaced by active\standby; Section 3.7.2 corrected Companion Slot configuration; Added section 6 SYSTEM SECURITY

Issue 19

Change
Not released

Issue 18, July 2006

Change
Modified Table 3 regarding Peer to Peer

Issue 17, November 2005

Change
Added T8442 Module (Table 6). Added T8424 Module (Table 4). Added Enhanced Peer to Peer (Table 3 & section 3.10).; Updated Table 10, forced air temperatures.; Changed suggested Global Protection to level 8 in table 8.; Corrected reference to NFPA 86 & EN 54 in 3.2.7 & 3.2.8

Issue 16, November 2004

Change
Updated to incorporate TÜV Rheinland comments to release 3.41; Record of amendments for issue 15 had incorrect table reference for 8472 Output module; Previously unlabeled figures and tables given references in issue 15 and hence figure and table numbering changed.; Some points in checklist 4.2.1 were changed in error and have been corrected in issue 16

Issue 15, March 2004

Change
Added Appendix B – Triguard (SC300E) support; Added Application and System Configuration archive to 3.12.1 and 3.12.2.; Added 8472 Output Module to Table 5; Reworded 2.2.1.10.3 & 3.2.4; Removed item 4 from section 3.13.3; Corrected reference in 3.11.3 to specify section 5; Added "Grey Channel" to glossary; Corrected 3.6.2 paragraph 2 to refer to the correct section.; 3.7.2 added 'companion slot' to a. and removed 'pair' from b.

Issue 14

Change
Added 3.7.1.6 & updated 3.22; System Release 3.4

Issue 13

Change
Updated Section 3.12.11 For Intelligent Update

Issue 12

Change
Not released

Issue 11, May 2003

Change
System release 3.3

Issue 10, May 2003

Change
Updated to reflect Technischer Überwachungs-Verein (TÜV) comments

Issue 9, May 2003

Change
Added IEC 61508, EN 54, NFPA 85 and HFPA 86 requirements

Issue 8, Jan 2003

Change
Updated to reflect EN 60204 stop categories. Reworded 3.5.1.2

Issue 7 , January 2003

Change
Updated to reflect 3.2 certification.

Issue 6, May- 2002

Change
Updated to reflect 3.1 certification.

Issue 5, March 2002

Change
Updated to correct table and figure numbering.

Issue 4, March 2002

Change
Updated to add new logo

Issue 3, November 2001

Change
Updated to reflect 3.0 certification.

Issue 2, September 2001

Change
Updated to reflect recertification as of September 2001

Issue 1, September 1999

Change
Initial Issue

Rockwell Automation support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	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 information on its website at rok.auto/pec.

Rockwell Otomayson Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenkÖy, İstanbul, Tel: +90 (216) 5698400 EEE YÖnetmeliğine Uygundur

Connect with us.

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

Rockwell Automation Publication ICSTT-RM459K-EN-P, November 2023
Supersedes Publication ICSTT-RM459J-EN-P, October 2021