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

Appendix D

Hazardous area and electrical safety information

Appendix E

Glossary

Appendix F

Recommended proof test methods

Appendix G

History of changes

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 1oo1 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 1oo1D.

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 (1oo2 also known as 1v2), with either channel able to initiate the fail-safe reaction, or Two-out-of-Two (2oo2 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.

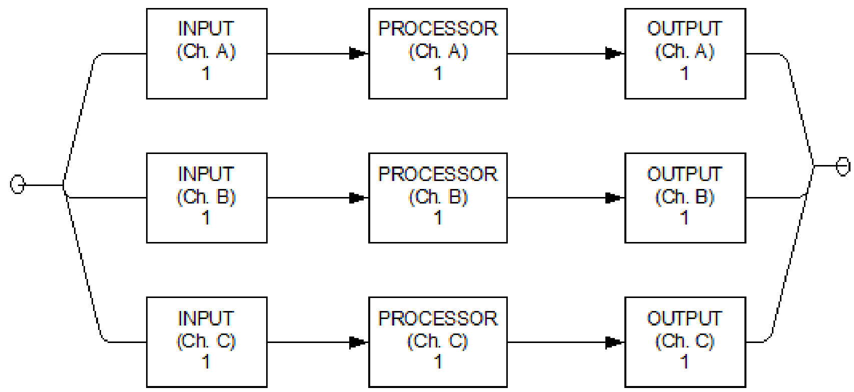

Figure 1: Simple Triplicated System

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.

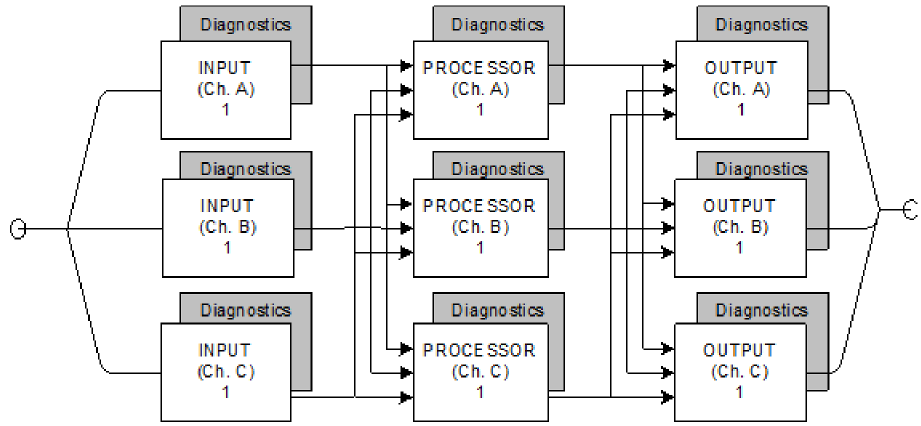

Figure 2: TMR Architecture

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.