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.

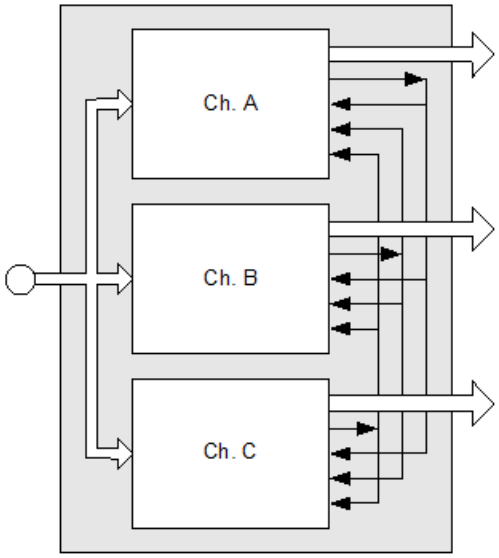

Figure 3: Single High-Density TMR I/O Module Architecture

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.

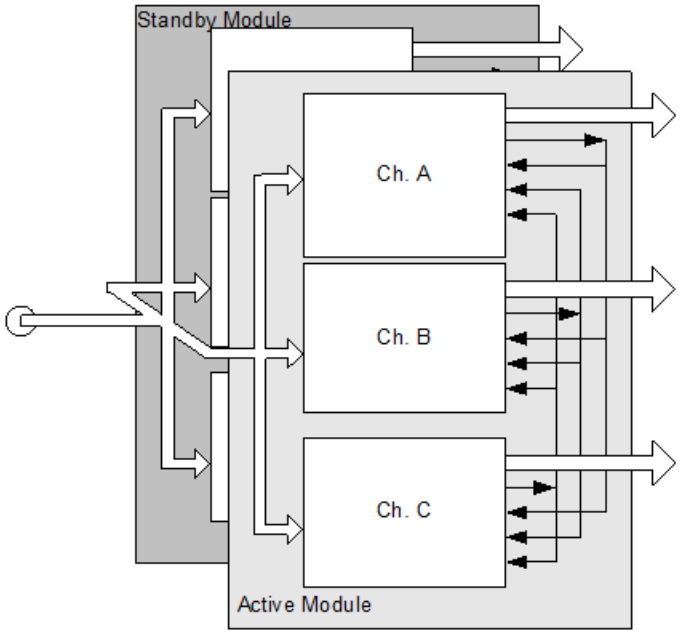

Figure 4: SmartSlot or Adjacent Slot TMR Module Configuration

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.