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

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