

Tricon Triple Modular Redundant (TMR) System Configuration and Degraded Mode of Operation

Functional Safety Requirements Category:	AK 1-6 (DIN 19250, DIN 0801) SIL 1-3 (IEC 61508)
Structure/Architecture:	2-out-of-3 with Diagnostics (2oo3D)
Mode of Operation	3-2-1-0 (configurable)

1. Central/Main Processors

Number of Central Processors	3
Structure of Central Processors	2oo3D
System response/behavior in the event of:	
1 st Central Processor failure	Shutdown and alarm of the faulted Central Processor. Central Processors structure degrades to 1oo2D. (See note 1, 2, & 3)
2 nd Central Processor failure	Shutdown and alarm of the faulted Central Processor. Central Processors structure degrades to 1oo1D. (See note 1, 2, & 3)
3 rd Central Processor failure	Shutdown and alarm of the faulted Central Processor. Controller de-energizes to the safe-state. (See note 1, 2, & 3)

2. I/O Communication Busses

Number of I/O Communication Busses	3
Structure of I/O Communication Busses	2oo3D
System response / behavior in the event of:	
1st I/O Communication Bus failure	Shutdown and alarm of the faulted I/O Comm. Bus. I/O Comm. Bus structure degrades to 1oo2D. (See note 1, 2, & 3)
2nd I/O Communication Bus failure	Shutdown and alarm of the faulted I/O Comm. Bus. I/O Comm. Bus structure degrades to 1oo1D. (See note 1, 2, & 3)
3rd I/O Communication Bus failure	Shutdown and alarm of the faulted I/O Comm. Bus. Controller de-energizes to the safe-state. (See note 1, 2, & 3)

Continued

Continued

3. I/O Modules

Number of I/O channels (Legs) per module	3
Structure of I/O channels (Legs) per module	2oo3D
System response/ behavior in the event of:	
1st failure of an I/O Module channel (Leg)	Shutdown and alarm of the faulted I/O channel (Leg). Modules I/O structure degrades to 1oo2D. (See note 1, 2, & 3)
2nd failure of an I/O Module channel (Leg)	Shutdown and alarm of the faulted I/O channel (Leg). Module I/O structure degrades to 1oo1D. (See note 1, 2, & 3)
3rd failure of an I/O Module channel (Leg)	Shutdown and alarm of the faulted I/O channel (Leg). Shutdown of faulted module and use safe default values for I/O points affected. (See note 1, 2, & 3)

Note 1:

All Tricon logic solver faults can be repaired online without further degradation of the system and should be performed before a 2nd fault occurrence to maintain the highest availability of the system. The highly effective means of modular insertion and replacement of faulted Tricon components is transparent to the operation of the system and the ease of replacement mitigates the risk of systematic failure as defined by IEC 61508. It is highly recommended that a faulted component be replaced within industry accepted Mean-Time-To-Repair (MTTR) periods.

Note 2:

The generic standards (IEC 61508 and DIN 19250 in companion with DIN 0801) do not give exact figures or operation guidelines for a system when a fault has been detected and the system structure has been degraded as a result of that fault. Please refer to the Tricon Safety Consideration Guide for recommended timing restrictions when operating in degraded mode. Refer to <http://www.tuv-fs.com/plcgen4.htm> for TUV guidelines when operating in degraded mode.

Within the time restriction for the degraded mode the probability of failure fulfils the requirements of the SIL level specified for Tricon system.

Note 3:

2oo3D, 1oo2D, and 1oo1D are Tricon system architectures for a given demand mode of operation.