

Trident V1.2 Triple Modular Redundant (TMR) System Configuration and Degradation

| | |
|---|--|
| 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 |
| Central/Main Processors | |
| Number of Central Processors | 3 |
| Structure of Central Processors | 2oo3D |
| System response/behavior in the event of: 1 st failure of a Central Processor | Shutdown and alarm of the faulted Central Processor Central Processors structure degrades to 2oo2D Temporary unlimited operation of the remaining Central Processors (see note 1 and 2) |
| 2 nd failure of a Central Processor | Shutdown and alarm of the faulted Central Processor Central Processors structure degrades to 1oo1D Temporary unlimited operation of the remaining Central Processor (see note 1 and 2) |
| 3 rd failure of a Central Processor | Shutdown and alarm of the faulted Central Processor Controller de-energizes to the safe-state |
| 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: 1 st failure of a I/O Communication Bus | Shutdown and alarm of the faulted I/O Comm. Bus Comm. Bus structure degrades to 2oo2D Temporary unlimited operation of the remaining Comm. Busses (see note 1 and 2) |
| 2 nd failure of a I/O Communication Bus | Shutdown and alarm of the faulted I/O Comm. Bus Comm. Bus structure degrades to 1oo1D Temporary unlimited operation of the remaining Comm. Bus (see note 1 and 2) |
| 3 rd failure of a I/O Communication Bus | Shutdown and alarm of the faulted I/O Comm. Bus Controller de-energizes to the safe-state |

Continued

Continued

I/O Modules

Each input and output point is considered to operate in Triple Modular Redundant (2oo3D), dual (2oo2D), single (1oo1D) or zero mode. The current mode indicates the number of channels controlling a point. I/O module degradation is at point level.

| | |
|---|--|
| Number of I/O channels (Legs) per point | 3 |
| Structure of I/O channels (Legs) per point | 2oo3D |
| System response/behavior in the event of: 1 st channel failure on a single I/O point per module or 1 st channel failure on multiple I/O points per module. | Alarm of the faulted I/O points Faulted I/O points structure degrades to 2oo2D Unlimited operation of all I/O point channels (see note 1 and 2) |
| 2 nd channel failure on a single I/O point per module or 2 nd channel failure on multiple I/O points per module. | Alarm of the faulted I/O points Faulted I/O point structure degrades to 1oo1D Temporary Unlimited operation of all I/O point channels (see note 1 and 2) |
| 3 rd channel failure on a single I/O point per module or 3 rd channel failure on multiple I/O points per module. | Fail-safe shutdown and alarm of the faulted I/O points |

Note 1: All Trident 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 Trident components is transparent to the operation of the system and the ease of replacement mitigates the risk of systematic and human induced 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 Trident V1.2 Safety Consideration Guide for recommended timing restrictions when operating in degraded mode. Go to www.tuv-fs.com/plcgen4.htm for TUV guidelines when operating in degraded mode.