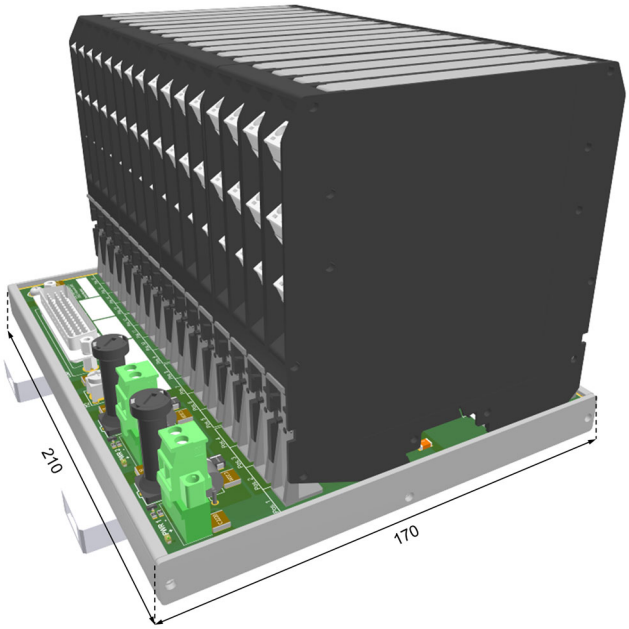
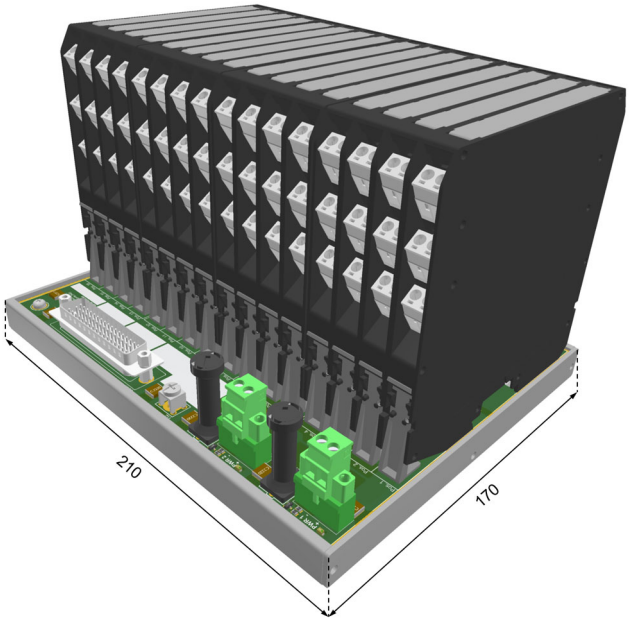




SAFETY MANUAL

SIL 3 Termination Board 16 positions for Tricon CX Universal card 3902X, Models TB-D5016-TRI-010 & TBE-D5016-TRI-010

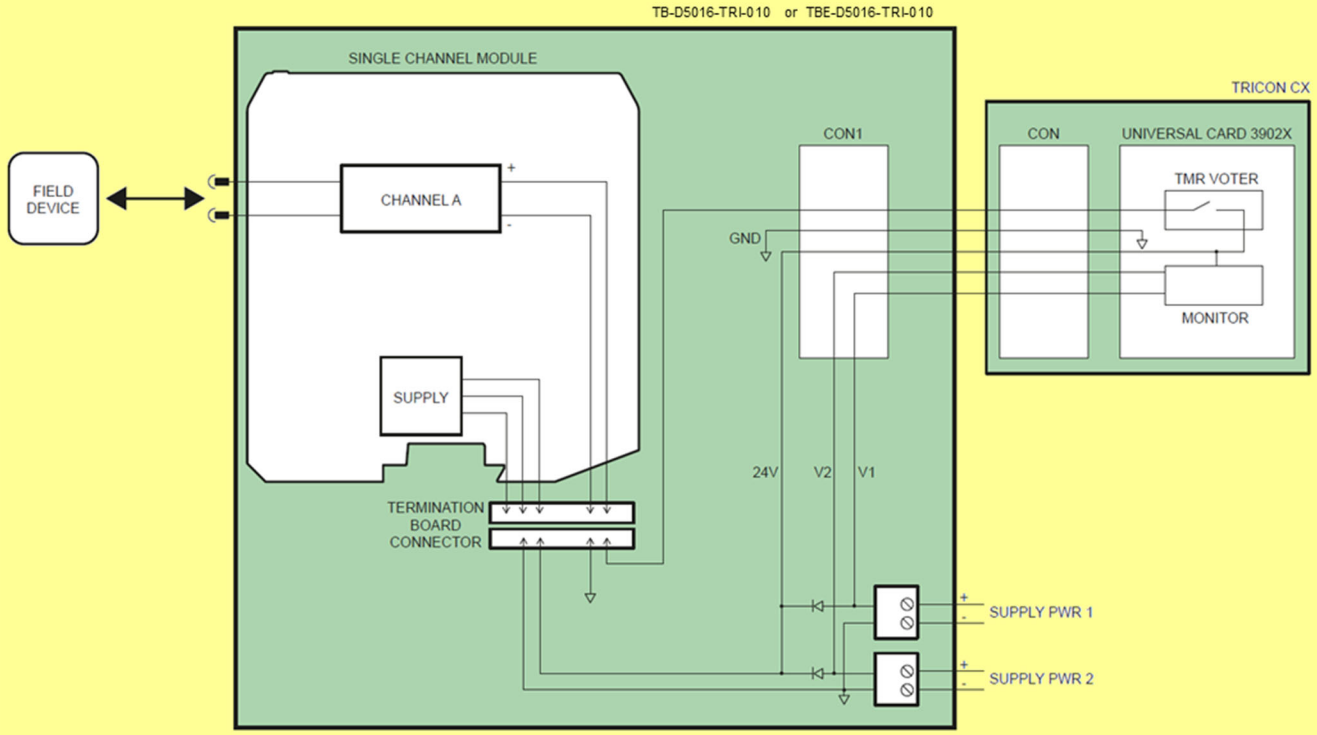
Approval: TÜV Certificate No. TUV IT 25 SIL 0634, SIL 3 conforms to IEC61508:2010 Ed.2 .
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Reference must be made to the relevant sections within the instruction manual ISM0452, which contain basic guides for the installation of the equipment.

gmi technology for safety

TB-D5016-TRI-010 or TBE-D5016-TRI-010 in connection with Tricon CX Universal card 3902X and D5000/D6000 series modules

Application for a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel, considering AI, AO, DI or DO module loop with DTT condition



Description:

The TB-D5016-TRI-010 or TBE-D5016-TRI-010 Termination Board provides direct connection between the Tricon CX Universal card 3902X and D5000 / D6000 series modules. The 24 Vdc Power Supply of the TB is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply. The 24 Vdc is used to supply D5000 / D6000 series modules by TB connector and it is given to Tricon CX Universal card 3902X to drive or control AI, AO, DI or DO module loop (with DTT De-energized To Trip condition of the loop). In the diagram is shown a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel connected to AI, AO, DI or DO single channel module by means of TMR voter of the Tricon CX Universal card 3902X.

Safety Function and Failure behavior:

The Tricon CX Universal card 3902X has got internal diagnostics to monitor both PWR1 supply source voltage V1 and PWR2 supply source voltage V2 and also 24 Vdc redundant power supply voltage after OR-ing diode mixing, detecting and notifying possible failure of these power supply lines. This failure detection can be enabled with the following Safety Function because it's can be used to detect safe failures. TB-D5016-TRI-010 or TBE-D5016-TRI-010 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel (connected to AI, AO, DI or DO module loop with De-energizing To Trip (DTT) condition of the loop) is described from the following definitions:

- □ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with de-energizing condition (DTT) of the loop connected to AI, AO, DI or DO module. Tricon CX 3902X card internal diagnostics can be used to detect and notify this failure so that it can be considered safe detected (SD).
- □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
- □ Fail Dangerous: failure mode that implies the redundant power supply voltage is blocked or oscillating in the range above 0 Vdc and below 20 Vdc or above 30 Vdc.
- □ Fail "No Effect": failure mode of a component that is part of the safety function but is neither a safe failure nor a dangerous failure, so that the redundant power supply voltage is in the range 20 to 30 Vdc. When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	1.04
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.04**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**109'923 years**
$\lambda_{no\ effect}$ = "No effect" failures	105.36
$\lambda_{not\ part}$ = "Not Part" failures	34.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**140.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**810 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S
1.04 FIT	0.00 FIT	0.00 FIT	0.00 FIT	100.00%	100.00%

where DC_S means the safe diagnostic coverage for TB supply+channel by Tricon CX Universal card 3902X.

When a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel operates in Low Demand mode:

the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel has **SIL 3 level for product lifetime of 20 years.**

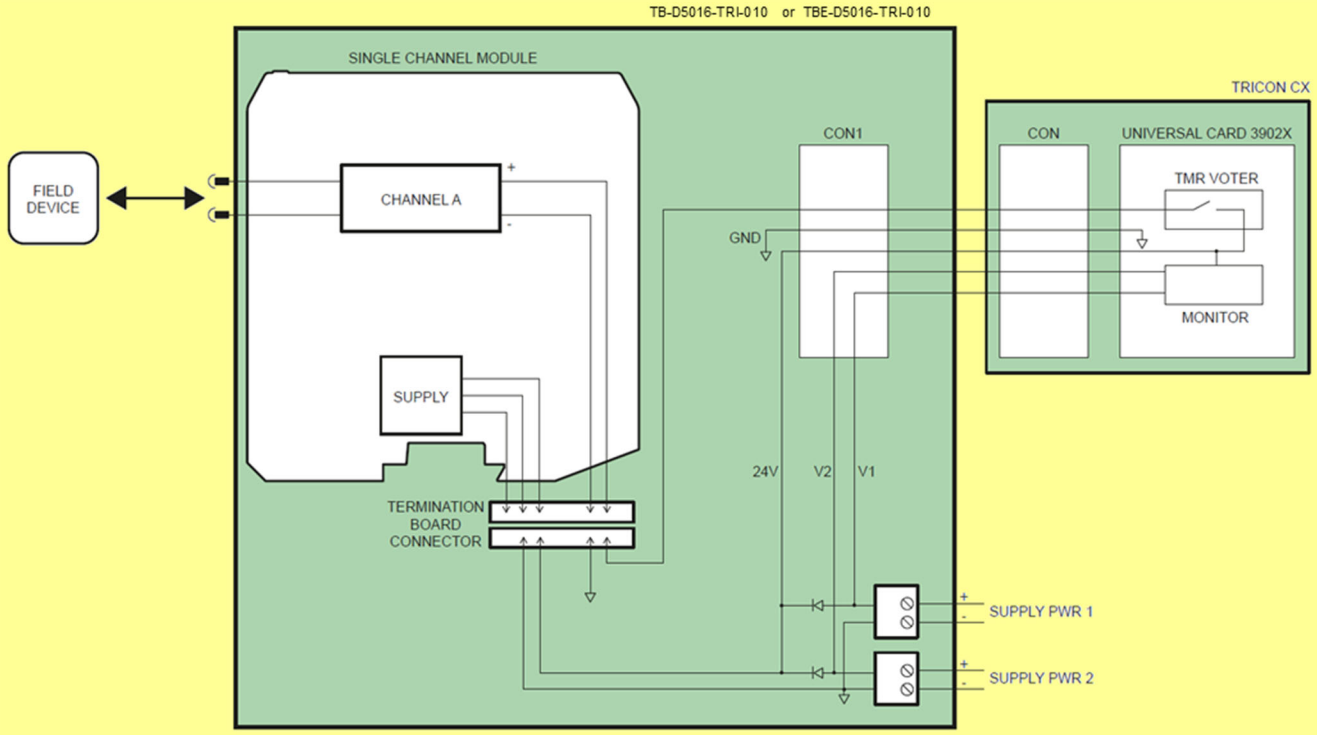
When a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel operates in High Demand mode:

the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

Systematic capability SIL 3.

TB-D5016-TRI-010 or TBE-D5016-TRI-010 in connection with Tricon CX Universal card 3902X and D5000/D6000 series modules

Application for a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel, considering DO module loop with ETT condition



Description:

The TB-D5016-TRI-010 or TBE-D5016-TRI-010 Termination Board provides direct connection between the Tricon CX Universal card 3902X and D5000 / D6000 series modules. The 24 Vdc Power Supply of the TB is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply. The 24 Vdc is used to supply D5000 / D6000 series modules by TB connector and it is given to Tricon CX Universal card 3902X to drive or control DO module loop (with ETT Energized To Trip condition of the loop). In the diagram is shown a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel connected to AI, AO, DI or DO single channel module by means of TMR voter of the Tricon CX Universal card 3902X.

Safety Function and Failure behavior:

The Tricon CX Universal card 3902X has got internal diagnostics to monitor both PWR1 supply source voltage V1 and PWR2 supply source voltage V2 and also 24 Vdc redundant power supply voltage after OR-ing diode mixing, detecting and notifying possible failure of these power supply lines. This failure detection must be enabled with the following Safety Function because it must be used to detect dangerous failures.

TB-D5016-TRI-010 or TBE-D5016-TRI-010 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel (connected to DO module loop with Energizing To Trip (ETT) condition of the loop) is described from the following definitions:

- □ Fail-Safe State: it is defined as the redundant power supply voltage in the range 20 to 30 Vdc, with energizing condition (ETT) of the loop connected to DO module.
- □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process, so that the redundant power supply voltage is blocked or oscillating below 20 Vdc or above 30 Vdc. Tricon CX 3902X card internal diagnostics must be used to detect and notify this failure so that it is considered dangerous detected (DD).
- □ Fail "Not part": failure mode of a component that is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	1.04
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.04**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**109'923 years**
$\lambda_{no\ effect}$ = "No effect" failures	105.36
$\lambda_{not\ part}$ = "Not Part" failures	34.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**140.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**810 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_D
0.00 FIT	0.00 FIT	1.04 FIT	0.00 FIT	100.00%	100.00%

where DC_D means the dangerous diagnostic coverage for TB supply+channel by Tricon CX Universal card 3902X.

When a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel operates in Low Demand mode:

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 8.32 E-09 - Valid for **SIL 3**	PFDavg = 1.66 E-07 - Valid for **SIL 3**

When a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel operates in High Demand mode:

the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

Systematic capability SIL 3.

Testing procedure at T-proof

Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

In particular, the Tricon CX Universal card 3902X has got internal diagnostics to monitor both PWR1 supply source voltage V1 and PWR2 supply source voltage V2 and also 24 Vdc redundant power supply voltage after OR-ing diode mixing, detecting and notifying possible failure of these power supply lines. This failure detection must be enabled when a TB-D5016-TRI-010 or TBE-D5016-TRI-010 channel is connected to DO module loop with Energizing To Trip (ETT) condition of the loop because it must be used to detect dangerous failures.