SAFETY MANUAL

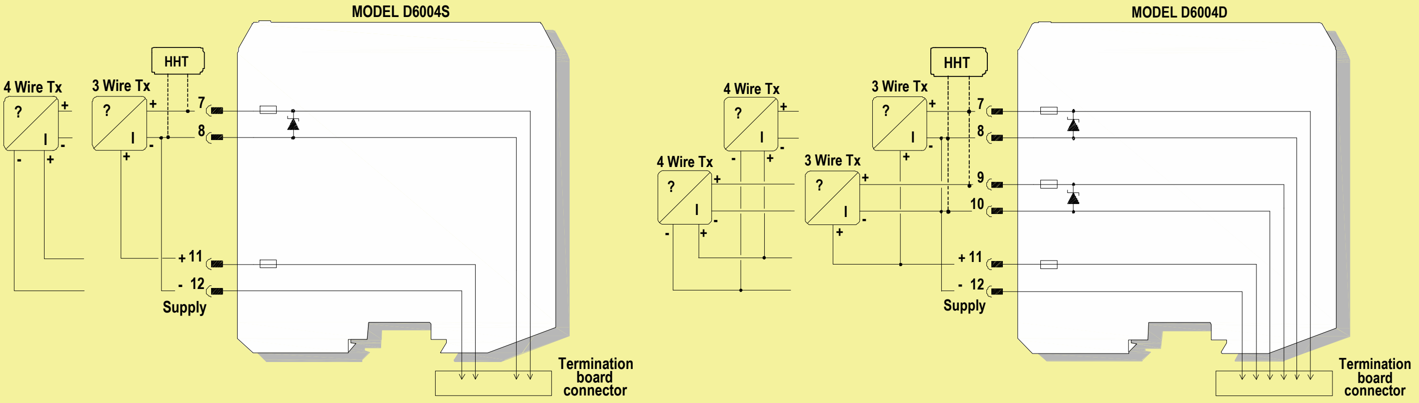
SIL 3 Pass-Through Module,
Termination Board,
Model D6004S, D6004D

Reference must be made to the relevant sections within the Instruction Manual ISM0447, which contain basic guides for the installation of the equipment.

gmi technology for safety

D6004 module in connection with TB-D5016-TRI-010 or other Termination Board and 3/4-wire field transmitter

Application for a D6004 channel, connected to field transmitter and AI module loop with DTT condition



Description:

The D6004S/D is a Single/Double channel pass-through models, marshalling for field and control side circuits, with over-current and over-voltage protection and supplying 3/4-wire transmitters through the power supply of the Termination board. Each D6004 channel provides direct connection between TB-D5016-TRI-010 (only for D6004S version) or other termination board (both D6004S and D6004D versions in accordance with TB model features) and 3/4-wire transmitter for an AI module loop operating (with DTT De-energized To Trip condition of the loop).

Safety Function and Failure behavior:

D6004S/D is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of a D6004 channel (connected to field transmitter and AI 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 de-energized condition (DTT) of the field transmitter loop connected to AI module by means of termination board.
□ 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.
□ Fail “No Effect”: failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure nor a dangerous failure and it has no effect on safety function. 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.

The following analysis is also valid for each channel of D6004D module because two channels are totally independent (for dangerous failures) one from other.
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	0.00
λ_{su} = Total Safe Undetected failures	10.95
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**10.95**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**10`425 years**
$\lambda_{no\ effect}$ = “No effect” failures	46.05
$\lambda_{not\ part}$ = “Not Part” failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**57.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**2002 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	10.95 FIT	0.00 FIT	0.00 FIT	100.00%

If the PLC/DCS I/O Card (connected to TB, therefore to module channel) has got short circuit and open loop detection enabled, the **λ_{su}** failures can be detected and converted on safe detected (SD) failures, with DC_S = 100.00 % of safe diagnostic coverage for module channel by I/O card of the PLC/DCS system.

When a D6004 channel operates in Low Demand mode:

the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a D6004 channel has **SIL 3 level for product lifetime of 20 years.**

When a D6004 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 (un)detected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.