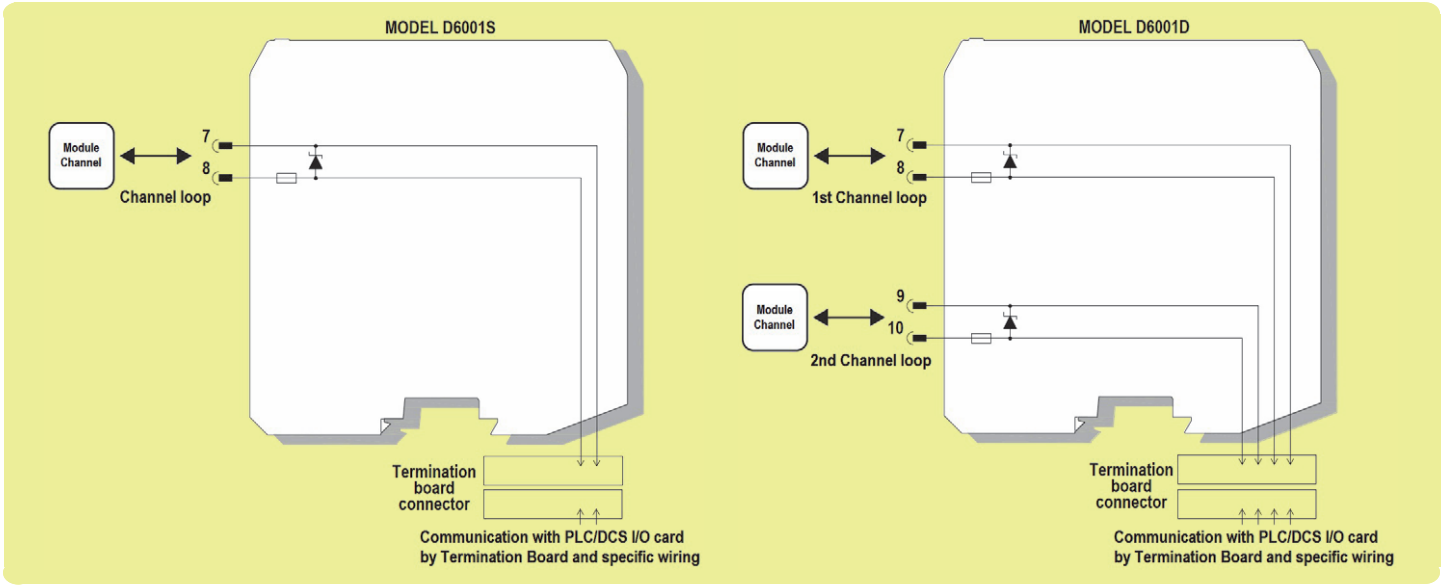
SAFETY MANUAL

SIL 3 Dummy Pass-Through Module, Termination Board, Model D6001S, D6001D

Reference must be made to the relevant sections within the datasheet DTS0810, which contain basic guides for the installation of the equipment.

D6001 module in connection with TB-D5016-TRI-010 or other Termination Board and AI, AO, DI, DO module

Application for a D6001 channel, connected to AI, AO, DI or DO module loop with DTT condition



Description:

The D6001S/D is a Single/Double channel dummy pass-through models, marshalling for field and control side circuits, with over-current and over-voltage protection.
Each D6001 channel provides direct connection between TB-D5016-TRI-010 (only for D6001S version) or other termination board (both D6001S and D6001D versions in accordance with TB model features) and AI, AO, DI or DO module loop (with DTT De-energized To Trip condition of the loop).

Safety Function and Failure behavior:

D6001S/D is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of a D6001 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 de-energized condition (DTT) of the loop connected to AI, AO, DI or 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.
- □ 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 D6001D module because two channels are totally independent 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	8.45
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**8.45**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**13'509 years**
$\lambda_{no\ effect}$ = "No effect" failures	23.55
$\lambda_{not\ part}$ = "Not Part" failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**32.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**3567 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	8.45 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 DCS = 100.00 % of safe diagnostic coverage for module channel by I/O card of the PLC/DCS system.

When a D6001 channel operates in Low Demand mode:

the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a D6001 channel has **SIL 3 level for product lifetime of 20 years.**

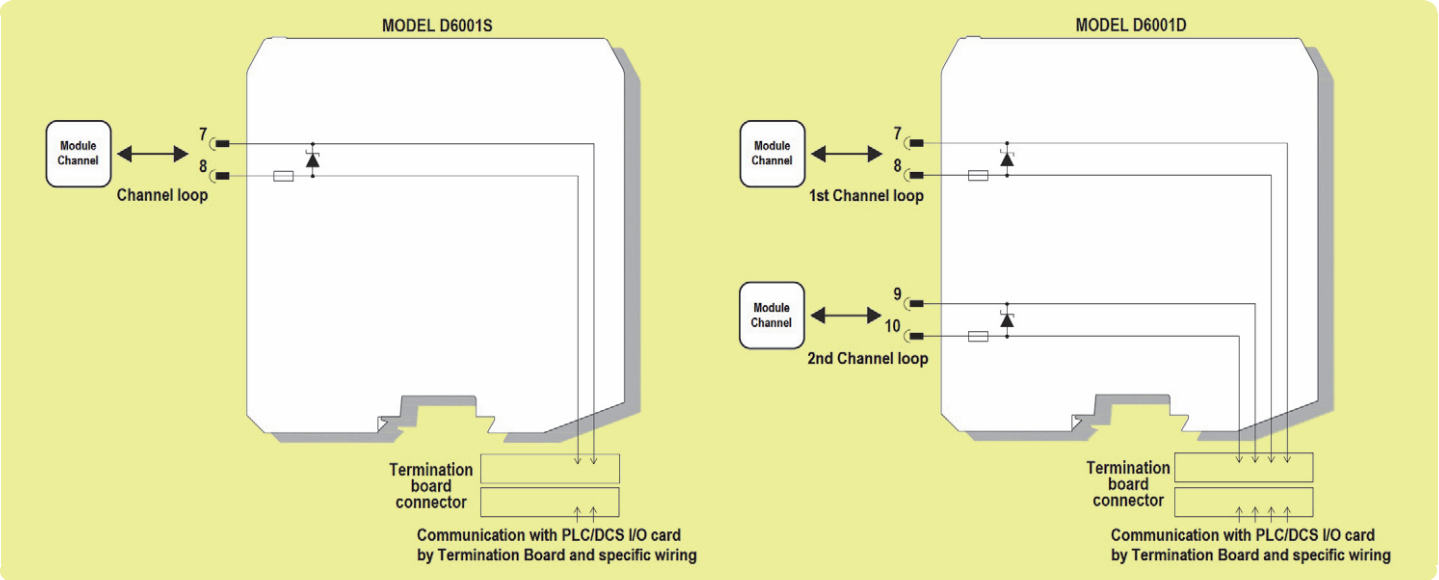
When a D6001 channel operates in High Demand mode:

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

Systematic capability SIL 3.

D6001 module in connection with TB-D5016-TRI-010 or other Termination Board and AI, AO, DI, DO module

Application for a D6001 channel, connected to DO module loop with ETT condition



Description:

The D6001S/D is a Single/Double channel dummy pass-through models, marshalling for field and control side circuits, with over-current and over-voltage protection.
Each D6001 channel provides direct connection between TB-D5016-TRI-010 (only for D6001S version) or other termination board (both D6001S and D6001D versions in accordance with TB model features) and DO module loop (with ETT Energized To Trip condition of the loop).

Safety Function and Failure behavior:

D6001S/D is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
When a D6001 channel (connected to DO module loop with Energizing To Trip (ETT) condition of the loop) is used on TB-D5016-TRI-010 or other termination board, it's mandatory that the PLC/DCS I/O Card (connected to TB, therefore to module channel) has got short circuit and open loop detection enabled in order to detect dangerous failure.
The failure behaviour of a D6001 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 energized 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 loop connected to DO module cannot be energized.
- □ 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 D6001D module because two channels are totally independent 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	8.45
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) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**8.45**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**13'509 years**
$\lambda_{no\ effect}$ = "No effect" failures	23.55
$\lambda_{not\ part}$ = "Not Part" failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**32.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**3567 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	8.45 FIT	0.00 FIT	100.00%	100.00%

where DC_D means the dangerous diagnostic coverage for module channel by I/O card of the PLC/DCS system, because the PLC/DCS I/O Card (connected to TB, therefore to module channel) must have short circuit and open loop detection enabled.

When a D6001 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 = 6.76 E-08 - Valid for **SIL 3**	PFDavg = 1.35 E-06 - Valid for **SIL 3**

When a D6001 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, when a D6001 channel (connected to DO module loop with Energizing To Trip (ETT) condition of the loop) is used on TB-D5016-TRI-010 or other termination board, it's mandatory that the PLC/DCS I/O Card (connected to TB, therefore to module channel) has got short circuit and open loop detection enabled in order to detect dangerous failure.