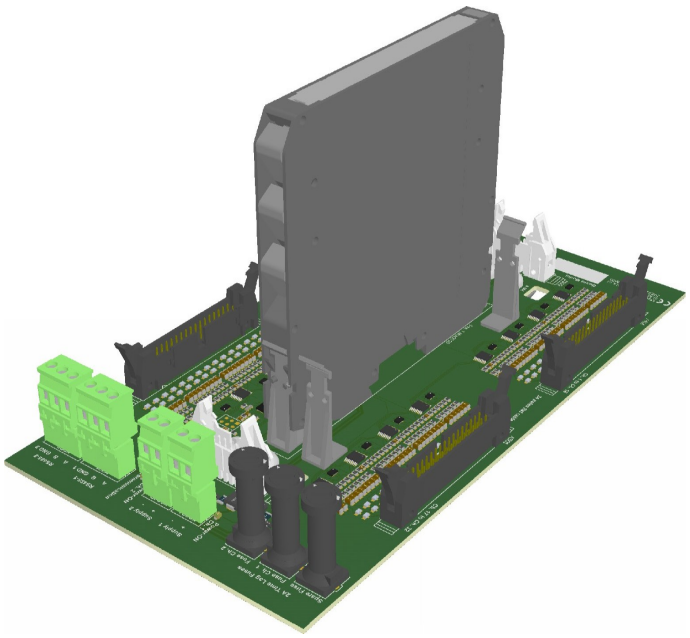
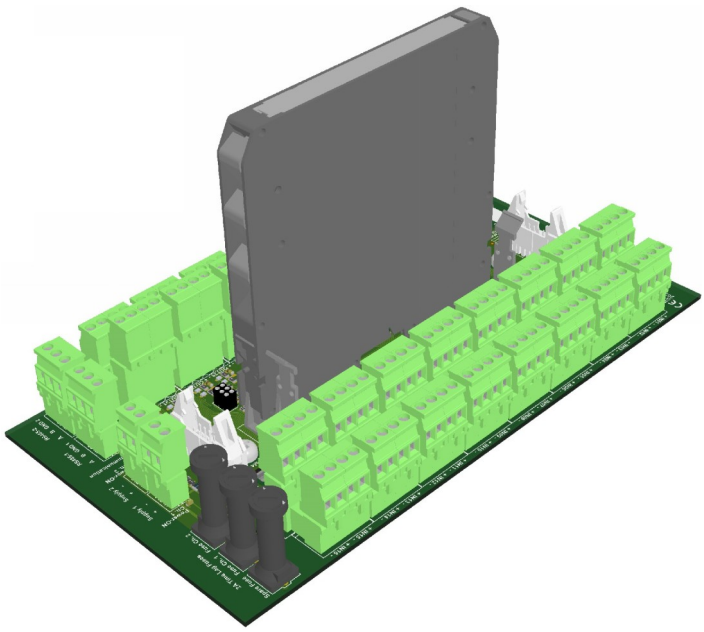




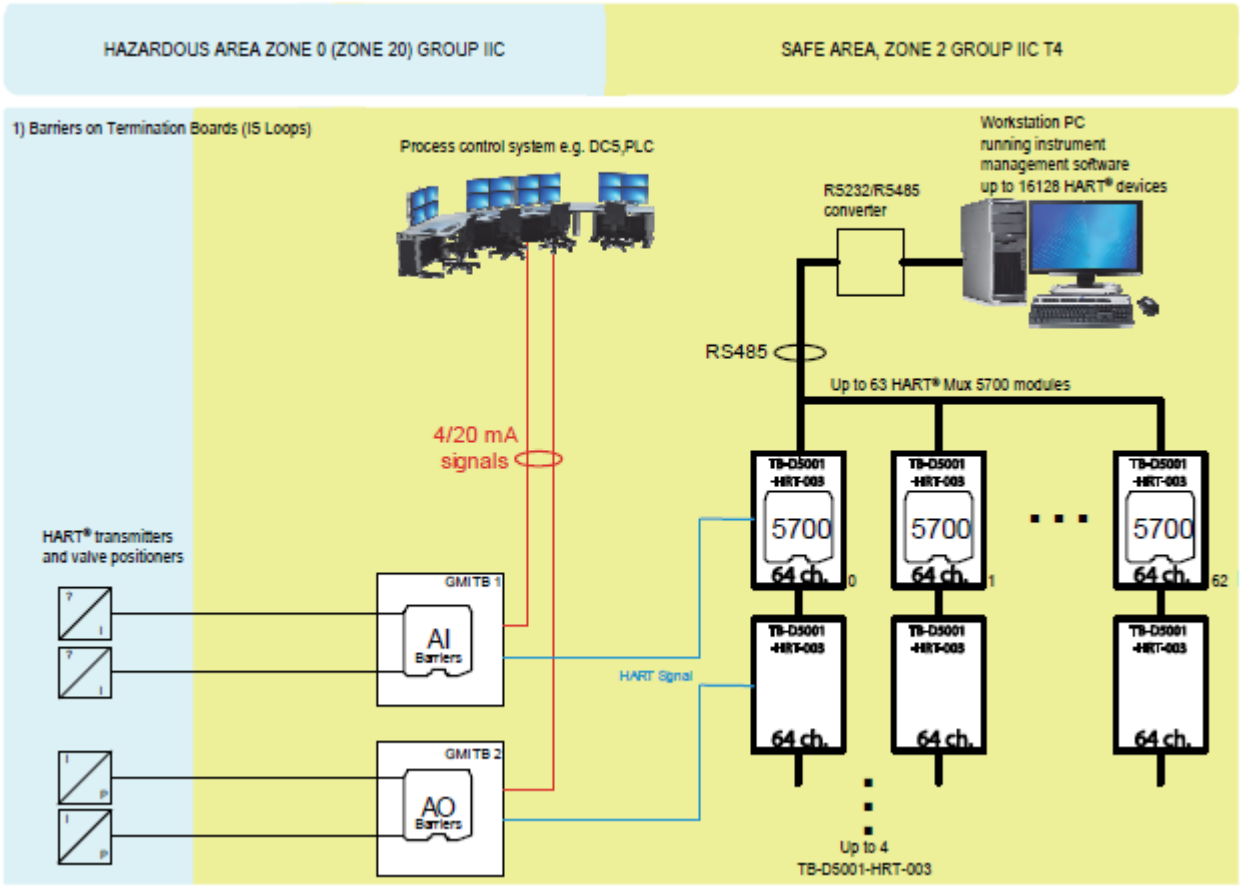
SAFETY MANUAL

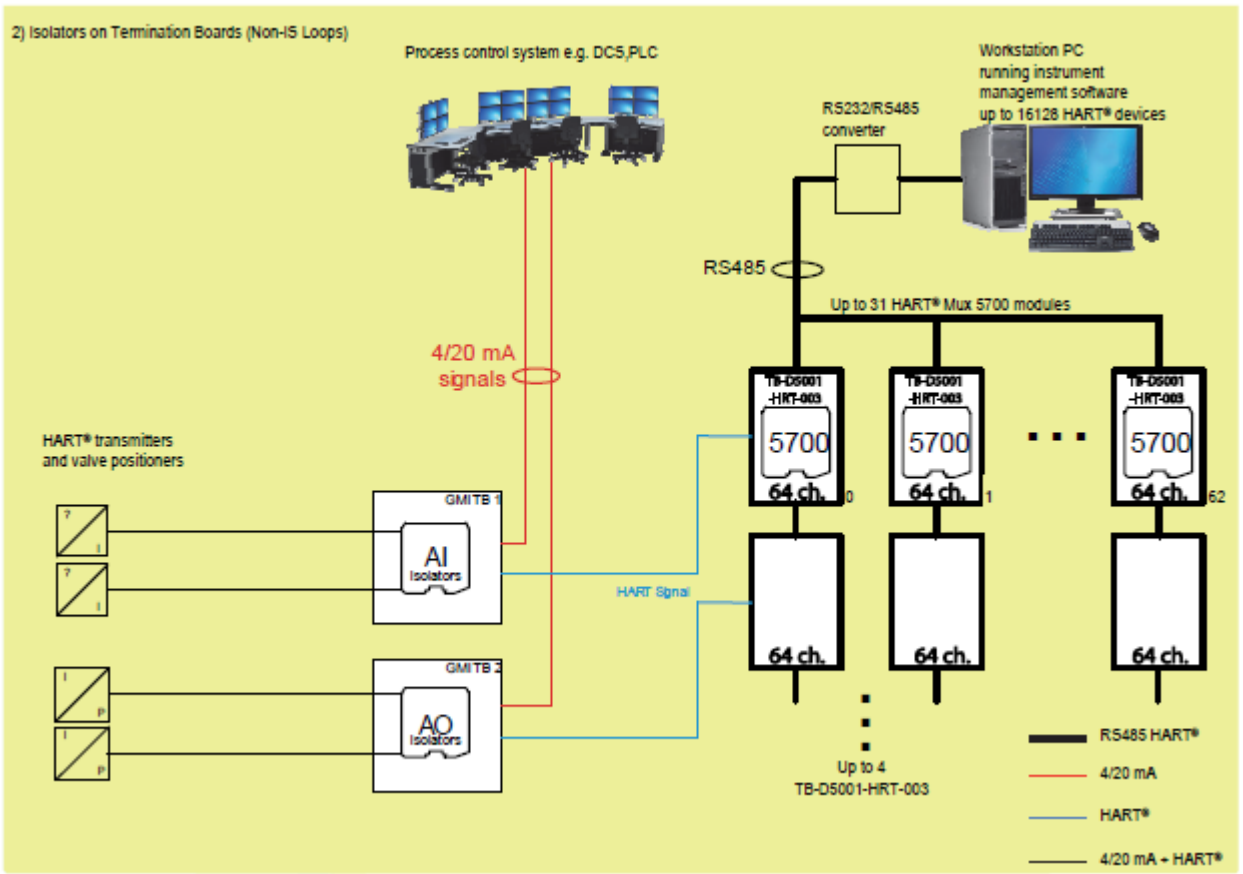
SIL 3 HART® Multiplexer Termination Board 1 position with SIL 3 HART® Multiplexer Modem 5700 for up to 64 channels (for TB-D5001-HRT-003) or 32 channels (for TB-D5001-HRT-004, -005, -006, -007) all extendable to 256 channels

Reference must be made to the relevant sections within the datsheets DTS0640 (for 5700), DTS0746 (for TB-D5001-HRT-003), DTS0747 (for TB-D5001-HRT-004), DTS0781 (for TB-D5001-HRT-005), DTS0803 (for TB-D5001-HRT-006), DTS0850 (for TB-D5001-HRT-007) and the instruction manual ISM0366 (for 5700 installed on TB-D5001-HRT-00x) which contain basic guides for the installation of the equipment.

gmi technology for safety

Application for TB-D5001-HRT-003 with 5700 in connection with G.M. International Termination Board for the remote monitoring of HART®-compatible 4/20 mA field loop signals





Description:

The TB-D5001-HRT-003 Termination Board, with its 5700 modem module and in connection with G.M. International Termination Board, provides remote monitoring of each HART®-compatible 4/20 mA field / signal loop (or channel).

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 also used to supply 5700 module by its TB connector.

There are dedicated RS-485 interface terminals to communicate with the HART® Mux unit or modem. The 5700 unit connects, via the RS-485 interface, to an external PC running an FDT-based software package (PACTware™, etc...) through a dedicated Device Type Manager (DTM) to identify each field device.

Safety Function and Failure behavior:

The TB-D5001-HRT-003 with 5700 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of TB-D5001-HRT-003 with 5700 on each HART®-compatible 4/20 mA field / signal loop (or channel) is described from the following definitions:

- □ Fail-Safe State: it's defined as the 4-20 mA loop current signal going to 0 mA.
- □ Fail Safe: this failure causes the system to go to the defined fail-safe state without a process demand.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process or deviates 4-20mA loop current signal by more than 3% (0.5mA) of full span respect to the correct value.
- □ Fail Dangerous Detected: it's defined as a failure mode that causes the 4-20mA loop current signal to go <4mA or >20mA. Assuming that the application program in the safety logic solver is configured to detect <4mA or >20mA failed signal value and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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. 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	0.05
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.48
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.53**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**215'387 years**
$\lambda_{no\ effect}$ = "No effect" failures	512.31
$\lambda_{not\ part}$ = "Not Part" failures	2586.65
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**3099.49**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**36 years**

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

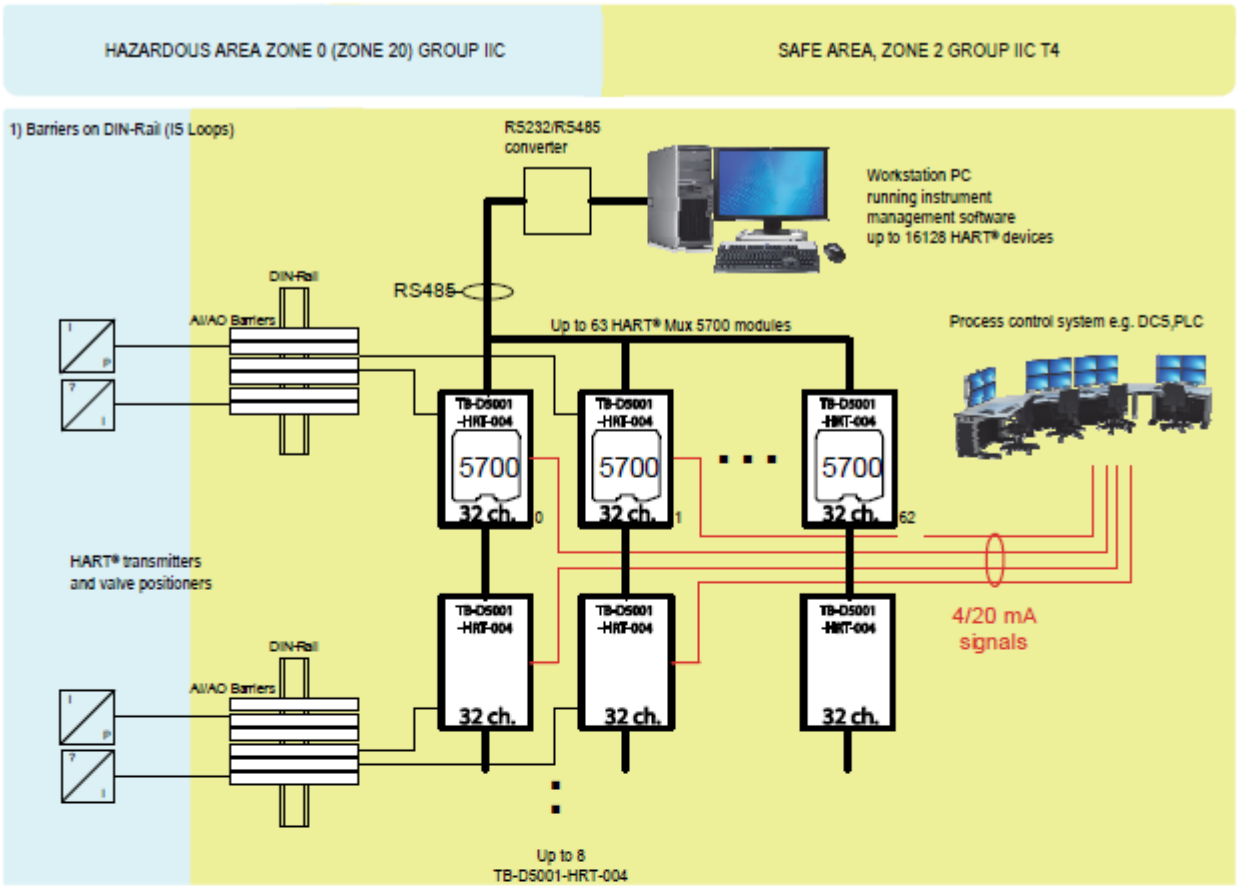
λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.48 FIT	0.00 FIT	0.05 FIT	90.57%

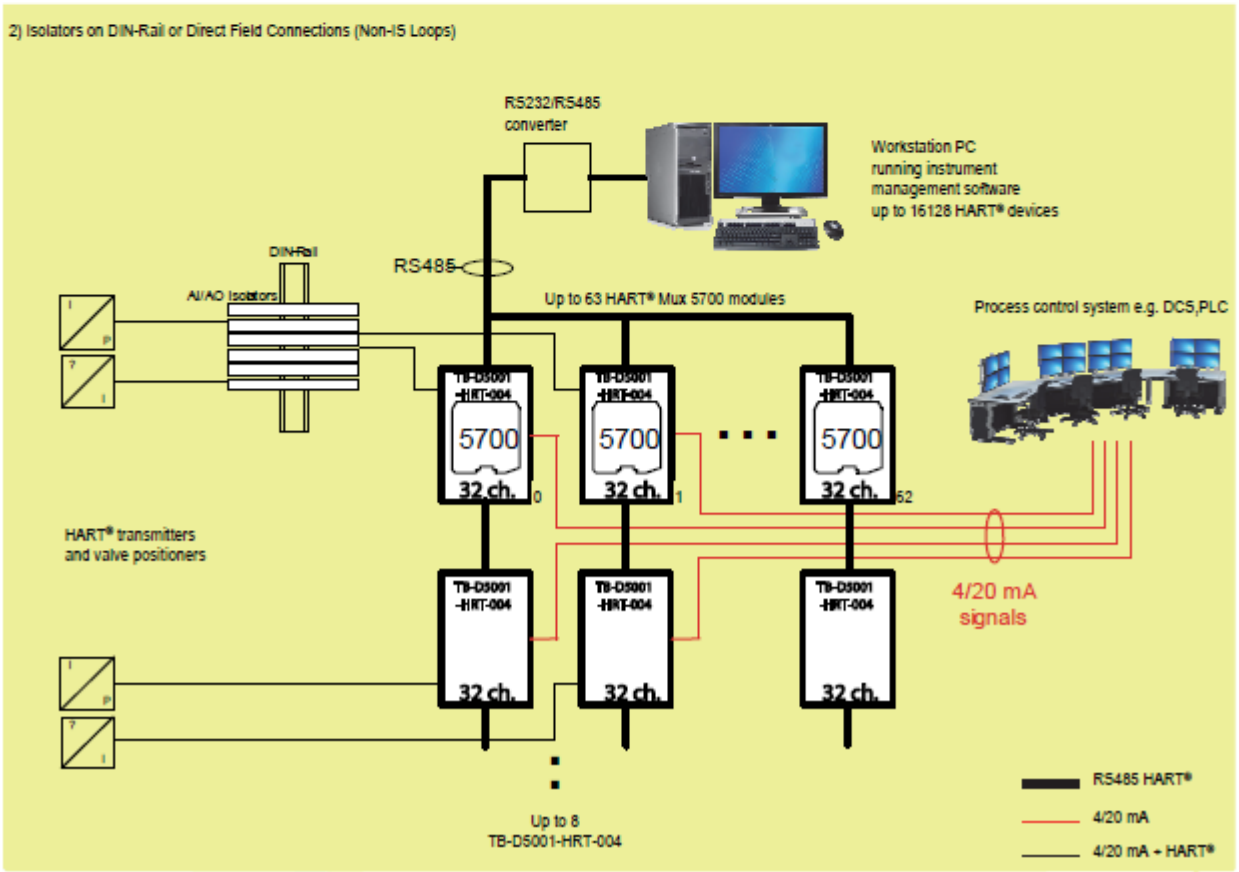
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.19 E-07 - Valid for **SIL 3**	PFDavg = 4.39 E-06 - Valid for **SIL 3**

Systematic capability SIL 3.

Application for TB-D5001-HRT-004 or -006 or -007 with 5700 in connection with AI / AO IS Barriers or Non IS Isolators for the remote monitoring of HART®-compatible 4/20 mA field loop signals





Description:

The TB-D5001-HRT-004 or -006 or -007 Termination Board, with its 5700 modem module and in connection with AI / AO IS Barriers or Non IS Isolators, provides remote monitoring of each HART®-compatible 4/20 mA field / signal loop (or channel). The TB interfaces AI cards of safety PLCs with typical input impedance of 250 Ω (with different value of input impedance included (for -006, -007) or without it (for -004)).

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 also used to supply 5700 module by its TB connector.

There are dedicated RS-485 interface terminals to communicate with the HART® Mux unit or modem. The 5700 unit connects, via the RS-485 interface, to an external PC running an FDT-based software package (PACTware™, etc...) through a dedicated Device Type Manager (DTM) to identify each field device.

Safety Function and Failure behavior:

The TB-D5001-HRT-004 or -006 or -007 with 5700 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of TB-D5001-HRT-004 or -006 or -007 with 5700 on each HART®-compatible 4/20 mA field / signal loop (or channel) is described from the following definitions:

- □ Fail-Safe State: it's defined as the 4-20 mA loop current signal going to 0 mA.
- □ Fail Safe: this failure causes the system to go to the defined fail-safe state without a process demand.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process or deviates 4-20mA loop current signal by more than 3% (0.5mA) of full span respect to the correct value.
- □ Fail Dangerous Detected: it's defined as a failure mode that causes the 4-20mA loop current signal to go <4mA or >20mA. Assuming that the application program in the safety logic solver is configured to detect <4mA or >20mA failed signal value and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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. 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	0.05
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.47
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.52**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**221'660 years**
$\lambda_{no\ effect}$ = "No effect" failures	490.98
$\lambda_{not\ part}$ = "Not Part" failures	999.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**1490.70**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**76 years**

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

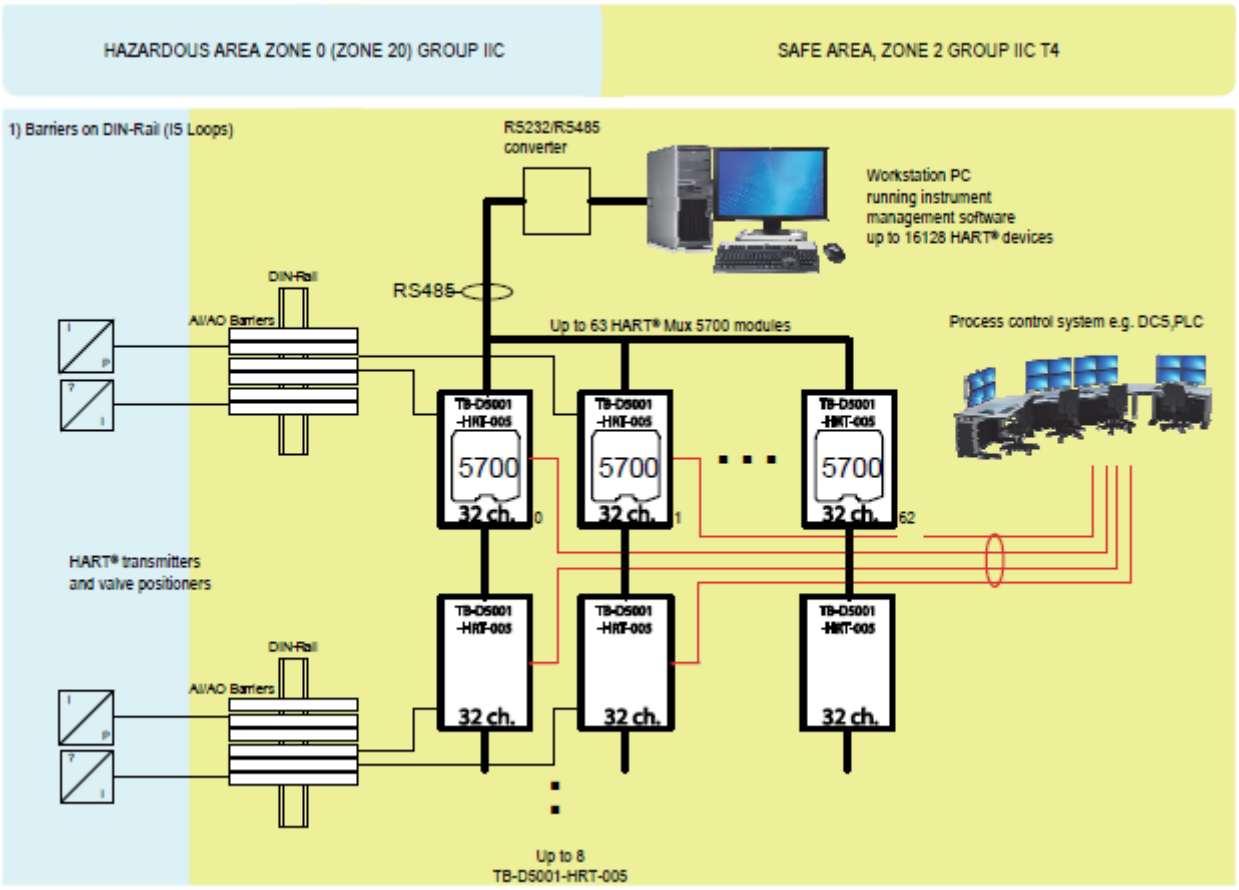
λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.47 FIT	0.00 FIT	0.05 FIT	90.38%

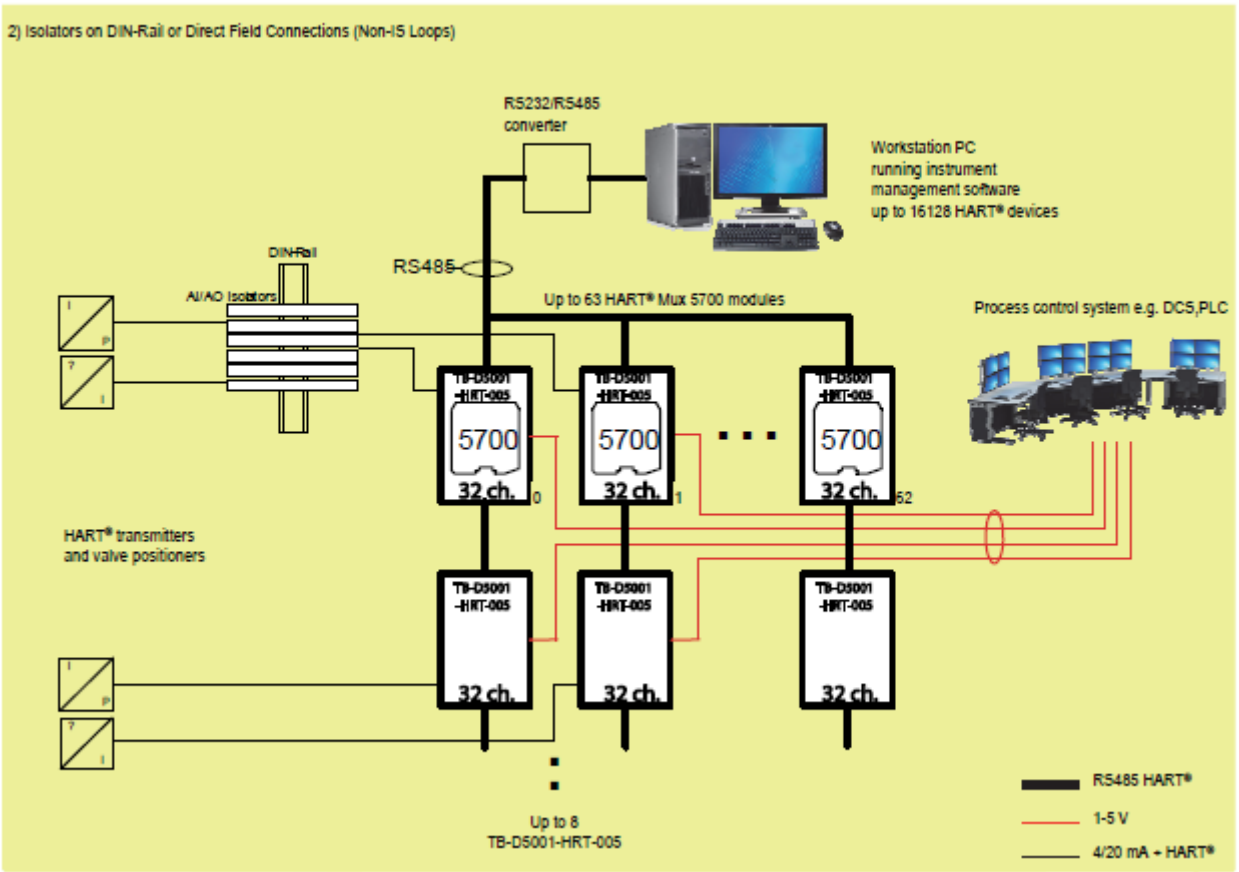
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.19 E-07 - Valid for **SIL 3**	PFDavg = 4.39 E-06 - Valid for **SIL 3**

Systematic capability SIL 3.

Application for TB-D5001-HRT-005 with 5700 in connection with AI / AO IS Barriers or Non IS Isolators for the remote monitoring of HART®-compatible 4/20 mA field loop signals converted into 1/5 V signals by resistors





Description:

The TB-D5001-HRT-005 Termination Board, with its 5700 modem module and in connection with AI / AO IS Barriers or Non IS Isolators, provides remote monitoring of each HART®-compatible 4/20 mA field / signal loop (or channel) converted into 1/5 V by included resistances. The TB interfaces AI (voltage) cards of safety PLCs because the TB includes 1/5 V conversion resistances.

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 also used to supply 5700 module by its TB connector.

There are dedicated RS-485 interface terminals to communicate with the HART® Mux unit or modem. The 5700 unit connects, via the RS-485 interface, to an external PC running an FDT-based software package (PACTware™, etc...) through a dedicated Device Type Manager (DTM) to identify each field device.

Safety Function and Failure behavior:

The TB-D5001-HRT-005 with 5700 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of TB-D5001-HRT-005 with 5700 on each HART®-compatible 4/20 mA field / signal loop (or channel) (with 1/5 V conversion resistances) is described from the following definitions:

- □ Fail-Safe State: it's defined as the 4-20 mA loop current signal converted to 1-5 V voltage signal going to 0 V .
- □ Fail Safe: this failure causes the system to go to the defined fail-safe state without a process demand.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process or deviates 4-20mA loop current signal converted to 1-5 V voltage signal by more than 3% (0.125V) of full span respect to the correct value.
- □ Fail Dangerous Detected: it's defined as a failure mode that causes the 4-20mA loop current signal converted to 1-5 V voltage signal to go <1V or >5V. Assuming that the application program in the safety logic solver is configured to detect <1V or >5V failed signal value and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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. 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	0.12
λ_{du} = Total Dangerous Undetected failures	0.11
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	1.42
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.65**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**69˙395 years**
$\lambda_{no\ effect}$ = "No effect" failures	491.35
$\lambda_{not\ part}$ = "Not Part" failures	1045.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**1538.70**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**74 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	1.42 FIT	0.12 FIT	0.11 FIT	93.33%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 4.84 E-07 - Valid for **SIL 3**	PFDavg = 9.67 E-06 - Valid for **SIL 3**

Systematic capability SIL 3.

Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be detected during proof test on each HART®-compatible 4/20 mA field loop with remote monitoring of the HART® Multiplexer Modem+Termination Board (5700 + TB-D5001-HRT-00x).
The **Proof Test** for TB-D5001-HRT-003, -004, -006, -007 consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, impose on the HART®-compatible 4/20 mA field loop some current values of 4-20 mA range and verify that the input current values read from PLC are within the functional safety specified accuracy (≤ 3%). This implies that the HART® Multiplexer Modem+Termination Board does not interfere with dangerous faults on the 4/20 mA field signal loop during its remote monitoring .
3	Restore the HART®-compatible 4/20 mA field loop to full operation.
4	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the the HART® Multiplexer Modem+Termination Board.

The **Proof Test** for TB-D5001-HRT-005 consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, impose on the HART®-compatible 4/20 mA field loop some current values of 4-20 mA range and verify that the input voltage values (because converted to 1-5 V by resistance on TB) read from PLC are within the functional safety specified accuracy (≤ 3%). This implies that the HART® Multiplexer Modem+Termination Board does not interfere with dangerous faults on the 4/20 mA field signal loop during its remote monitoring .
3	Restore the HART®-compatible 4/20 mA field loop to full operation.
4	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the the HART® Multiplexer Modem+Termination Board.