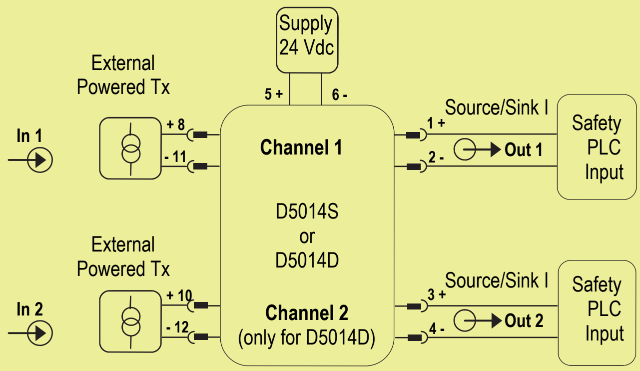
SAFETY MANUAL

SIL 3 Repeater Power Supply
Hart, DIN-Rail and Termination Board,
Models D5014S, D5014D

Reference must be made to the relevant sections within the instruction manual ISM0103, which contain basic guides for the installation of the equipment.

gmi technology for safety

Application for D5014S or D5014D, with active input (external powered Tx)



Description:

For this application, enable 4 - 20 mA Source or Sink mode for ch. 1 or ch. 2, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D5014S)	1	2	3	4
4 - 20 mA Source mode	ON	ON	OFF	OFF
4 - 20 mA Sink mode	OFF	OFF	ON	OFF

Dip-switch position (D5014D)	1	2	3	4	5	6	7	8
4 - 20 mA Source mode ch. 1	ON	ON	OFF	OFF	-	-	-	-
4 - 20 mA Sink mode ch. 1	OFF	OFF	ON	OFF	-	-	-	-
4 - 20 mA Source mode ch.2	-	-	-	-	ON	ON	OFF	OFF
4 - 20 mA Sink mode ch.2	-	-	-	-	OFF	OFF	ON	OFF

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Active input signals from external powered Tx are applied to Pins 8-11 (In 1 - Ch.1) and Pins 10-12 (In 2 - Ch.2).
Source or Sink output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D5014 is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

- □ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
- □ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
- □ fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the safety logic solver is configured to detect Low failure 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 which 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 2 channels of D5014D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D5014S (single channel) are also valid for each channel of D5014D (double channel).
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	146.72
λ_{du} = Total Dangerous Undetected failures	14.97
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**161.69**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**706 years**
$\lambda_{no\ effect}$ = "No Effect" failures	205.11
$\lambda_{not\ part}$ = "Not Part" failures	4.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**371.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**307 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	146.72 FIT	14.97 FIT	90.74%	0%	90.74%

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

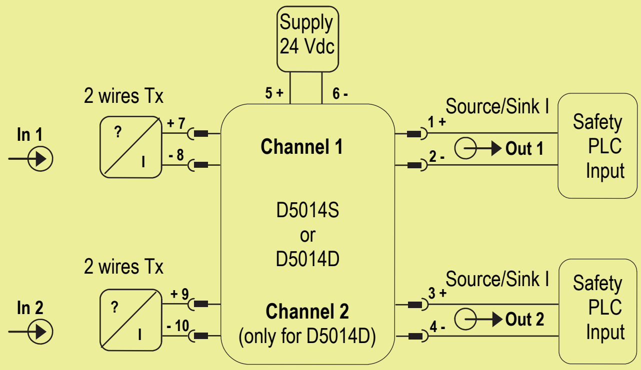
T[Proof] = 1 year	T[Proof] = 14 years
PFDavg = 6.69E-05 Valid for **SIL 3**	PFDavg = 9.37E-04 Valid for **SIL 2**

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] = 10 years	T[Proof] = 20 years
PFDavg = 6.69E-04 Valid for **SIL 3**	PFDavg = 1.34E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Application for D5014S or D5014D, with passive input (2 wires Tx)



Description:

For this application, enable 4 - 20 mA Source or Sink mode for ch. 1 or ch. 2, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D5014S)	1	2	3	4
4 - 20 mA Source mode	ON	ON	OFF	OFF
4 - 20 mA Sink mode	OFF	OFF	ON	OFF

Dip-switch position (D5014D)	1	2	3	4	5	6	7	8
4 - 20 mA Source mode ch. 1	ON	ON	OFF	OFF	-	-	-	-
4 - 20 mA Sink mode ch. 1	OFF	OFF	ON	OFF	-	-	-	-
4 - 20 mA Source mode ch.2	-	-	-	-	ON	ON	OFF	OFF
4 - 20 mA Sink mode ch.2	-	-	-	-	OFF	OFF	ON	OFF

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Passive input signals from 2 wires Tx are applied to Pins 7-8 (In 1 - Ch.1) and Pins 9-10 (In 2 - Ch.2).
Source or Sink output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D5014 is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

- □ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
- □ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
- □ fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the safety logic solver is configured to detect Low failure 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 which 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 2 channels of D5014D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D5014S (single channel) are also valid for each channel of D5014D (double channel).
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	135.30
λ_{du} = Total Dangerous Undetected failures	14.25
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**149.55**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**763 years**
$\lambda_{no\ effect}$ = "No Effect" failures	201.25
$\lambda_{not\ part}$ = "Not Part" failures	20.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**371.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**307 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	135.30 FIT	14.25 FIT	90.47%	0%	90.47%

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

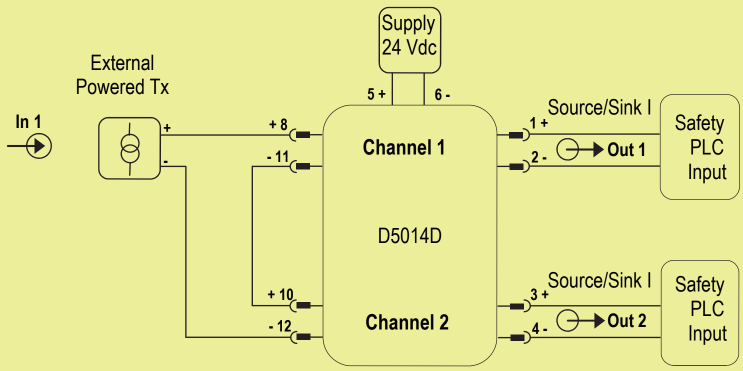
T[Proof] = 1 year	T[Proof] = 15 years
PFDavg = 6.36 E-05 Valid for **SIL 3**	PFDavg = 9.54 E-04 Valid for **SIL 2**

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] = 10 years	T[Proof] = 20 years
PFDavg = 6.36 E-04 Valid for **SIL 3**	PFDavg = 1.27 E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Application for D5014D, duplicator (for external powered Tx) with input loop on two active inputs



Description:

For this application, enable 4 - 20 mA Source or Sink mode for ch. 1 and ch. 2, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D5014D)	1	2	3	4	5	6	7	8
4 - 20 mA Source mode ch. 1	ON	ON	OFF	OFF	-	-	-	-
4 - 20 mA Sink mode ch. 1	OFF	OFF	ON	OFF	-	-	-	-
4 - 20 mA Source mode ch.2	-	-	-	-	ON	ON	OFF	OFF
4 - 20 mA Sink mode ch.2	-	-	-	-	OFF	OFF	ON	OFF

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Active input signal from external powered Tx is applied by input loop to Pins 8-11 (In 1 - Ch.1) and Pins 10-12 (In 2 - Ch.2).
Source or Sink output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D5014D (as duplicator for external powered Tx) is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

- □ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
- □ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
- □ fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the safety logic solver is configured to detect Low failure 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 which 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 date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	146.96
λ_{du} = Total Dangerous Undetected failures	14.97
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**161.93**
MTBF (safety function, one channel of duplicator) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**705 years**
$\lambda_{no\ effect}$ = "No Effect" failures	205.11
$\lambda_{not\ part}$ = "Not Part" failures	376.16
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**743.20**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**153 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	146.96 FIT	14.97 FIT	90.76%	0%	90.76%

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

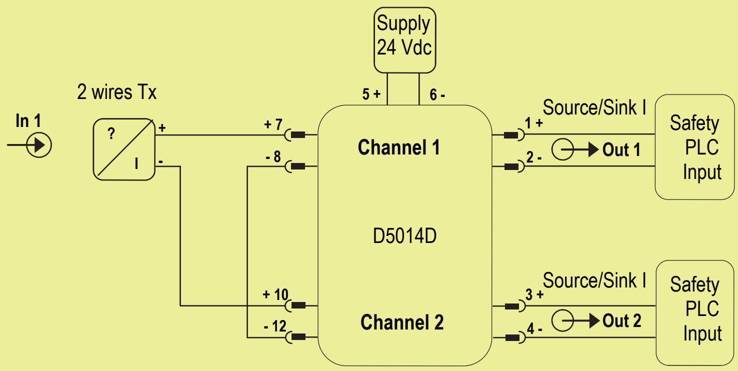
T[Proof] = 1 year	T[Proof] = 14 years
PFDavg = 6.69E-05 Valid for **SIL 3**	PFDavg = 9.37E-04 Valid for **SIL 2**

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] = 10 years	T[Proof] = 20 years
PFDavg = 6.69E-04 Valid for **SIL 3**	PFDavg = 1.34E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Application for D5014D, duplicator (for 2 wires Tx) with input loop on a passive input and an active input



Description:

For this application, enable 4 - 20 mA Source or Sink mode for ch. 1 and ch. 2, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D5014D)	1	2	3	4	5	6	7	8
4 - 20 mA Source mode ch. 1	ON	ON	OFF	OFF	-	-	-	-
4 - 20 mA Sink mode ch. 1	OFF	OFF	ON	OFF	-	-	-	-
4 - 20 mA Source mode ch.2	-	-	-	-	ON	ON	OFF	OFF
4 - 20 mA Sink mode ch.2	-	-	-	-	OFF	OFF	ON	OFF

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Passive input signals from 2 wires Tx is applied by input loop to Pins 7-8 (In 1 - Ch.1 as passive input) and Pins 10-12 (In 2 - Ch.2 as active input).
Source or Sink output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D5014D (as duplicator for 2 wires Tx) is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

- □ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
- □ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
- □ fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the safety logic solver is configured to detect Low failure 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 which 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 date: taken from Siemens Standard SN29500.

<u>Analysis for the Channel 1 with passive input</u>

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	135.54
λ_{du} = Total Dangerous Undetected failures	14.25
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**149.79**
MTBF (safety function, Channel 1 of duplicator) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**762 years**
$\lambda_{no\ effect}$ = “No Effect” failures	201.25
$\lambda_{not\ part}$ = “Not Part” failures	392.16
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**743.20**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**153 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	135.54 FIT	14.25 FIT	90.49%	0%	90.49%

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] = 15 years
PFDavg = 6.36 E-05 Valid for **SIL 3**	PFDavg = 9.54 E-04 Valid for **SIL 2**

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] = 10 years	T[Proof] = 20 years
PFDavg = 6.36 E-04 Valid for **SIL 3**	PFDavg = 1.27 E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Application for D5014D, duplicator (for 2 wires Tx) with input loop on a passive input and an active input

Analysis for the Channel 2 with active input

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	257.76
λ_{du} = Total Dangerous Undetected failures	21.69
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**279.45**
MTBF (safety function, Channel 2 of duplicator) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**408 years**
$\lambda_{no\ effect}$ = "No Effect" failures	339.15
$\lambda_{not\ part}$ = "Not Part" failures	124.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**743.20**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**153 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	257.76 FIT	21.69 FIT	92.24%	0%	92.24%

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] = 10 years
PFDavg = 9.72 E-05 Valid for **SIL 3**	PFDavg = 9.72 E-04 Valid for **SIL 2**

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] = 5 years	T[Proof] = 20 years
PFDavg = 4.86 E-04 Valid for **SIL 3**	PFDavg = 9.72 E-03 Valid for **SIL 2**

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 revealed during proof test. **The Proof test 1** 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, set the transmitter connected to the input of the repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
3	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to low alarm current and verify that the output current of the repeater reaches that value. This tests for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 30 % of possible Dangerous Undetected failures in the repeater.

The **Proof test 2** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the **Proof Test 1**.
3	Perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the input of the repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.
4	Restore the loop to full operation.
5	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 repeater.