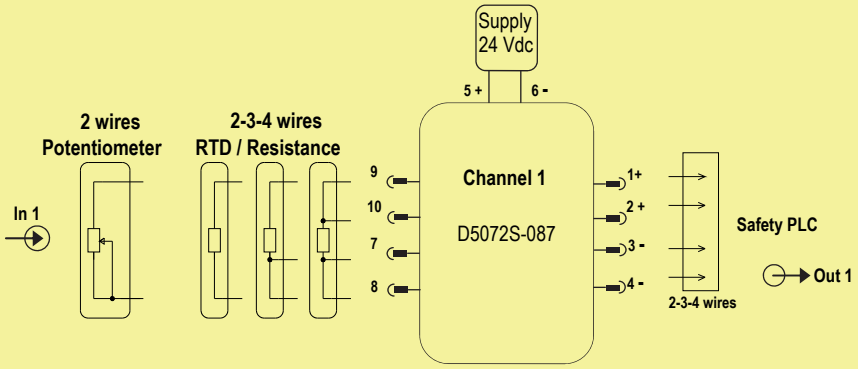
SAFETY MANUAL

SIL 2 Resistance Repeater, DIN-Rail
Models D5072S-087, D5072D-087

Reference must be made to the relevant sections within the instruction manual ISM0178 (for D5072-087) and ISM0154 (for SWC5090 Configuration Software instruction manual), which contain basic guides for the installation and configuration of the equipment.

gmi technology for safety

Application for D5072S-087, with 2-3-4 wires resistance/RTD or 2-wires transmitting potentiometer sensor



Description:
By means of SWC5090 Configuration Software, as user interface on a PC to comunicate with the module, select: Burnout "Active" on Configuration Input 1; Fault cells of "Burnout" and "Input fault" on Configuration Output 1, so that channel output resistance is forced to 450 Ohm in case of fault presence. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) and 6 (- negative). The green LED is lit in presence of supply power. Input sensor (2-3-4 wires resistance/RTD, 2 wires transmitting potentiometer) is applied from Pins 7 to 10 (see instruction manual of the module for more information about input settings). Safety PLC is connected to output wires from Pins 1 to 4.

Safety Function and Failure behavior:
D5072S-087 is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of module is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output resistance going above the maximum resistance value of the input sensor range because of module shutdown. The Safety logic can detect above out of range and convert this High failure to the Fail-Safe state.
- □ Fail Safe: failure mode that causes the module / (sub)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 or deviates the channel output resistance by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output resistance to go above the maximum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect above out of range and it does not automatically trip on high failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Low: failure mode that causes the channel output resistance to go below the minimum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect below out of range and it does not automatically trip on low failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output resistance is forced to 450 Ohm (as Fail High), above 400 Ohm maximum output resistance value in the valid range 0 to 400 Ohm.
- □ 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 is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.
Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	142.26
λ_{du} = Total Dangerous Undetected failures	23.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	121.54
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**286.89**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**397 years**
$\lambda_{no\ effect}$ = "No effect" failures	216.91
$\lambda_{not\ part}$ = "Not Part" failures	30.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**534.50**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**213 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	121.54 FIT	142.26 FIT	23.09 FIT	86.03%	91.95%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits and by Safety logic solver. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 86.03 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

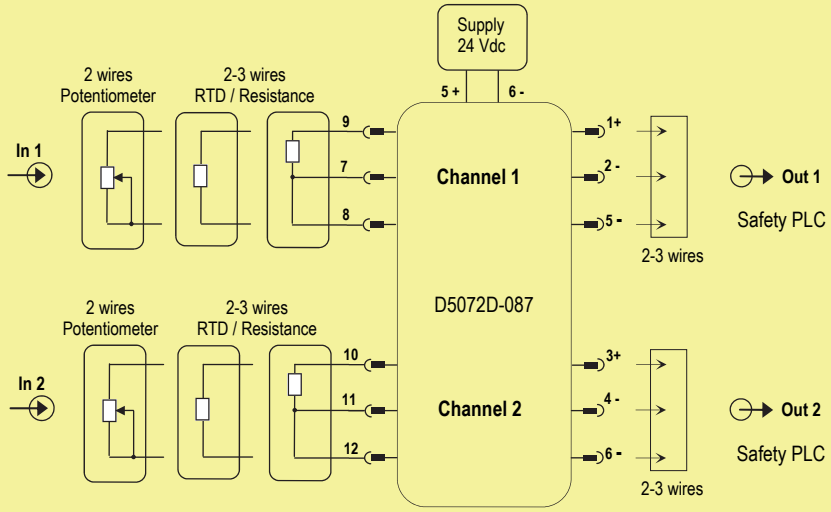
T[Proof] = 1 year	T[Proof] = 9 years
PFDavg = 1.02 E-04 - Valid for **SIL 2**	PFDavg = 9.22 E-04 - Valid for **SIL 2**

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] = 20 years
PFDavg = 2.05 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D5072D-087, with independent channels for 2-3 wires resistance/RTD or 2-wires transmitting potentiometer sensor



Description:
By means of SWC5090 Configuration Software, as user interface on a PC to comunicate with the module, select: Burnout "Active" on Configuration Input 1 and 2; Fault cells of "Burnout" and "Input fault" on Configuration Output 1 and 2, so that channel output resistance is forced to 450 Ohm in case of fault presence. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) and 6 (- negative). The green LED is lit in presence of supply power. Input sensors (2-3 wires resistance/RTD, 2 wires transmitting potentiometer) are applied from Pins 7 to 9 (for channel 1) and from Pins 10 to 12 (for channel 2) (see instruction manual of the module for more information about input settings). Safety PLC is connected to output wires Pins 1, 2 and 5 (for channel 1) and Pins 3, 4 and 6 (for channel 2).

Safety Function and Failure behavior:
D5072D-087 is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of module is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output resistance going above the maximum resistance value of the input sensor range because of module shutdown. The Safety logic can detect above out of range and convert this High failure to the Fail-Safe state.
- □ Fail Safe: failure mode that causes the module / (sub)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 or deviates the channel output resistance by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output resistance to go above the maximum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect above out of range and it does not automatically trip on high failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Low: failure mode that causes the channel output resistance to go below the minimum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect below out of range and it does not automatically trip on low failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output resistance is forced to 450 Ohm (as Fail High), above 400 Ohm maximum output resistance value in the valid range 0 to 400 Ohm.
- □ 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 is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.
Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	162.40
λ_{du} = Total Dangerous Undetected failures	23.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	138.87
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**324.36**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**351 years**
$\lambda_{no\ effect}$ = "No effect" failures	258.04
$\lambda_{not\ part}$ = "Not Part" failures	206.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**788.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**144 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	138.87 FIT	162.40 FIT	23.09 FIT	87.55%	92.88%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits and by Safety logic solver. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 87.55 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

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

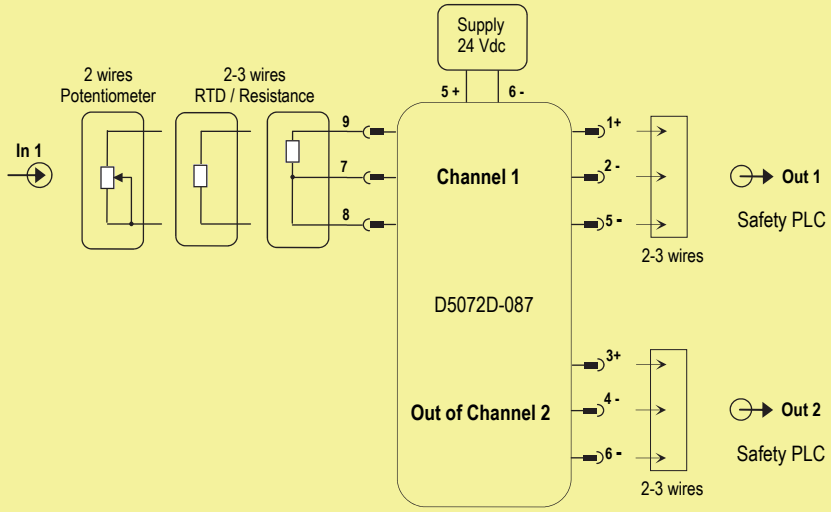
T[Proof] = 1 year	T[Proof] = 9 years
PFDavg = 1.03 E-04 - Valid for **SIL 2**	PFDavg = 9.27 E-04 - Valid for **SIL 2**

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] = 20 years
PFDavg = 2.06 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D5072D-087, as duplicator with one Input and two Outputs, for 2-3 wires resistance/RTD or 2-wires transmitting potentiometer sensor



Description:
By means of SWC5090 Configuration Software, as user interface on a PC to comunicate with the module, select: Burnout "Active" on Configuration Input 1; Fault cells of "Burnout" and "Input fault" on Configuration Output 1, so that channel output resistance is forced to 450 Ohm in case of fault presence; Output duplication cell "Active" on Configuration to enable duplicator configuration where Output 2 is a duplication of Output 1. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) and 6 (- negative). The green LED is lit in presence of supply power. Input sensor (2-3 wires resistance/RTD, 2 wires transmitting potentiometer) is applied from Pins 7 to 9 (for channel 1) (see instruction manual of the module for more information about input settings). Safety PLC is connected to output wires Pins 1, 2 and 5 (for Output 1) and Pins 3, 4 and 6 (for Output 2).

Safety Function and Failure behavior:
D5072D-087 is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of module is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output resistance going above the maximum resistance value of the input sensor range because of module shutdown. The Safety logic can detect above out of range and convert this High failure to the Fail-Safe state.
- □ Fail Safe: failure mode that causes the module / (sub)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 or deviates the channel output resistance by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output resistance to go above the maximum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect above out of range and it does not automatically trip on high failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Low: failure mode that causes the channel output resistance to go below the minimum resistance value of the input sensor range. Assuming that the application program in the Safety logic solver is configured to detect below out of range and it does not automatically trip on low failure, this failure has been classified as a dangerous failure (DD) detected by logic solver.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output resistance is forced to 450 Ohm (as Fail High), above 400 Ohm maximum output resistance value in the valid range 0 to 400 Ohm.
- □ 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 is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.
Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	162.40
λ_{du} = Total Dangerous Undetected failures	23.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	138.87
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**324.36**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**351 years**
$\lambda_{no\ effect}$ = "No effect" failures	258.04
$\lambda_{not\ part}$ = "Not Part" failures	206.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**788.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**144 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	138.87 FIT	162.40 FIT	23.09 FIT	87.55%	92.88%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits and by Safety logic solver. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 87.55 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

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] = 9 years
PFDavg = 1.03 E-04 - Valid for **SIL 2**	PFDavg = 9.27 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] = 20 years
PFDavg = 2.06 E-03 - Valid for **SIL 2**

SC 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 faults, which have been noted during the FMEDA, can be revealed during the proof test.

Proof test (to reveal approximately 99 % of possible Dangerous Undetected failures in the resistance repeater)	
Steps	**Action**
1	Bypass the Safety-related PLC or take any other appropriate action to avoid a false trip.
2	Connect a resistive decade to the input terminals (‘7’-‘8’-‘9’-‘10’ for single channel; ‘7’-‘8’-‘9’ or ‘10’-‘11’-‘12’ for channel 1 or channel 2 of double channel), according to the different input sensor allowed configurations (2, 3 wires resistance for single and double channel; 4 wire resistance for only single channel), and an ohmmeter to the output terminals (‘1’/’2’ - ‘3’/’4’ for single channel; ‘1’-‘2’/’5’ or ‘3’-‘4’/’6’ for channel 1 or channel 2 of double channel). Change the input resistance value within the 0 to 400 Ω range and check that the measured output resistance value is deviated by less than 3% respect to the input. This test detects any dangerous failure in the resistance repeater.
3	Restore the loop to full operation.
4	Remove the bypass from the safety-related PLC or otherwise restore normal operation.