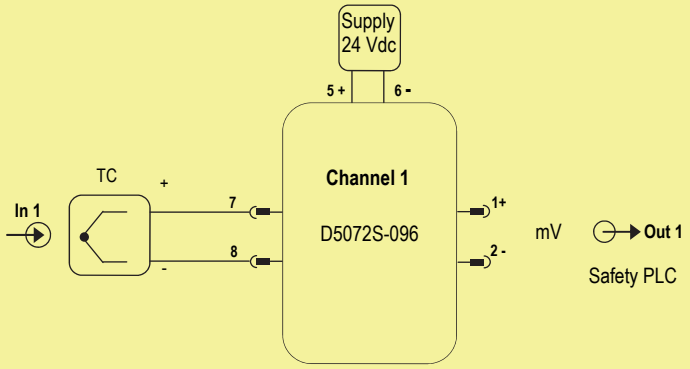
SAFETY MANUAL

SIL 2 Thermocouple/mV Repeater, DIN-Rail
Models D5072S-096, D5072D-096

Reference must be made to the relevant sections within the instruction manual ISM0388 (for D5072-096)
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-096



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 mV signal is forced to 110 mV 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 (Thermocouple) is applied to Pins 7 - 8 (see instruction manual of the module for more information about input settings). Safety PLC is connected to channel output Pins 1 - 2.

Safety Function and Failure behavior:
D5072S-096 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 mV signal to go above the maximum mV value of the input thermocouple range. 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 mV signal by more than 3% of the correct value or the output signal is 0 mV .
- □ Fail Low: failure mode that causes the channel output mV signal to go below the minimum mV value of the input thermocouple 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 value is forced to 110 mV (as Fail High), above 100 mV maximum output value in the valid range -10 to 100 mV .
- □ 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	171.16
λ_{du} = Total Dangerous Undetected failures	103.62
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	15.67
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**290.45**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**393 years**
$\lambda_{no\ effect}$ = "No effect" failures	211.95
$\lambda_{not\ part}$ = "Not Part" failures	30.90
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**533.30**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**214 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	15.67 FIT	171.16 FIT	103.62 FIT	62.29%	64.32%

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 = 62.29 % ≥ 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:

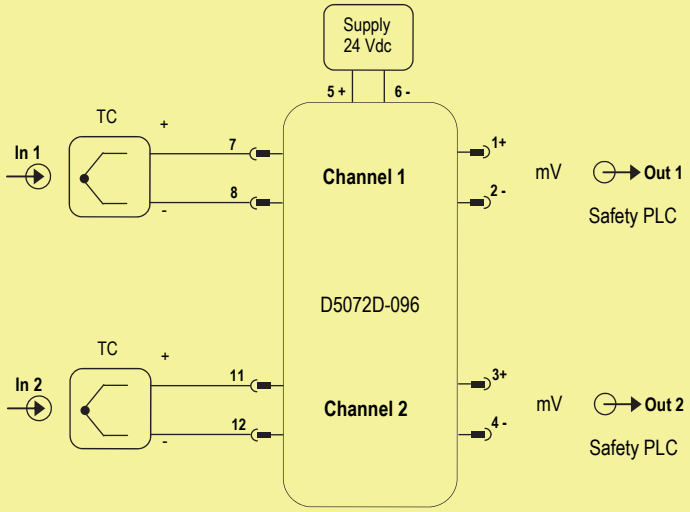
T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 4.56 E-04 - Valid for **SIL 2**	PFDavg = 9.12 E-04 - Valid for **SIL 2**	PFDavg = 9.12 E-03 - Valid for **SIL 1**

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 = 2.28 E-03 - Valid for **SIL 2**	PFDavg = 9.12 E-03 - Valid for **SIL 1**

SC 3: Systematic capability SIL 3.

Application for D5072D-096, with independent channels



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 mV signal is forced to 110 mV 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 (Thermocouple) are applied to Pins 7 - 8 (for channel 1) and to Pins 11 - 12 (for channel 2) (see instruction manual of the module for more information about input settings). Safety PLC is connected to output Pins 1 - 2 (for channel 1) and Pins 3 - 4 (for channel 2).

Safety Function and Failure behavior:
D5072D-096 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 mV signal to go above the maximum mV value of the input thermocouple range. 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 mV signal by more than 3% of the correct value or the output signal is 0 mV .
- □ Fail Low: failure mode that causes the channel output mV signal to go below the minimum mV value of the input thermocouple 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 value is forced to 110 mV (as Fail High), above 100 mV maximum output value in the valid range -10 to 100 mV .
- □ 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	191.28
λ_{du} = Total Dangerous Undetected failures	108.12
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	15.67
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**315.07**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**362 years**
$\lambda_{no\ effect}$ = "No effect" failures	237.93
$\lambda_{not\ part}$ = "Not Part" failures	236.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**789.40**
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	15.67 FIT	191.28 FIT	108.12 FIT	63.89%	65.68%

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 = 63.89 % ≥ 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:

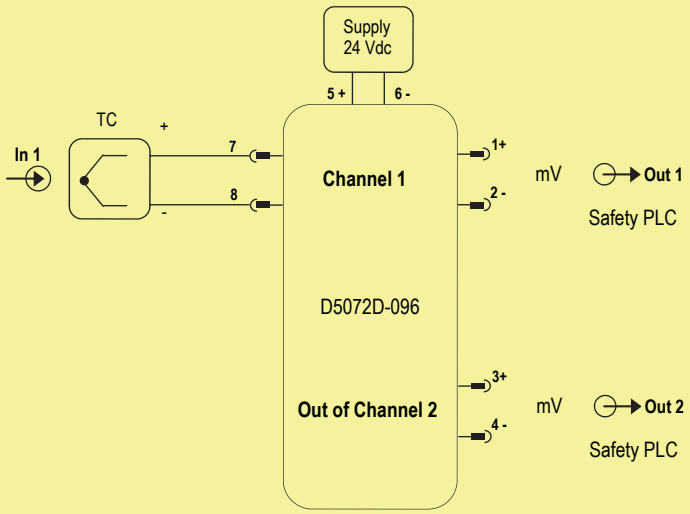
T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 4.76 E-04 - Valid for **SIL 2**	PFDavg = 9.52 E-04 - Valid for **SIL 2**	PFDavg = 9.52 E-03 - Valid for **SIL 1**

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 = 2.38 E-03 - Valid for **SIL 2**	PFDavg = 9.52 E-03 - Valid for **SIL 1**

SC 3: Systematic capability SIL 3.

Application for D5072D-096, as duplicator with one Input and two Outputs



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 mV signal is forced to 110 mV 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 sensors (Thermocouple) are applied to Pins 7 - 8 (for channel 1) and to Pins 11 - 12 (for channel 2) (see instruction manual of the module for more information about input settings). Safety PLC is connected to output Pins 1 - 2 (for channel 1) and Pins 3 - 4 (for channel 2).

Safety Function and Failure behavior:
D5072D-096 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 mV signal to go above the maximum mV value of the input thermocouple range. 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 mV signal by more than 3% of the correct value or the output signal is 0 mV .
- □ Fail Low: failure mode that causes the channel output mV signal to go below the minimum mV value of the input thermocouple 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 value is forced to 110 mV (as Fail High), above 100 mV maximum output value in the valid range -10 to 100 mV .
- □ 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	191.28
λ_{du} = Total Dangerous Undetected failures	108.12
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	15.67
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**315.07**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**362 years**
$\lambda_{no\ effect}$ = "No effect" failures	237.93
$\lambda_{not\ part}$ = "Not Part" failures	236.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**789.40**
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	15.67 FIT	191.28 FIT	108.12 FIT	63.89%	65.68%

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 = 63.89 % ≥ 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] = 2 years	T[Proof] = 20 years
PFDavg = 4.76 E-04 - Valid for **SIL 2**	PFDavg = 9.52 E-04 - Valid for **SIL 2**	PFDavg = 9.52 E-03 - Valid for **SIL 1**

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 = 2.38 E-03 - Valid for **SIL 2**	PFDavg = 9.52 E-03 - Valid for **SIL 1**

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 Thermocouple / mV repeater)	
Steps	**Action**
1	Bypass the Safety-related PLC or take any other appropriate action to avoid a false trip.
2	Connect mV signal generator to the input terminals ('7'-'8' for single channel; '7'-'8' or '11'-'12' for channel 1 or channel 2 of double channel) and a voltmeter the output terminals ('1'-'2' for single channel; '1'-'2' or '3'-'4' for channel 1 or channel 2 of double channel). Change the input signal value within the -10 to +100 mV range and check that the measured output voltage value is deviated by less than 3% respect to the input. This test detects any dangerous failure in the Thermocouple/mV repeater .
3	Restore the loop to full operation.
4	Remove the bypass from the safety-related PLC or otherwise restore normal operation.