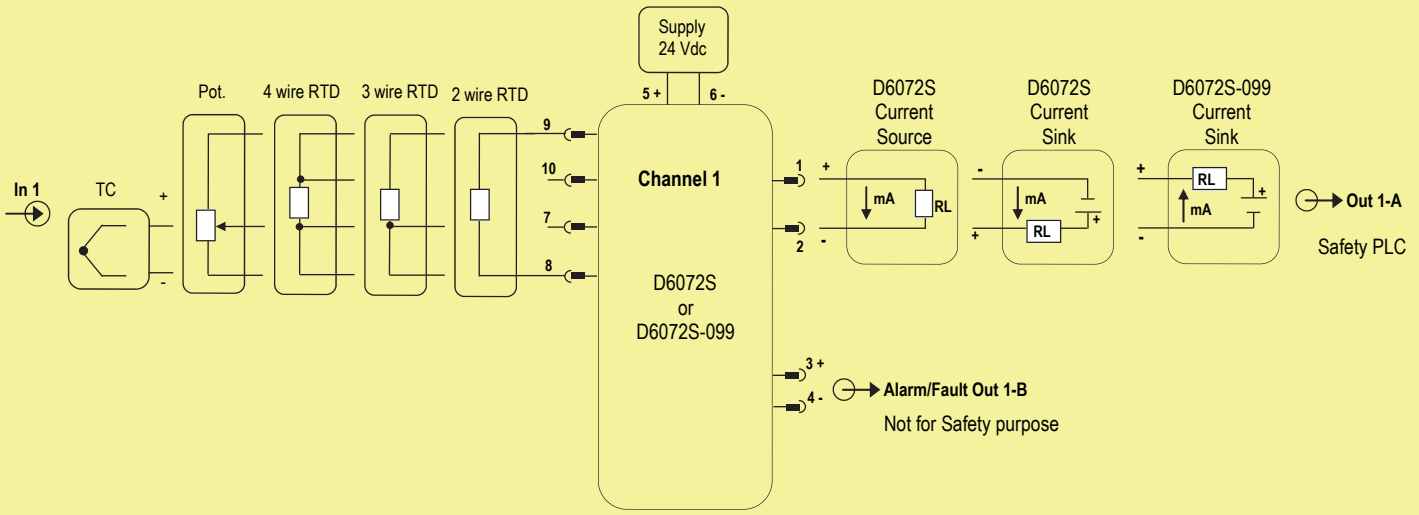
SAFETY MANUAL

SIL 2 Multifunction Temperature Converter
Models D6072S, D6072D and
SIL 2 Multifunction Sink-Out Temperature Converter
Models D6072S-099, D6072D-099
DIN-Rail and Termination Board

Reference must be made to the relevant sections within the instruction manual ISM0216 (for D6072) and ISM0438 (for D6072-099)
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 D6072S or D6072S-099 , with 4-20 mA Analog Current Output



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; Drive "Source" (only for D6072S) or "Sink" on Configuration Output 1; Type "4-20 mA Low" or "4-20 mA High" or "4-20 mA NE43 Low" or "4-20 mA NE43 High" or "Custom Scale (with equivalent Down/Up scale, Under/Over range and Fault output value as previous Types)" on Configuration Output 1; Fault cells of "Burnout", "Input fault" and "Sensor out of specification" on Configuration Output 1, so that analog output is forced to Fault output value < 4mA or > 20mA 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, RTD, Potentiometer) is applied from Pins 7 to 10 (see instruction manual of the module for more information about input settings). Source (only for D6072S) or Sink output current is applied to Pins 1-2.
Alarm/Fault Output is only used for service purpose (not for Safety purpose) and it is applied to Pins 3-4.

Safety Function and Failure behavior:
D6072S or D6072S-099 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 (only the 4 - 20 mA current Source/Sink output configuration is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output going to 0 mA due to module shutdown.
- □ 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 current by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user > 20 mA. Assuming that the application program in the Safety logic solver is configured to detect High failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Low: failure mode that causes the channel output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user < 4 mA. Assuming that the application program in the Safety logic solver is configured to detect Low failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output signal is forced below the minimum output current < 4mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).
- □ 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	153.16
λ_{du} = Total Dangerous Undetected failures	22.35
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	107.70
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**283.21**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**403 years**
$\lambda_{no\ effect}$ = "No effect" failures	198.39
$\lambda_{not\ part}$ = "Not Part" failures	86.30
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**567.90**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**201 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	107.70 FIT	153.16 FIT	22.35 FIT	87.26%	92.11%

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 = 87.26 % ≥ 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:

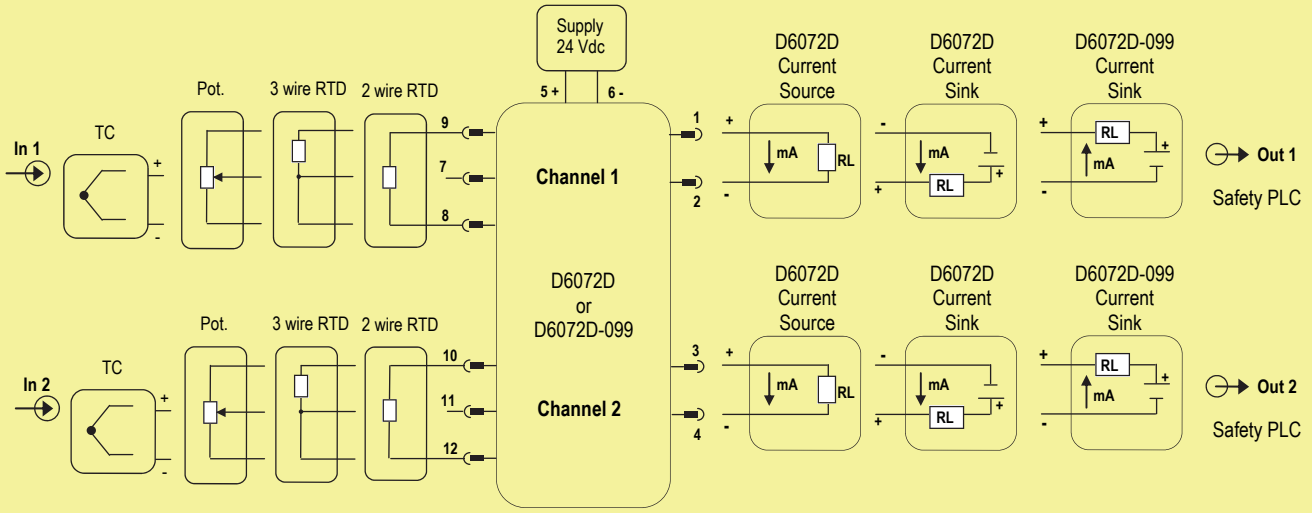
T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.93 E-05 - Valid for **SIL 2**	PFDavg = 9.93 E-04 - Valid for **SIL 2**

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 = 1.99 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D6072D or D6072D-099 , with independent channels and 4-20 mA Analog Current 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 and 2; Drive "Source" (only for D6072D) or "Sink" on Configuration Output 1 and 2; Type "4-20 mA Low" or "4-20 mA High" or "4-20 mA NE43 Low" or "4-20 mA NE43 High" or "Custom Scale (with equivalent Down/Up scale, Under/Over range and Fault output value as previous Types)" on Configuration Output 1 and 2; Fault cells of "Burnout", "Input fault" and "Sensor out of specification" on Configuration Output 1 and 2, so that analog output is forced to Fault output value < 4mA or > 20mA 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, RTD, 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). Source (only for D6072D) or Sink output currents are applied to Pins 1-2 (for channel 1) and to Pins 3-4 (for channel 2).

Safety Function and Failure behavior:
D6072D or D6072D-099 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 (only the 4 - 20 mA current Source/Sink output configuration is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output going to 0 mA due to module shutdown.
- □ 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 current by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user > 20 mA. Assuming that the application program in the Safety logic solver is configured to detect High failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Low: failure mode that causes the channel output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user < 4 mA. Assuming that the application program in the Safety logic solver is configured to detect Low failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output signal is forced below the minimum output current < 4mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).
- □ 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	173.30
λ_{du} = Total Dangerous Undetected failures	22.35
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	121.35
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**317.00**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**360 years**
$\lambda_{no\ effect}$ = "No effect" failures	238.80
$\lambda_{not\ part}$ = "Not Part" failures	242.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**798.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**142 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	121.35 FIT	173.30 FIT	22.35 FIT	88.58%	92.95%

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 = 88.58 % ≥ 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:

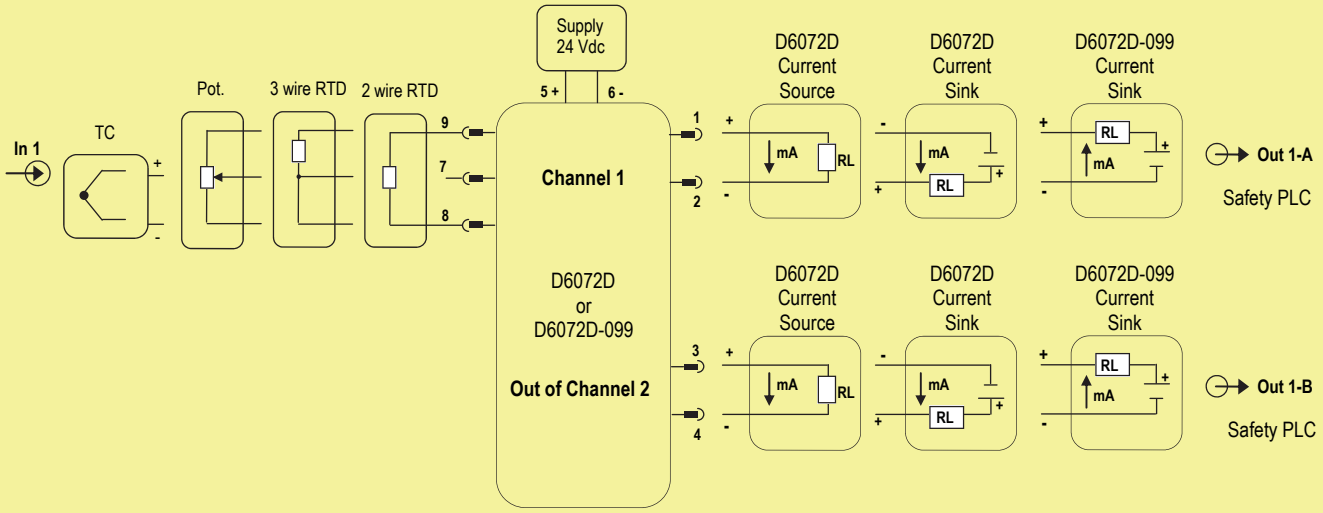
T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.95 E-05 - Valid for **SIL 2**	PFDavg = 9.95 E-04 - Valid for **SIL 2**

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 = 1.99 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D6072D or D6072D-099 , as duplicator with one Input and two 4-20 mA Analog Current 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; the same input sensor (Input 1 related) for the "Function" on Configuration Output 1 and 2; Drive "Source" (only for D6072D) or "Sink" on Configuration Output 1 and 2; Type "4-20 mA Low" or "4-20 mA High" or "4-20 mA NE43 Low" or "4-20 mA NE43 High" or "Custom Scale (with equivalent Down/Up scale, Under/Over range and Fault output value as previous Types)" on Configuration Output 1 and 2; Fault cells of "Burnout", "Input fault" and "Sensor out of specification" on Configuration Output 1 and 2, so that analog output is forced to Fault output value < 4mA or > 20mA 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, RTD, Potentiometer) is applied from Pins 7 to 9 (only for channel 1) (see instruction manual of the module for more information about input settings). Source (only for D6072D) or Sink output currents are applied to Pins 1-2 (for channel 1) and to Pins 3-4 (for channel 2).

Safety Function and Failure behavior:
D6072D or D6072D-099 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 (only the 4 - 20 mA current Source/Sink output configuration is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: is defined as the channel output going to 0 mA due to module shutdown.
- □ 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 current by more than 3% of the correct value.
- □ Fail High: failure mode that causes the channel output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user > 20 mA. Assuming that the application program in the Safety logic solver is configured to detect High failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Low: failure mode that causes the channel output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user < 4 mA. Assuming that the application program in the Safety logic solver is configured to detect Low failures, they have been classified as Dangerous Detected (DD) failures.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that channel output signal is forced below the minimum output current < 4mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).
- □ 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	173.30
λ_{du} = Total Dangerous Undetected failures	22.35
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	121.35
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**317.00**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**360 years**
$\lambda_{no\ effect}$ = "No effect" failures	238.80
$\lambda_{not\ part}$ = "Not Part" failures	242.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**798.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**142 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	121.35 FIT	173.30 FIT	22.35 FIT	88.58%	92.95%

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 = 88.58 % ≥ 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:

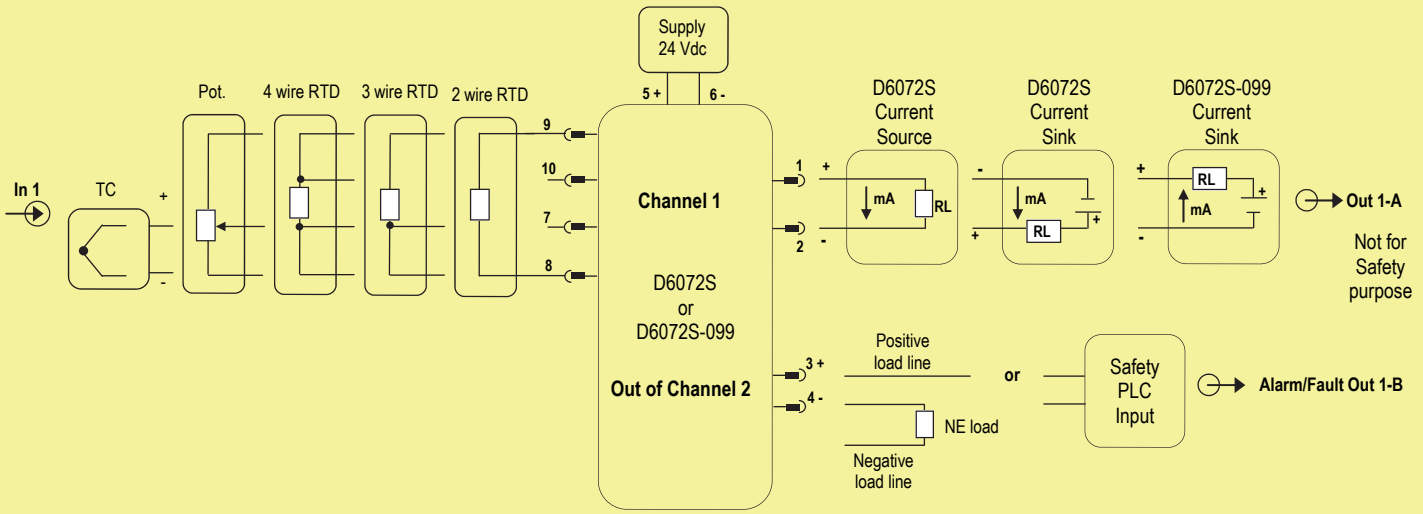
T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.95 E-05 - Valid for **SIL 2**	PFDavg = 9.95 E-04 - Valid for **SIL 2**

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 = 1.99 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D6072S or D6072S-099 , with Alarm Output



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; Type "Low" or "High" or "Window" or "Fault Repeater" on Configuration Alarm; Function "Temp 1" or "Value 1" on Configuration Alarm; Contact position in alarm "Open" on Configuration Alarm; impose Low Set and Low Hysteresys values if Type "Low" or "Window" have been chosen on Configuration Alarm, OR impose High Set and High Hysteresys values if Type "High" or "Window" have been chosen on Configuration Alarm; In case of fault "Alarm Active" if Type "Fault Repeater" have been chosen on Configuration Alarm; Fault cells of "Burnout", "Input fault" and "Sensor out of specification" if Type "Fault Repeater" have been chosen on Configuration Alarm. 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, RTD, Potentiometer) is applied from Pins 7 to 10 (see instruction manual of the module for more information about input settings). Alarm/Fault Output is applied to Pins 3-4, with possible connection to Normally Energized (NE) load or to Safety PLC input. Source (only for D6072S) or Sink output current is only used for service purpose (not for Safety purpose) and it is applied to Pins 1-2.

Safety Function and Failure behavior:
D6072S or D6072S-099 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 (only the alarm on 2nd channel output is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: is defined as the alarm output being de-energized, with open contact (the user can program the trip point value, according to the input measured value, at which the alarm output must be de-energized) .
- □ 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 leads to a measurement error more than 3% of the correct value and therefore has the potential not to respond to a demand from the process, so that the alarm output remains energized with closed contact.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that alarm output is forced to be de-energized (that is to Fail-Safe state), with open contact .
- □ 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	114.44
λ_{du} = Total Dangerous Undetected failures	22.89
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	128.53
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**265.86**
MTBF (safety function, alarm channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**429 years**
$\lambda_{no\ effect}$ = "No effect" failures	187.94
$\lambda_{not\ part}$ = "Not Part" failures	114.10
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**567.90**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**201 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	114.44 FIT	128.53 FIT	22.89 FIT	84.88%	91.39%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 84.88 % ≥ 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:

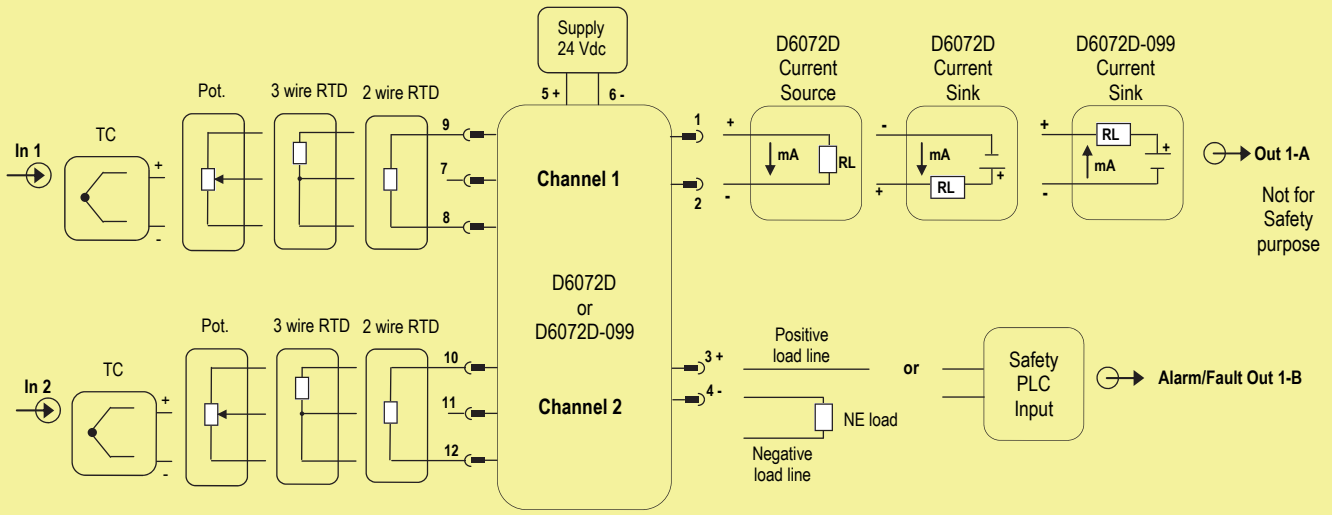
T[Proof] = 1 year	T[Proof] = 9 years
PFDavg = 1.01 E-04 - Valid for **SIL 2**	PFDavg = 9.13 E-04 - Valid for **SIL 2**

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 = 2.03 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Application for D6072D or D6072D-099 , with Alarm Output



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; Type "Low" or "High" or "Window" or "Fault Repeater" on Configuration Alarm; Function "Temp 1 or 2" or "Temp 1 - 2 or 2 - 1" or "Temp mean" or "Minimum" or "Maximum" or "Value 1 or 2" on Configuration Alarm; Contact position in alarm "Open" on Configuration Alarm; impose Low Set and Low Hysteresys values if Type "Low" or "Window" have been chosen on Configuration Alarm, OR impose High Set and High Hysteresys values if Type "High" or "Window" have been chosen on Configuration Alarm; In case of fault "Alarm Active" if Type "Fault Repeater" have been chosen on Configuration Alarm; Fault cells of "Burnout", "Input fault" and "Sensor out of specification" if Type "Fault Repeater" have been chosen on Configuration Alarm. 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, RTD, 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). Alarm/Fault Output is applied to Pins 3-4, with possible connection to Normally Energized (NE) load or to Safety PLC input. Source (only for D6072D) or Sink output current is only used for service purpose (not for Safety purpose) and it is applied to Pins 1-2.

Safety Function and Failure behavior:
D6072D or D6072D-099 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 (only the alarm on 2nd channel output is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: is defined as the alarm output being de-energized, with open contact (the user can program the trip point value, according to the input measured value, at which the alarm output must be de-energized) .
- □ 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 leads to a measurement error more than 3% of the correct value and therefore has the potential not to respond to a demand from the process, so that the alarm output remains energized with closed contact.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that alarm output is forced to be de-energized (that is to Fail-Safe state), with open contact .
- □ 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	134.58
λ_{du} = Total Dangerous Undetected failures	23.89
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	146.81
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**305.28**
MTBF (safety function, alarm channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**373 years**
$\lambda_{no\ effect}$ = "No effect" failures	235.12
$\lambda_{not\ part}$ = "Not Part" failures	258.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**798.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**142 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	146.81 FIT	134.58 FIT	23.89 FIT	84.92%	92.17%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 84.92 % ≥ 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 = 1.06 E-04 - Valid for **SIL 2**	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] = 20 years
PFDavg = 2.12 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.
The test on **D6072S, D6072D or D6072S-099, D6072D-099 for Analog Current output** consists of the following steps:

Proof test 1 (to reveal 50 % of possible Dangerous Undetected failures)	
Steps	**Action**
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Connect a mV signal generator (in order to give an equivalent thermocouple signal) to the input terminals ('7'-'8' for single channel; '7'-'8' or '11'-'12' for channel 1 or channel 2 of double channel) of the temperature converter.
3	For each channel, force an input signal value to go module current output to full scale value and verify that the analog current reaches that value. This tests is for voltage compliance problems, such as low supply voltage or increased wiring resistance, and for other possible failures.
4	For each channel, force an input signal value to go module current output to low scale value and verify that the analog current reaches that value. This tests is for possible quiescent current related failures.
5	Restore the loop to full operation.
6	Remove the bypass from the Safety-related PLC or restore normal operation.

Proof test 2 (to reveal 99 % of possible Dangerous Undetected failures)	
Steps	**Action**
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Perform steps 2, 3 and 4 of **Proof Test 1**.
3	For each channel, force some input signal values, verifying that the module output current related values are within the specified accuracy (3% of the correct value) as defined in the Safety Function.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety-related PLC or restore normal operation.

The test on **D6072S, D6072D or D6072S-099, D6072D-099 for Alarm output** consists of the following steps:

Proof test (to reveal 99 % of possible Dangerous Undetected failures)	
Steps	**Action**
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Connect a mV signal generator (in order to give an equivalent thermocouple signal) to the input terminals ('7'-'8' for single channel; '7'-'8' or '11'-'12' for channel 1 or channel 2 of double channel) of the temperature converter.
3	According to Alarm Function setting, force an input signal value bigger than high limit for alarm tripping and verify that the photo MOS alarm on the 2nd channel output (terminals '3'-'4') is open because alarm output change from normally energize state to de-energize to trip state.
4	According to Alarm Function setting, force an input signal value smaller than low limit for alarm tripping and verify that the photo MOS alarm on the 2nd channel output (terminals '3'-'4') is open because alarm output change from normally energize state to de-energize to trip state.
5	Restore the loop to full operation.
6	Remove the bypass from the Safety-related PLC or restore normal operation.