SAFETY MANUAL

I.S. SIL 2 Temperature Trip Amplifier with Zero/Span Trimmers DIN-Rail

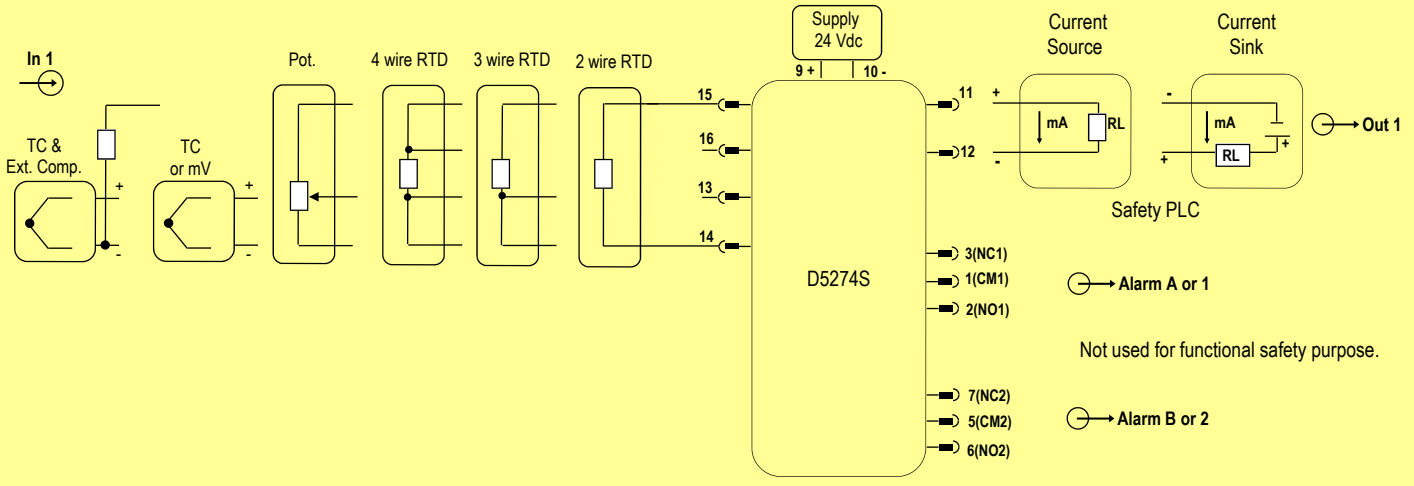
Model D5274S

Approval: TÜV Certificate No. TUV IT 26 SIL xxxx A, SIL 2 conforms to IEC61508:2010 Ed.2 .
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Reference must be made to the relevant sections within the instruction manual ISM0661 and ISM0154 (for SWC5090 Configuration Software instruction manual), which contain basic guides for the installation and configuration of the equipment.

gmi technology for safety

1) Application for D5274S with 4-20 mA Analog Current Output (source or sink mode)



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" 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; in case of "Burnout" analog output is forced to Fault output value (< 4mA or > 20mA); *on Configuration Output 1* ***"Output trimmers enable"*** *cell must be DISABLED because this option must NOT BE USED in Functional Safety application*. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) and 10 (- negative). The green LED is lit in presence of supply power. Input sensor (mV or Thermocouple with or without external compensator, RTD, Potentiometer) is applied from Pins 13 to 16 (see instruction manual of the module for more information about input settings) and related settings must be chosen on Configuration Input 1 of SWC5090 Configuration Software. Source or Sink output current is applied to Pins 11-12.
Alarm A or 1 (Pins 1-2-3) and Alarm B or 2 (Pins 5-6-7) Outputs are only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:
D5274S 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: it is defined as the analog 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 output current by more than 5% (= 1 mA) of full scale range (= 20 mA) respect to the correct value.
- □ Fail High: failure mode that causes the analog output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user and in this analysis the output upscale has been set to 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 analog output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user and in this analysis the output downscale has been set to 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 analog output signal is forced below the minimum output current < 4 mA (as Fail Low) or above the maximum output current > 20 mA (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	142.28
λ_{du} = Total Dangerous Undetected failures	29.21
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	162.23
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**333.72**
MTBF (safety function, analog channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**342 years**
$\lambda_{no\ effect}$ = "No effect" failures	372.57
$\lambda_{not\ part}$ = "Not Part" failures	260.30
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**966.59**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**118 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	162.23 FIT	142.28 FIT	29.21 FIT	82.97%	91.25%

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 = 82.97 % ≥ 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:

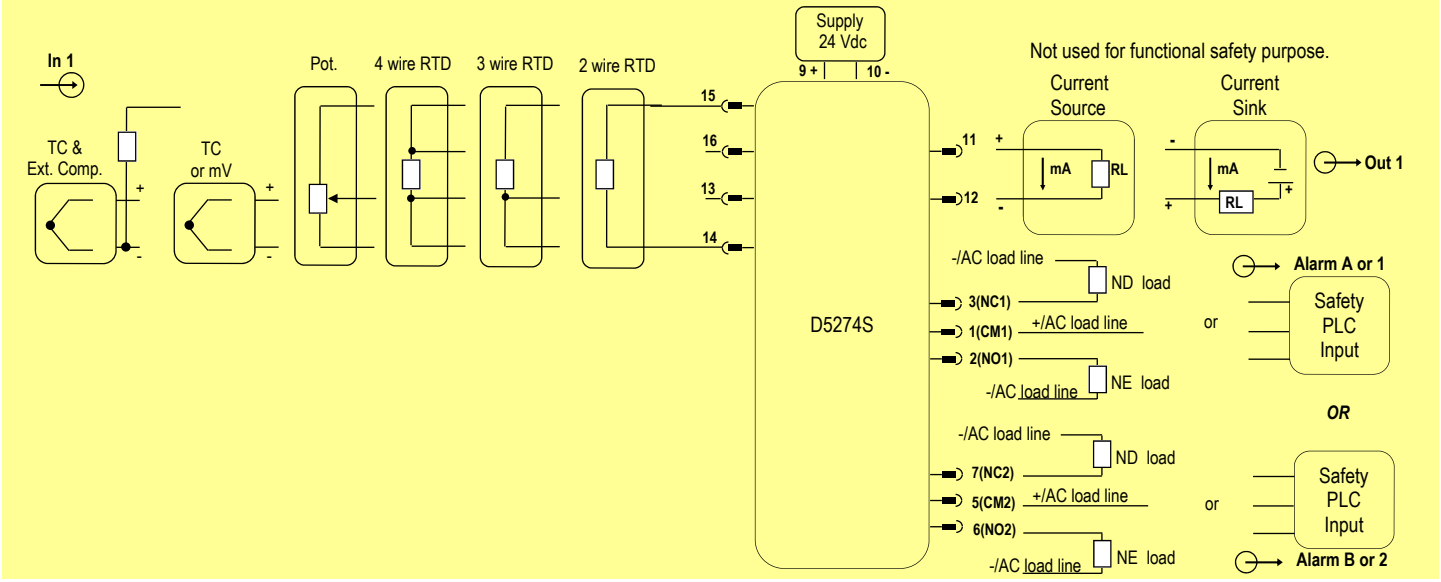
T[Proof] = 1 year	T[Proof] = 7.5 years
PFDavg = 1.29 E-04 - Valid for **SIL 2**	PFDavg = 9.70 E-04 - Valid for **SIL 2**

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 = 2.59 E-03 - Valid for **SIL 2**

SC 2: Systematic capability SIL 2.

2) Application for D5274S of single Alarm Trip Amplifier with Relay 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 "Burnout Repeater" on Configuration Alarm 1 or 2; NO Contact position in alarm "Open" on Configuration Alarm 1 or 2; impose Low Set and Low Hysteresis values if Type "Low" or "Window" have been chosen on Configuration Alarm 1 or 2, OR impose High Set and High Hysteresis values if Type "High" or "Window" have been chosen on Configuration Alarm 1 or 2; in case of input burnout "Alarm Active" for any Type ("Low" or "High" or "Window" or "Burnout Repeater") chosen for Configuration Alarm 1 or 2. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) and 10 (- negative). The green LED is lit in presence of supply power. Input sensor (mV or Thermocouple with or without external compensator, RTD, Potentiometer) is applied from Pins 13 to 16 (see instruction manual of the module for more information about input settings) and related settings must be chosen on Configuration Input 1 of SWC5090 Configuration Software. Alarm A or 1 (Pins 1-2-3) or Alarm B or 2 (Pins 5-6-7) Output permits possible connection to Normally Energized (NE) load or Normally De-energized (ND) load or to Safety PLC input. Alarm A or Alarm B output relay is normally energized, NO contact is closed so that NE load is normally energized, while NC contact is open so that ND load is normally de-energized. In case of alarm, the system goes in Safe State, de-energizing the output relay: NO contact goes open so that NE load is de-energized, while NC contact goes closed so that ND load is energized. To prevent relay contacts from damaging, connect an external protection (fuse or similar), chosen according to the relay breaking capacity (for relay contact rating, see "Technical Data" section of Instruction manual ISM0661).
Source or Sink output current (Pins 11-12) is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D5274S 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 A or Alarm B output configuration is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: it is defined as the output relay being de-energized or NO contact remaining open (de-energizing the NE load) or NC contact remaining closed (energizing the ND load) (the user can program the trip point value, according to the input measured value, at which the output relay 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 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that the output relay remains energized or NO contact fixes closed or NC contact fixes open.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that output relay is forced to be de-energized (that is to Fail-Safe state), with NO contact open or NC contact closed.
- □ 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	121.63
λ_{du} = Total Dangerous Undetected failures	53.70
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	190.48
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**365.81**
MTBF (safety function, single alarm) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**312 years**
$\lambda_{no\ effect}$ = "No effect" failures	353.68
$\lambda_{not\ part}$ = "Not Part" failures	247.10
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**966.59**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**118 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	190.48 FIT	121.63 FIT	53.70 FIT	69.37%	85.32%

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 = 69.37 % ≥ 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:

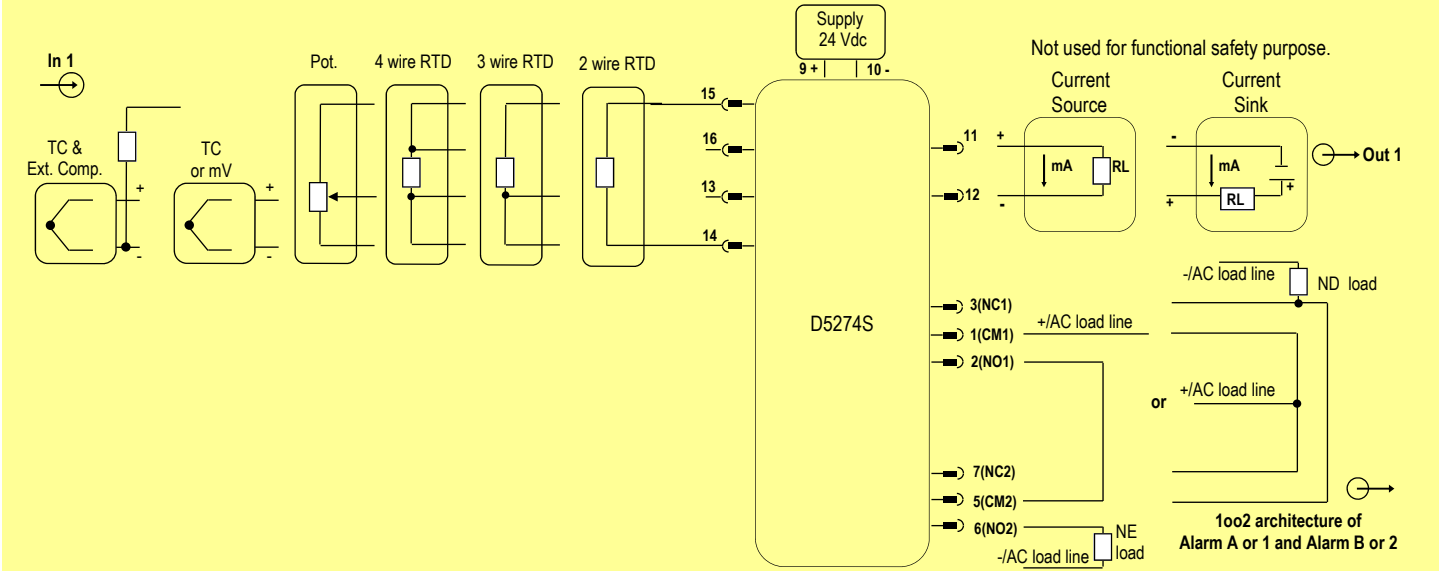
T[Proof] = 1 year	T[Proof] = 4 years
PFDavg = 2.37 E-04 - Valid for **SIL 2**	PFDavg = 9.48 E-04 - Valid for **SIL 2**

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 = 4.74 E-03 - Valid for **SIL 2**

SC 2: Systematic capability SIL 2.

3) Application for D5274S of 1oo2 architecture of Alarm Trip Amplifiers with Relay outputs



Description: By means of SWC5090 Configuration Software, as user interface on a PC to comunicate with the module, select equal parameters for both Alarm 1 and Alarm 2: Burnout "Active" on Configuration Input 1; Type "Low" or "High" or "Window" or "Burnout Repeater" on Configuration Alarm 1 & 2; NO Contact position in alarm "Open" on Configuration Alarm 1 & 2; impose Low Set and Low Hysteresis values if Type "Low" or "Window" have been chosen on Configuration Alarm 1 & 2, OR impose High Set and High Hysteresis values if Type "High" or "Window" have been chosen on Configuration Alarm 1 & 2; in case of input burnout "Alarm Active" for any Type ("Low" or "High" or "Window" or "Burnout Repeater") chosen for Configuration Alarm 1 & 2. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) and 10 (- negative). The green LED is lit in presence of supply power. Input sensor (mV or Thermocouple with or without external compensator, RTD, Potentiometer) is applied from Pins 13 to 16 (see instruction manual of the module for more information about input settings) and related settings must be chosen on Configuration Input 1 of SWC5090 Configuration Software. Alarm A or 1 (Pins 1-2-3) or Alarm B or 2 (Pins 5-6-7) Output permits 1oo2 series / parallel architecture with their NO / NC contacts. NO contacts in 1oo2 series architecture must be only used for Normally Energized (NE) load, while NC contacts in 1oo2 parallel architecture must be only used for Normally De-energized (ND) load. Alarm A and Alarm B output relays are normally energized, NO contacts are closed so that NE load is normally energized, while NC contacts are open so that ND load is normally de-energized. In case of alarm, the system de-energizes to trip, output relays are de-energized, NO contacts are open so that NE load is de-energized, while NC contacts are closed so that ND load is energized. To prevent relay contacts from damaging, connect an external protection (fuse or similar), chosen according to the relay breaking capacity (for relay contact rating, see "Technical Data" section of Instruction manual ISM0661).
Source or Sink output current (Pins 11-12) is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D5274S 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 1oo2 architecture of Alarm A & Alarm B output configuration is used for functional safety application) is described from the following definitions:

- □ Fail-Safe State: it is defined as the output relays being de-energized or NO contacts remaining open (de-energizing the NE load) or NC contacts remaining closed (energizing the ND load) (user must program for both alarm amplifiers the same trip point value, in according with input measured value, at which both output relays 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 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that the output relays remain energized or NO contacts fix closed or NC contacts fix open.
- □ Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that output relays are forced to be de-energized (that is to Fail-Safe state), with NO series contacts open or NC parallel contacts closed.
- □ 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	121.63
λ_{du} = Total Dangerous Undetected failures	21.18
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	240.24
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**383.05**
MTBF (safety function, alarms in 1oo2 architect.) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**298 years**
$\lambda_{no\ effect}$ = "No effect" failures	423.64
$\lambda_{not\ part}$ = "Not Part" failures	159.90
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**966.59**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**118 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	240.24 FIT	121.63 FIT	21.18 FIT	85.17%	94.47%

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 = 85.17 % ≥ 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] = 10.5 years
PFDavg = 9.39 E-05 - Valid for **SIL 2**	PFDavg = 9.86 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 = 1.88 E-03 - Valid for **SIL 2**

SC 2: Systematic capability SIL 2.

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 **D5274S for Analog Current output** consists of the following steps:

Proof test 1A (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 ('13'-'14') of the temperature converter.
3	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	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 2A (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 1A**.
3	Force some input signal values, verifying that the module output current related values are within the specified accuracy (5% (= 1 mA) of full scale range (= 20 mA) respect to 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 **D5274S for each Alarm Trip Amplifier with Relay output** consists of the following steps:

Proof test 1B (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 ('13'-'14') of the temperature converter.
3	For each trip amplifier, impose High or Window type configuration, force a high input signal value so that module alarm amplifier trips for high input condition and verify that the related relay contacts (on terminal blocks 1-2 or 1-3 for trip amplifier 1 and terminal blocks 5-6 or 5-7 for trip amplifier 2) are switched respect to previous normal condition.
4	For each trip amplifier, impose Low or Window type configuration, force a low input signal value so that module alarm amplifier trips for low input condition and verify that the related relay contacts (on terminal blocks 1-2 or 1-3 for trip amplifier 1 and terminal blocks 5-6 or 5-7 for trip amplifier 2) are switched respect to previous normal condition.
5	Restore the loop to full operation.
6	Remove the bypass from the Safety-related PLC or restore normal operation.

Proof test 2B (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 1B**.
3	Force some input signal values, included in the input range of sensor, and for each trip amplifier set a (Low or High or Window) alarm value in the input range. Verify that the related relay contacts (on terminal blocks 1-2 or 1-3 for trip amplifier 1 and terminal blocks 5-6 or 5-7 for trip amplifier 2) are switched when input signal increases / decreases (according to high / low or window alarm setting) above / below the set alarm value, considering a tripping value with a maximum error of 5% respect to the correct input value.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety-related PLC or restore normal operation.