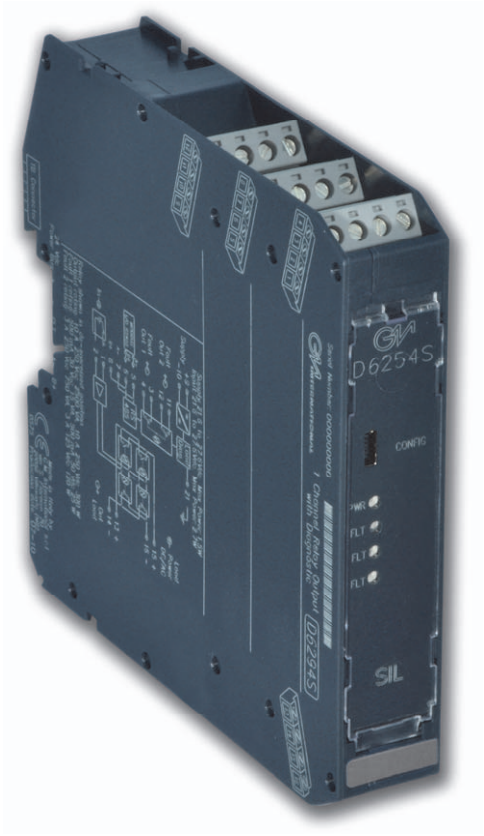


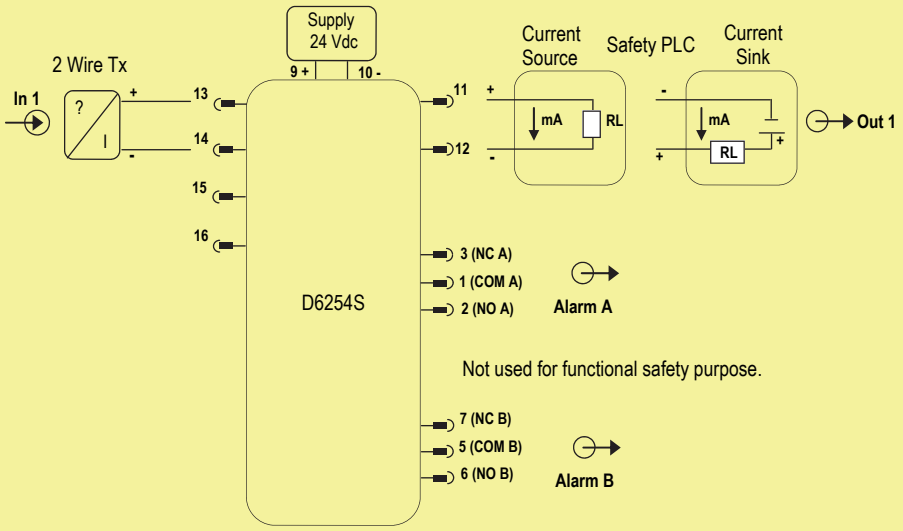
SAFETY MANUAL

SIL 2 - SC 3 Repeater Power Supply / Analog Signal Converter and Trip Amplifiers, DIN-Rail & Termination Board, Model D6254S

Reference must be made to the relevant sections within the instruction manual ISM0310, which contain basic guides for the installation of the equipment.

gmi technology for safety

1) Application for D6254S, Passive input and 4-20 mA Analog Current Output



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and 4 - 20 mA current Source or Sink output mode (with analog output forced to Fault Output value < 4mA or > 20mA in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Passive input signal from 2 wires Tx is applied to Pins 13-14. Source or Sink output current is applied to Pins 11-12. Alarm A and Alarm B Outputs are not used for functional safety purpose. Alarm acknowledgement input (Pins 4-8, not shown in figure) cannot be used with analog current output because it's only an optional feature of alarm trip amplifiers.

Safety Function and Failure behavior:

D6254S 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 output going to 0 mA due to D6254S 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 3% of the correct value.
- □ Fail High: failure mode that causes the 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 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: a dangerous failure which has been detected from D6254S internal diagnostic so that 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	168.00
λ_{du} = Total Dangerous Undetected failures	21.08
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	142.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**331.39**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**344 years**
$\lambda_{no\ effect}$ = "No effect" failures	329.11
$\lambda_{not\ part}$ = "Not Part" failures	262.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	142.31 FIT	168.00 FIT	21.08 FIT	88.85%	93.64%

where DC means the diagnostic coverage for the input sensor by the safety logic solver and internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 88.85 % ≥ 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:

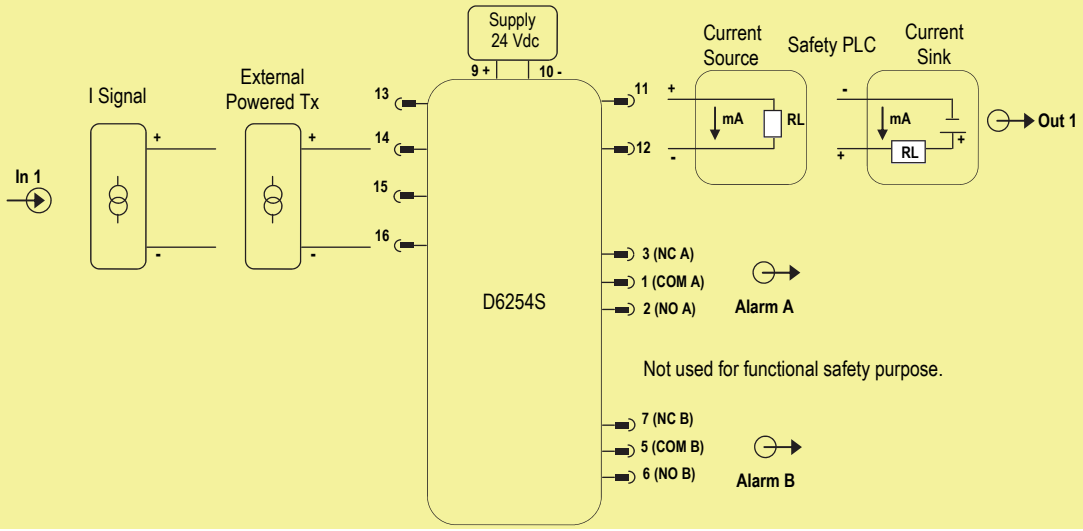
T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.38 E-05 - Valid for **SIL 2**	PFDavg = 9.38 E-04 - Valid for **SIL 2**

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 3: Systematic capability SIL 3. Two channels (each with input + analog current output) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to SIL 3.

2) Application for D6254S, Active input and 4-20 mA Analog Current Output



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and 4 - 20 mA current Source or Sink output mode (with analog output forced to Fault Output value < 4mA or > 20mA in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Active input signal from external powered Tx or current signal from external source is applied to Pins 14-16. Source or Sink output current is applied to Pins 11-12. Alarm A and Alarm B Outputs are not used for functional safety purpose. Alarm acknowledgement input (Pins 4-8, not shown in figure) cannot be used with analog current output because it's only an optional feature of alarm trip amplifiers.

Safety Function and Failure behavior:

D6254S 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 output going to 0 mA due to D6254S 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 3% of the correct value.
- □ Fail High: failure mode that causes the 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 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: a dangerous failure which has been detected from D6254S internal diagnostic so that 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	163.29
λ_{du} = Total Dangerous Undetected failures	21.05
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	142.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**326.65**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**349 years**
$\lambda_{no\ effect}$ = "No effect" failures	320.65
$\lambda_{not\ part}$ = "Not Part" failures	275.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	142.31 FIT	163.29 FIT	21.05 FIT	88.58%	93.56%

where DC means the diagnostic coverage for the input sensor by the safety logic solver and internal diagnostic circuits. 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:

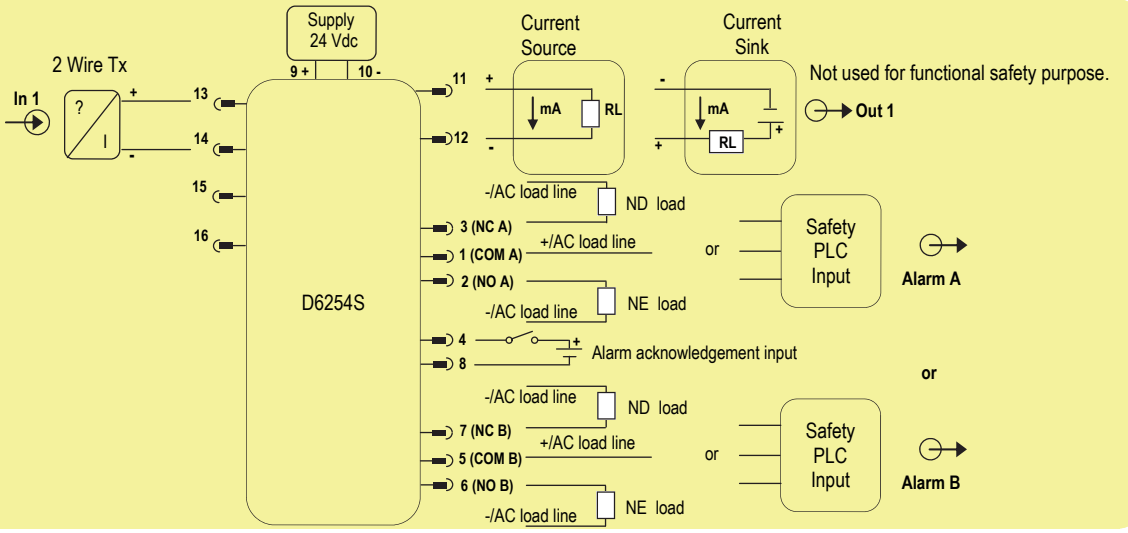
T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.37 E-05 - Valid for **SIL 2**	PFDavg = 9.37 E-04 - Valid for **SIL 2**

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 = 1.87 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3. Two channels (each with input + analog current output) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to SIL 3.

3) Application for D6254S, Passive input and Single Alarm Trip amplifier with Relay output



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and program Alarm A or Alarm B Trip Amplifier using NO contact position open (equivalent to NC contact position closed) in case of alarm (with alarm also triggered in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Passive input signal from 2 wires Tx is applied to Pins 13-14. Alarm acknowledgement input (Pins 4-8) can be used because it doesn't affect this Functional Safety application. Each Alarm Trip Amplifier has got 2 relay contacts: Normally Open (NO) contact (Pins 1-2 for Alarm A or Pins 5-6 for Alarm B) and Normally Closed (NC) contact (Pins 1-3 for Alarm A or Pins 5-7 for Alarm B). NO contact must be only used for Normally Energized (NE) load, while NC contact must be only used for Normally De-energized (ND) load. 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 de-energizes to trip, output relay is de-energized, NO contact is open so that NE load is de-energized, while NC contact is 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 ISM0310). Analog current output is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D6254S 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 of more than 3% of the correct value and, therefore, it has the potential not 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 holds energized or NO contact fixes closed (energizing the NE load) or NC contact fixes open (de-energizing the ND load).
- □ Fail Dangerous Detected: a dangerous failure which has been detected from D6254S 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	108.41
λ_{du} = Total Dangerous Undetected failures	42.46
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	192.29
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**343.16**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**332 years**
$\lambda_{no\ effect}$ = "No effect" failures	256.69
$\lambda_{not\ part}$ = "Not Part" failures	322.65
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	192.29 FIT	108.41 FIT	42.46 FIT	71.86%	87.63%

where DC means the dangerous diagnostic coverage for the input sensor by the internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 71.86 % ≥ 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:

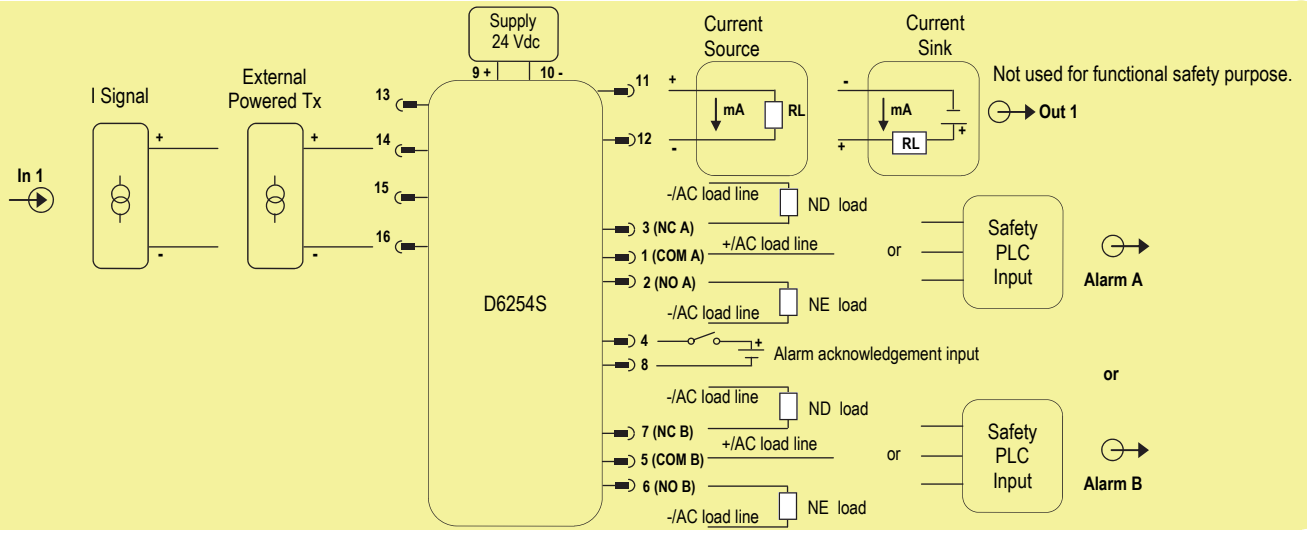
T[Proof] = 1 year	T[Proof] = 5 years
PFDavg = 1.87 E-04 - Valid for **SIL 2**	PFDavg = 9.37 E-04 - Valid for **SIL 2**

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 = 3.74 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3. Two channels (each with input + single alarm trip amplifier with relay output) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to SIL 3.

4) Application for D6254S, Active input and Single Alarm Trip amplifier with Relay output



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and program Alarm A or Alarm B Trip Amplifier using NO contact position open (equivalent to NC contact position closed) in case of alarm (with alarm also triggered in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Active input signal from external powered Tx or current signal from external source is applied to Pins 14-16. Alarm acknowledgement input (Pins 4-8) can be used because it doesn't affect this Functional Safety application. Each Alarm Trip Amplifier has got 2 relay contacts: Normally Open (NO) contact (Pins 1-2 for Alarm A or Pins 5-6 for Alarm B) and Normally Closed (NC) contact (Pins 1-3 for Alarm A or Pins 5-7 for Alarm B). NO contact must be only used for Normally Energized (NE) load, while NC contact must be only used for Normally De-energized (ND) load. 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 de-energizes to trip, output relay is de-energized, NO contact is open so that NE load is de-energized, while NC contact is 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 ISM0310). Analog current output is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D6254S 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 of more than 3% of the correct value and, therefore, it has the potential not 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 holds energized or NO contact fixes closed (energizing the NE load) or NC contact fixes open (de-energizing the ND load).
- □ Fail Dangerous Detected: a dangerous failure which has been detected from D6254S 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	103.70
λ_{du} = Total Dangerous Undetected failures	42.43
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	192.29
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**338.42**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**337 years**
$\lambda_{no\ effect}$ = "No effect" failures	248.23
$\lambda_{not\ part}$ = "Not Part" failures	335.85
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	192.29 FIT	103.70 FIT	42.43 FIT	70.96%	87.46%

where DC means the dangerous diagnostic coverage for the input sensor by the internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 70.96 % ≥ 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:

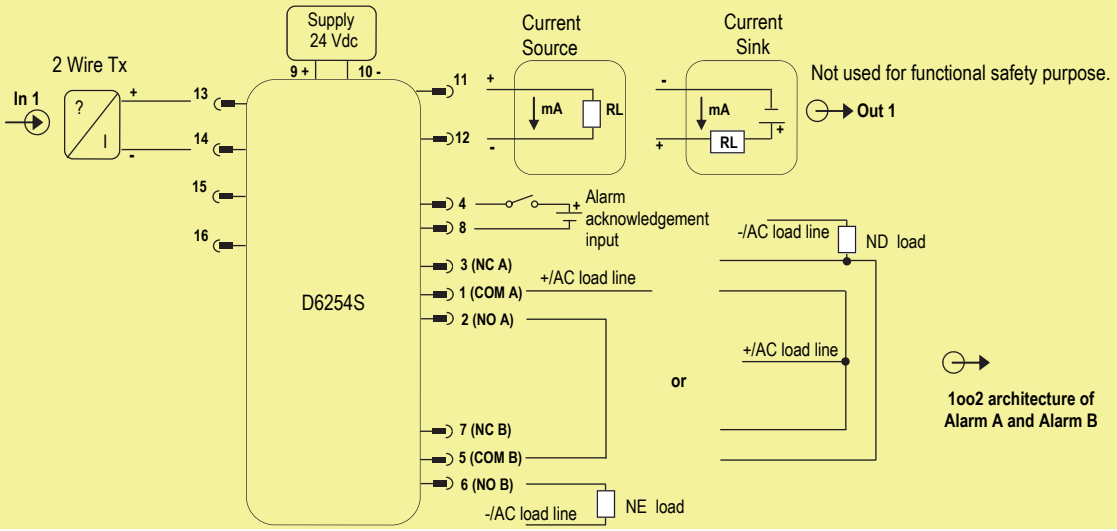
T[Proof] = 1 year	T[Proof] = 5 years
PFDavg = 1.87 E-04 - Valid for **SIL 2**	PFDavg = 9.35 E-04 - Valid for **SIL 2**

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 = 3.74 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3. Two channels (each with input + single alarm trip amplifier with relay output) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to SIL 3.

5) Application for D6254S, Passive input and 1oo2 architecture of Alarm Trip amplifiers with Relay outputs



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and program both Alarm A and Alarm B Trip Amplifiers are with the same setup, also using NO contact position open (equivalent to NC contact position closed) in case of alarm (with alarm also triggered in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Passive input signal from 2 wires Tx is applied to Pins 13-14. Alarm acknowledgement input (Pins 4-8) can be used because it doesn't affect this Functional Safety application. Each Alarm Trip Amplifier has got 2 relay contacts: Normally Open (NO) contact (Pins 1-2 for Alarm A or Pins 5-6 for Alarm B) and Normally Closed (NC) contact (Pins 1-3 for Alarm A or Pins 5-7 for Alarm B). 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 ISM0310) Analog current output is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D6254S 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 series contacts remaining open (de-energizing the NE load) or NC parallel contacts remaining closed (energizing the ND load); the user can program the trip point value, according to the input measured value, at which the 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 of more than 3% of the correct value and, therefore, it has the potential not 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 hold energized or NO series contacts fix closed (energizing the NE load) or NC parallel contacts fix open (de-energizing the ND load).
- □ Fail Dangerous Detected: a dangerous failure which has been detected from D6254S 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	108.41
λ_{du} = Total Dangerous Undetected failures	10.95
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	162.27
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**281.63**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**405 years**
$\lambda_{no\ effect}$ = "No effect" failures	403.17
$\lambda_{not\ part}$ = "Not Part" failures	237.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	162.27 FIT	108.41 FIT	10.95 FIT	90.83%	96.11%

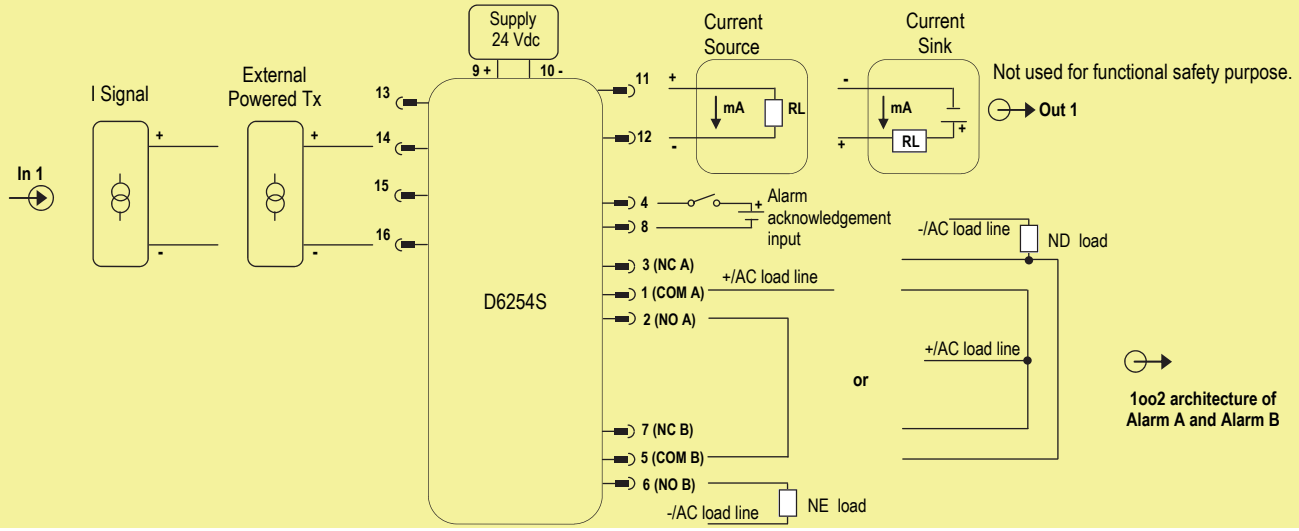
where DC means the dangerous diagnostic coverage for the input sensor by the internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 90.83 % ≥ 60 as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

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] = 20 years
PFDavg = 4.89 E-05 - Valid for **SIL 2**	PFDavg = 9.78 E-04 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3. Two channels (each with input + 1oo2 architecture of alarm trip amplifiers with relay outputs) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to SIL 3.

6) Application for D6254S, Active input and 1oo2 architecture of Alarm Trip amplifiers with Relay outputs



Description:

For this application, enable Current input type (with Out of range < 4 mA and > 20 mA fault detection) and program both Alarm A and Alarm B Trip Amplifiers are with the same setup, also using NO contact position open (equivalent to NC contact position closed) in case of alarm (with alarm also triggered in case of Out of range fault presence on input). For more information, see "Configuration parameters" section of Instruction manual ISM0310. The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power. Active input signal from external powered Tx or current signal from external source is applied to Pins 14-16.
Alarm acknowledgement input (Pins 4-8) can be used because it doesn't affect this Functional Safety application. Each Alarm Trip Amplifier has got 2 relay contacts: Normally Open (NO) contact (Pins 1-2 for Alarm A or Pins 5-6 for Alarm B) and Normally Closed (NC) contact (Pins 1-3 for Alarm A or Pins 5-7 for Alarm B). 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 ISM0310). Analog current output is only used for service purpose (not for Safety purpose).

Safety Function and Failure behavior:

D6254S 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 series contacts remaining open (de-energizing the NE load) or NC parallel contacts remaining closed (energizing the ND load); the user can program the trip point value, according to the input measured value, at which the 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 of more than 3% of the correct value and, therefore, it has the potential not 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 hold energized or NO series contacts fix closed (energizing the NE load) or NC parallel contacts fix open (de-energizing the ND load).
- □ Fail Dangerous Detected: a dangerous failure which has been detected from D6254S 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	103.70
λ_{du} = Total Dangerous Undetected failures	10.92
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	162.27
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**276.89**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**412 years**
$\lambda_{no\ effect}$ = "No effect" failures	394.71
$\lambda_{not\ part}$ = "Not Part" failures	250.90
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**922.50**
MTBF (device, one channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**123 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	162.27 FIT	103.70 FIT	10.92 FIT	90.47%	96.06%

where DC means the dangerous diagnostic coverage for the input sensor by the internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 90.47 % ≥ 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] = 20 years
PFDavg = 4.87 E-05 - Valid for **SIL 2**	PFDavg = 9.75 E-04 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3. Two channels (each with input + 1oo2 architecture of alarm trip amplifiers with relay outputs) of two different D6254S modules can used to increase the hardware fault tolerance to HFT = 1, needed for a Safety Function requiring a higher SIL level equal to 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 **D6254S for Analog Current output** consists of the following steps:

Proof test 1A (to reveal 50 % of possible Dangerous Undetected failures in the repeater)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Set the input transmitter or give an input current signal to go to the full scale current output 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.
3	Set the input transmitter or give an input current signal to go to the low scale current output and verify that the analog current reaches that value. This tests is 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.

Proof test 2A (to reveal 99 % of possible Dangerous Undetected failures in the repeater)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Perform steps 2 and 3 of **Proof Test 1A**.
3	Perform a two-point calibration of the input transmitter or the input current source (i.e. 4 mA and 20 mA) and verify that the module output current is within the specified accuracy. This test requires that the transmitter or the input current source has already been tested without the repeater and that it works correctly according to its specifications.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety-related PLC or restore normal operation.

The test on **D6254S for each Alarm Trip amplifier with Relay output** consists of the following steps:

Proof test 1B (to reveal 50 % of possible Dangerous Undetected failures in the alarm trip amplifier and relay output)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	For each trip amplifier, set the input transmitter or give an input current signal to go to the high alarm current output and verify that the related relay contacts (between terminal blocks 1-2 or 1-3 for trip amplifier 1 and 5-6 or 5-7 for trip amplifier 2) are switched.
3	For each trip amplifier, set the input transmitter or give an input current signal to go to the low alarm current output and verify that the related relay contacts (between terminal blocks 1-2 or 1-3 for trip amplifier 1 and 5-6 or 5-7 for trip amplifier 2) are switched.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety-related PLC or restore normal operation.

Proof test 2B (to reveal 99 % of possible Dangerous Undetected failures in the alarm trip amplifier and relay output)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Perform steps 2 and 3 of **Proof Test 1B**.
3	Perform a two-point calibration of each trip amplifier (i.e. 4 mA and 20 mA) and verify that the related relay contacts (between terminal blocks 1-2 or 1-3 for trip amplifier 1 and 5-6 or 5-7 for trip amplifier 2) are switched when related current signal (by input transmitter or source) is imposed to module input.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety-related PLC or restore normal operation.