SAFETY MANUAL

SIL 2 Quadruple Repeater Power Supply DIN-Rail and Termination Board Model D6212Q

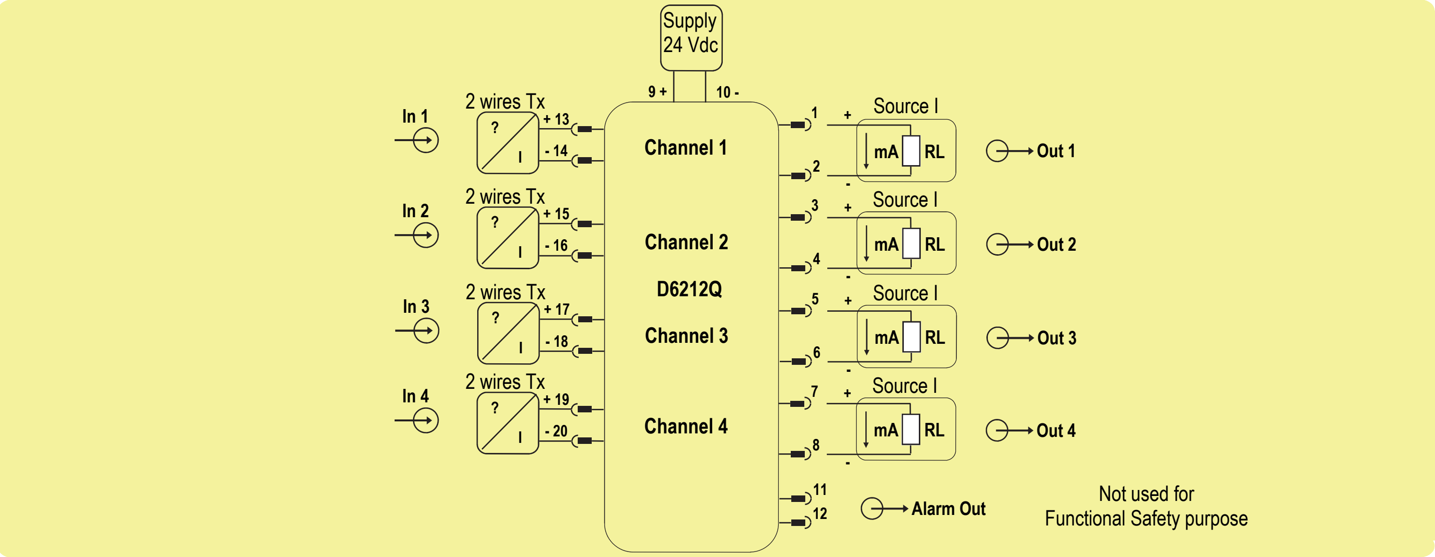
Approval: TÜV Certificate No. C-IS-722160171, SIL 2 conforms to IEC61508:2010 Ed.2 .
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Reference must be made to the relevant sections within the instruction manual ISM0455 and ISM0154 (for SWC5090 Configuration Software instruction manual), which contain basic guides for the installation and configuration of the equipment.

gm technology for safety

Functional Safety Manual and Application

Application for each channel of D6212Q, with passive transmitter Tx input and 4-20 mA current source output.



Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select for each channel: Input window with "Out of range" selection (Low threshold < 4000, High threshold > 20000); Output window with Type "4-20 mA Source", with Fault output value < 3000 or > 21000, with "Fault in case of Out of range" selection. If "Advanced settings" button is clicked, each Output can be associated to Input from 1 to 4 (as Out 1 to In 1 or also Out 1 to In 4) and Output operations must be set to "None".

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 signals from passive transmitters or 2-wires Tx are applied to: Pins 13-14 (In 1 - Ch.1), Pins 15-16 (In 2 - Ch.2), Pins 17-18 (In 3 - Ch.3), Pins 19-20 (In 4 - Ch.4).

Source output currents are applied to: Pins 1-2 (Out 1), Pins 3-4 (Out 2), Pins 5-6 (Out 3), Pins 7-8 (Out 4). Alarm output is only used for service purpose (not for Functional Safety).

Safety Function and Failure behavior:

D6212Q is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For each channel of D6212Q module, the failure behavior with 4-20 mA current source output is described by the following definitions:

□ fail-Safe State: it is defined as the 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 3% (0.5 mA) of full span respect to correct value;

□ fail High: failure mode that causes the output signal to go above the maximum output current (> 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). 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 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 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 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	175.91
λ_{du} = Total Dangerous Undetected failures	33.83
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	112.13
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**321.87**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**355 years**
$\lambda_{no\ effect}$ = "No effect" failures	368.62
$\lambda_{not\ part}$ = "Not Part" failures	201.30
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**891.79**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**128 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	112.13 FIT	175.91 FIT	33.83 FIT	83.87%	89.49%

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 = 83.87 % ≥ 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] = 6 years
PFDavg = 1.50 E-04 Valid for **SIL 2**	PFDavg = 9.00 E-04 Valid for **SIL 2**

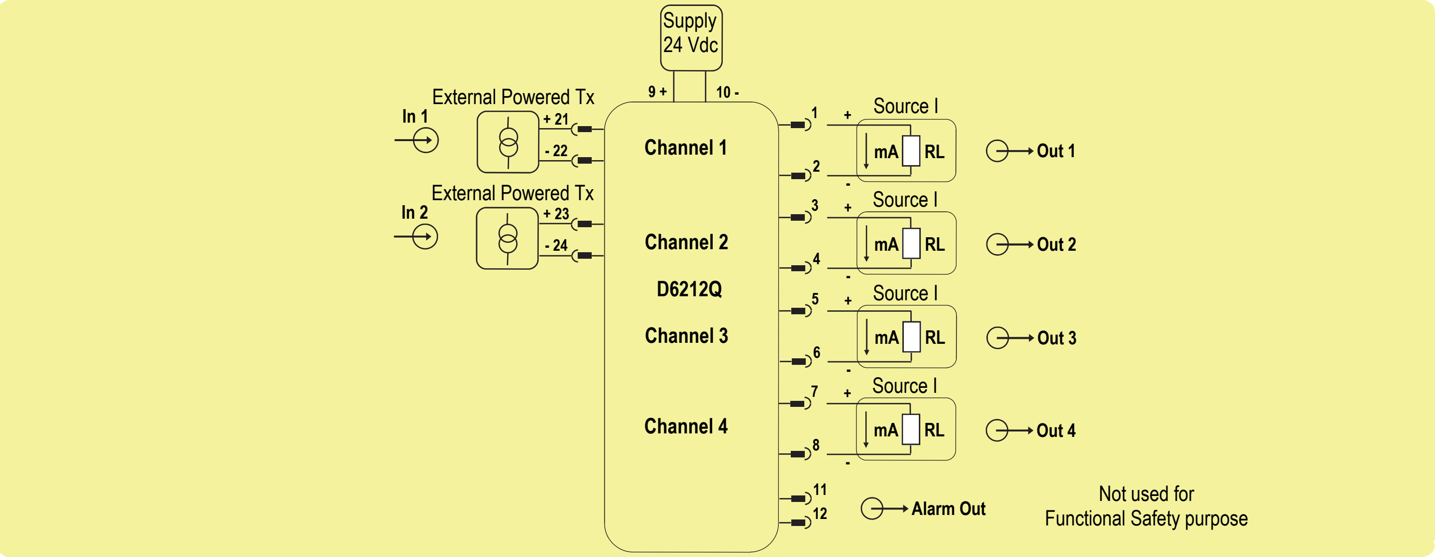
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 3.00 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Functional Safety Manual and Application

Application for only input channels 1 and 2 of D6212Q, with active transmitter Tx input and 4-20 mA current source output.



Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select for only channel 1 and 2: Input window with "Out of range" selection (Low threshold < 4000, High threshold > 20000); Output window with Type "4-20 mA Source", with Fault output value < 3000 or > 21000, with "Fault in case of Out of range" selection. If "Advanced settings" button is clicked, each Output can be associated to Input 1 or 2 (as Out 1 to In 1 or also Out 1 to In 2) and Output operations must be set to "None".

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 signals from active transmitters or External powered Tx are applied to: Pins 21-22 (In 1 - Ch.1), Pins 23-24 (In 2 - Ch.2).

Source output currents are applied to: Pins 1-2 (Out 1), Pins 3-4 (Out 2), Pins 5-6 (Out 3), Pins 7-8 (Out 4). Alarm output is only used for service purpose (not for Functional Safety).

Safety Function and Failure behavior:

D6212Q is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For only channel 1 and 2 of D6212Q module, the failure behavior with 4-20 mA current source output is described by the following definitions:

□ fail-Safe State: it is defined as the 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 3% (0.5 mA) of full span respect to correct value;

□ fail High: failure mode that causes the output signal to go above the maximum output current (> 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). 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 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 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 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	175.16
λ_{du} = Total Dangerous Undetected failures	30.66
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	112.13
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**317.95**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**359 years**
$\lambda_{no\ effect}$ = "No effect" failures	368.14
$\lambda_{not\ part}$ = "Not Part" failures	205.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**891.79**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**128 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	112.13 FIT	175.16 FIT	30.66 FIT	85.10%	90.36%

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 = 85.10 % ≥ 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 years
PFDavg = 1.36 E-04 Valid for **SIL 2**	PFDavg = 9.52 E-04 Valid for **SIL 2**

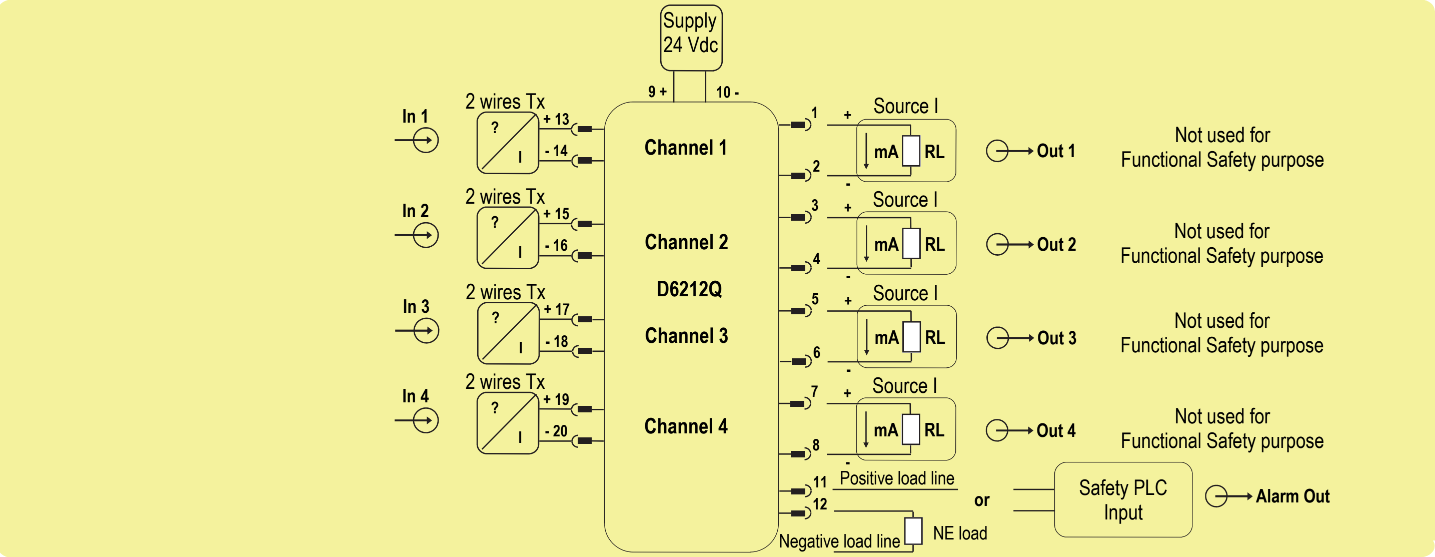
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 2.72 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Functional Safety Manual and Application

Application for each input channel of D6212Q, with passive transmitter Tx input and alarm output.



Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select for each channel: Input window with "Out of range" selection (Low threshold < 4000, High threshold > 20000); Alarm window with Type "Low" or "High" or "Window" or "Fault Repeater", with Input from 1 to 4 as Input selector and Output operations set to "None", with NO (Normally open) contact position = Open (that is, alarm output is closed under regular working conditions, and it opens in case of alarm); Alarm window with setting of Low Set and Low Hysteresys values if Type "Low" or "Window" have been chosen, OR imposing High Set and High Hysteresys values if Type "High" or "Window" have been chosen; then, in case of fault "Alarm Active" if "Fault" have been enabled when input is out of configured range.

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 signals from passive transmitters or 2-wires Tx are applied to: Pins 13-14 (In 1 - Ch.1), Pins 15-16 (In 2 - Ch.2), Pins 17-18 (In 3 - Ch.3), Pins 19-20 (In 4 - Ch.4).

Alarm Output is applied to Pins 11-12, with possible connection to Normally Energized (NE) load or to Safety PLC input.

Source output currents are only used for service purpose (not for Safety purpose) and they are applied to: Pins 1-2 (Out 1), Pins 3-4 (Out 2), Pins 5-6 (Out 3), Pins 7-8 (Out 4); to choose Input to Output correspondence see "Advanced settings" in the Output window.

Safety Function and Failure behavior:

D6212Q is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For each input channel of D6212Q module, the failure behavior with alarm output is described by the following definitions:

□ fail-Safe State: it 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 leads to a measurement error more than 3% (0.5 mA) of full span respect to correct value and therefore it 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 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 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	139.09
λ_{du} = Total Dangerous Undetected failures	38.90
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	136.28
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**314.27**
MTBF (safety function, alarm channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**363 years**
$\lambda_{no\ effect}$ = "No effect" failures	338.42
$\lambda_{not\ part}$ = "Not Part" failures	239.10
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**891.79**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**128 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	136.28 FIT	139.09 FIT	38.90 FIT	78.14%	87.62%

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 = 78.14 % ≥ 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 = 1.72 E-04 Valid for **SIL 2**	PFDavg = 8.60 E-04 Valid for **SIL 2**

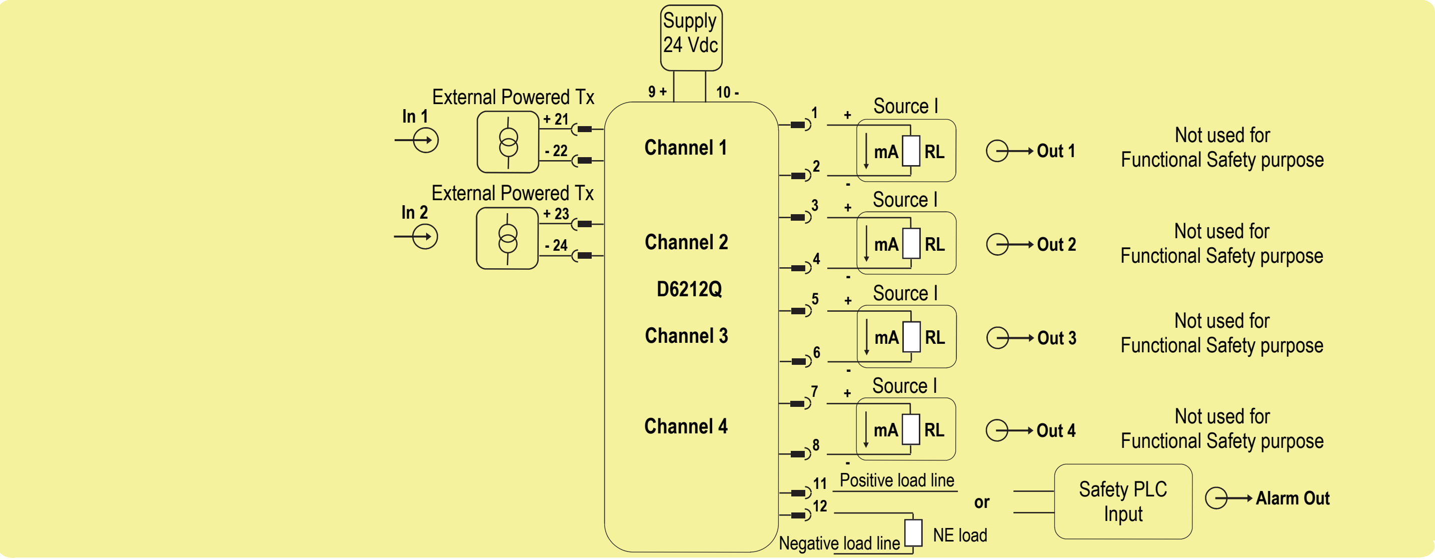
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 3.44 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Functional Safety Manual and Application

Application for only input channels 1 and 2 of D6212Q, with active transmitter Tx input and alarm output.



Description:

By means of SWC5090 Configuration Software, as user interface on PC to comunicate with the module, select for only channel 1 and 2: Input window with "Out of range" selection (Low threshold < 4000, High threshold > 20000); Alarm window with Type "Low" or "High" or "Window" or "Fault Repeater", with Input 1 or 2 as Input selector and Output operations set to "None", with NO (Normally open) contact position = Open (that is, alarm output is closed under regular working conditions, and it opens in case of alarm); Alarm window with setting of Low Set and Low Hysteresys values if Type "Low" or "Window" have been chosen, OR imposing High Set and High Hysteresys values if Type "High" or "Window" have been chosen; then, in case of fault "Alarm Active" if "Fault" have been enabled when input is out of configured range.

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 signals from active transmitters or External powered Tx are applied to: Pins 21-22 (In 1 - Ch.1), Pins 23-24 (In 2 - Ch.2).

Alarm Output is applied to Pins 11-12, with possible connection to Normally Energized (NE) load or to Safety PLC input.

Source output currents are only used for service purpose (not for Safety purpose) and they are applied to: Pins 1-2 (Out 1), Pins 3-4 (Out 2), Pins 5-6 (Out 3), Pins 7-8 (Out 4); to choose Input to Output correspondence see "Advanced settings" in the Output window.

Safety Function and Failure behavior:

D6212Q is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

For only channel 1 and 2 of D6212Q module, the failure behavior with alarm output is described by the following definitions:

□ fail-Safe State: it 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 leads to a measurement error more than 3% (0.5 mA) of full span respect to correct value and therefore it 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 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 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	138.34
λ_{du} = Total Dangerous Undetected failures	35.73
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	136.28
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**310.35**
MTBF (safety function, alarm channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**368 years**
$\lambda_{no\ effect}$ = "No effect" failures	337.94
$\lambda_{not\ part}$ = "Not Part" failures	243.50
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**891.79**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**128 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	136.28 FIT	138.34 FIT	35.73 FIT	79.47%	88.49%

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 = 79.47 % ≥ 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] = 6 years**
PFDavg = 1.58 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 = 3.16 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.

For each channel, the test on **D6212Q with passive or active input transmitter and 4-20 mA current source output** consists of the following steps:

Proof test 1 (to reveal approximately 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 transmitter connected to the input of the repeater in order to go to high current value (> 20 mA but lower than out of range superior limit imposed during module configuration by SWC5090) and verify that the output current of the repeater reaches that value. This test is for voltage compliance problems, such as a low power supply voltage or an increased wiring resistance, and for other possible failures .
3	Set the transmitter connected to the input of the repeater in order to go to low current value (< 4 mA but higher than out of range inferior limit imposed during module configuration by SWC5090) and verify that the output current of the repeater 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 PLC or restore normal operation.

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

Steps	Action
1	Bypass the Safety PLC or take other appropriate action to avoid a false trip.
2	Perform steps 2 and 3 of **Proof Test 1**.
3	Perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the input of the repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy (3 % (± 0.5 mA) of full span) as defined in the Safety Function. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance and it does not contain any dangerous undetected failures.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.

For each channel, the test on **D6212Q with passive or active input transmitter and alarm output** consists of the following steps:

Proof test (to reveal approximately 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	According to Alarm Function setting, force an input signal value bigger than high limit for alarm tripping and verify that the photo MOS of alarm output (terminals ‘11’-‘12’) is open because alarm output changes from normally energize state to de-energize to trip state .
3	According to Alarm Function setting, force an input signal value smaller than low limit for alarm tripping and verify that the photo MOS of alarm output (terminals ‘11’-‘12’) is open because alarm output changes from normally energize state to de-energize to trip state.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.