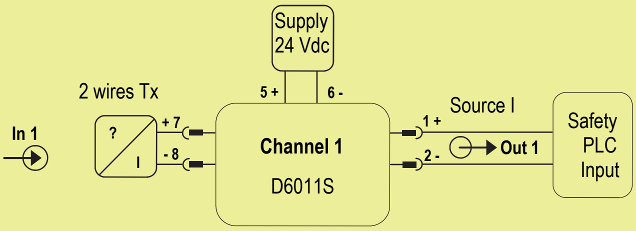
SAFETY MANUAL

SIL 3 Repeater Power Supply Hart, DIN-Rail and Termination Board, Models D6011S, D6011D

Reference must be made to the relevant sections within the instruction manual ISM0211, which contain basic guides for the installation of the equipment.

technology for safety

Application for D6011S, with passive input (2 wires Tx)



Description:

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Passive input signal from 2 wires Tx are applied to Pins 7-8 (In 1 - Ch.1).
Source output current is applied to Pins 1-2.

Safety Function and Failure behavior:

D6011S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

□ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
□ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
□ 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 failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
□ 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 failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
□ 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 part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	131.47
λ_{du} = Total Dangerous Undetected failures	13.46
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**144.94**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**787 years**
$\lambda_{no\ effect}$ = "No Effect" failures	194.87
$\lambda_{not\ part}$ = "Not Part" failures	4.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**344.00**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**331 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	131.47 FIT	13.46 FIT	90.71%	0%	90.71%

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

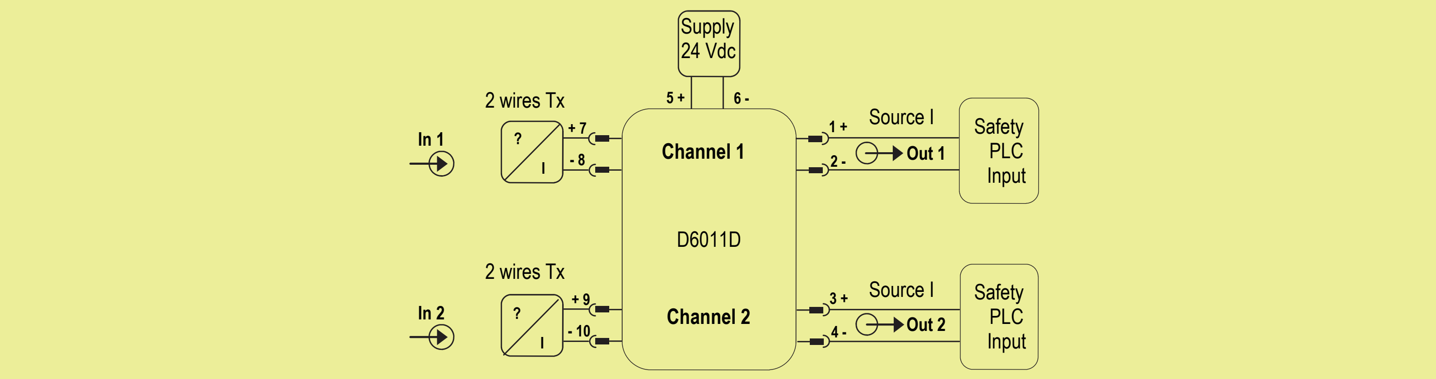
T[Proof] = 1 year	T[Proof] = 16 years
PFDavg = 6.01 E-05 Valid for **SIL 3**	PFDavg = 9.62 E-04 Valid for **SIL 2**

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] = 10 years	T[Proof] = 20 years
PFDavg = 6.01 E-04 Valid for **SIL 3**	PFDavg = 1.20 E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Application for D6011D, with passive input (2 wires Tx)



Description:

The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power.
Passive input signals from 2 wires Tx are applied to Pins 7-8 (In 1 - Ch.1) and Pins 9-10 (In 2 - Ch.2).
Source output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D6011D is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described from the following definitions :

□ fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;
□ fail Safe: failure mode that causes the module 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;
□ 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 failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
□ 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 failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
□ 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 part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

The 2 channels of D6011D module should not be used to increase the hardware fault tolerance needed for a Safety Function requiring higher SIL, as they are not completely independent from each other.
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	155.47
λ_{du} = Total Dangerous Undetected failures	13.46
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**168.94**
MTBF (safety function, one channel with other channel influence) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**675 years**
$\lambda_{no\ effect}$ = “No Effect” failures	227.87
$\lambda_{not\ part}$ = “Not Part” failures	193.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**589.80**
MTBF (device, double channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**193 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	155.47 FIT	13.46 FIT	92.03%	0%	92.03%

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] = 16 years
PFDavg = 6.03 E-05 Valid for **SIL 3**	PFDavg = 9.65 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] = 10 years	T[Proof] = 20 years
PFDavg = 6.03 E-04 Valid for **SIL 3**	PFDavg = 1.21 E-03 Valid for **SIL 2**

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 fault, which have been noted during the FMEDA, can be revealed during proof test. **The Proof test 1** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
3	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to low alarm current and verify that the output current of the repeater reaches that value. This tests 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.

This test will reveal approximately 30 % of possible Dangerous Undetected failures in the repeater.

The **Proof test 2** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the **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. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the repeater.