SAFETY MANUAL

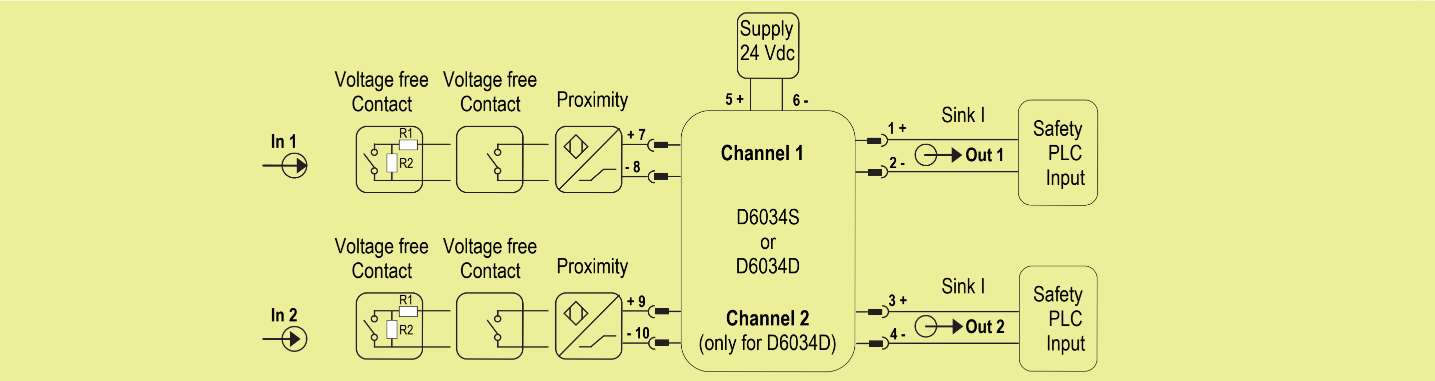
SIL 3 Switch/Proximity Interface DIN-Rail and Termination Board

Models D6034S, D6034D

Reference must be made to the relevant sections within the instruction manual ISM0215, which contain basic guides for the installation of the equipment.

Functional Safety Manual and Application

Application for D6034S or D6034D



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.
Voltage free contact or proximity detector are applied to Pins 7-8 (In 1 - Ch.1) and Pins 9-10 (In 2 - Ch.2).
Sink output currents are applied to Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2).

Safety Function and Failure behavior:

D6034 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% (0.4 mA) of 8 mA full scale;
□ fail High: failure mode that causes the output signal to go above 7 mA (as short circuit of input). 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 0.35 mA (as input line breakage). 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 D6034D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D6034S (single channel) are also valid for each channel of D6034D (double channel).
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	125.63
λ_{du} = Total Dangerous Undetected failures	12.64
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**138.27**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**825 years**
$\lambda_{no\ effect}$ = “No Effect” failures	182.53
$\lambda_{not\ part}$ = “Not Part” failures	4.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**325.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**350 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	125.63 FIT	12.64 FIT	90.86%	0%	90.86%

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] = 17 years
PFDavg = 5.65 E-05 Valid for **SIL 3**	PFDavg = 9.61 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 = 5.65 E-04 Valid for **SIL 3**	PFDavg = 1.13 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 faults, which have been noted during the FMEDA, can be revealed during proof test.

Note for switch input: to detect a broken wire, or a short circuit condition, in the input connections it is necessary to mount, close to the switches, the end of line resistors:
R1=1 KΩ typical (470 Ω to 2 KΩ range) resistor in series and R2=10 kΩ typical (5 KΩ to 15 KΩ range) resistor in parallel to the contacts.

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	Vary the state condition of the input sensors /contacts or the proximity switches connected in the field in order to go to short circuit condition and verify that the output current of the repeater reaches high current value (> 7 mA). This test for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
3	Vary the state condition of the input sensors / contacts or the proximity switches connected in the field in order to go to open connection condition (equivalent to line breakage) and verify that the output current of the repeater reaches low current value (< 0.35 mA). 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	Connect an ammeter in series to the input sensors / contacts or the proximity switches in order to measure the input sensor current. Then vary the state condition of the input sensors / contacts (from open to close condition and vice versa) or the proximity switches (from ON to OFF condition and vice versa), and verify that the output current of repeater is in accordance with the input sensor current, within the specified accuracy. This requires that the input sensors / contacts or the proximity switches have already been tested without the repeater and they work correctly according to their 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.