

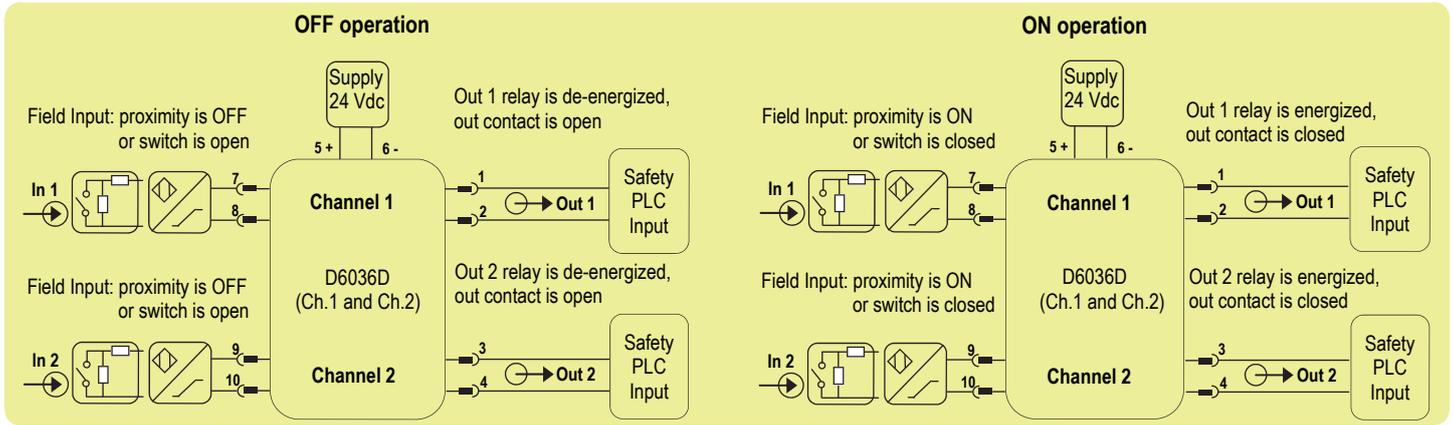
SAFETY MANUAL

SIL 2 Switch/Proximity Detector Repeater, Relay Output DIN-Rail Models D6036S, D6036D

Reference must be made to the relevant sections within the instruction manual ISM0407,
which contain basic guides for the installation of the equipment.



Application for D6036D



Description: For this application, enable input line fault (open or short) detection and direct input to output transfer function, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position	1	2	3	4
ON/OFF state	ON	OFF	ON	OFF

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.

Input signals from field are applied to Pins 7-8 (In 1 - Ch.1) and Pins 9-10 (In 2 - Ch.2).

Relay contact outputs Pins 1-2 (for Channel 1) and Pins 3-4 (for Channel 2) are both normally open (or relay de-energized as safe state condition) for OFF operation, while they are both closed (or relay energized) for ON operation.

The following table describes for each channel the state (open or closed) of its output when its input signal is in OFF or ON state, and it gives information about turn-on or turn-off of the related channel status LED and channel fault LED:

Input signal state Pins 7-8 (In 1 - Ch.1) or 9-10 (In 2 - Ch.2)	Output relay contact state Pins 1-2 (Out 1 - Ch.1) or 3-4 (Out 2 - Ch.2)	Channel status yellow LED state	Channel fault red LED state
Proximity sensor is OFF or switch is open	Open (De-energize relay)	OFF	OFF
Proximity sensor is ON or switch is closed	Closed (Energized relay)	ON	OFF
Independently from proximity sensor or switch state, the input line is break	Open (De-energized relay as safe state condition)	OFF	ON
Independently from proximity sensor or switch state, the input line is in short circuit	Open (De-energized relay as safe state condition)	OFF	ON

Safety Function and Failure behavior:

D6036D is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behavior is described from the following definitions :

- Fail-Safe State: it is defined as the relay output being de-energized (so that the NO contact is open);
- 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 (i.e. being unable to go to the defined Fail-Safe state), so that the relay output remains energized (the NO contact is blocked in closed position);
- 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 that is not part of the Safety Function but that is 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 D6036D module must not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components.

Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	51.22
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	130.16
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	181.38
MTBF (safety function, one channel) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	629 years
$\lambda_{no\ effect}$ = "No Effect" failures	138.62
$\lambda_{not\ part}$ = "Not Part" failures	200.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	520.20
MTBF (device, one channel) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	219 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	130.16 FIT	0.00 FIT	51.22 FIT	71.76%

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

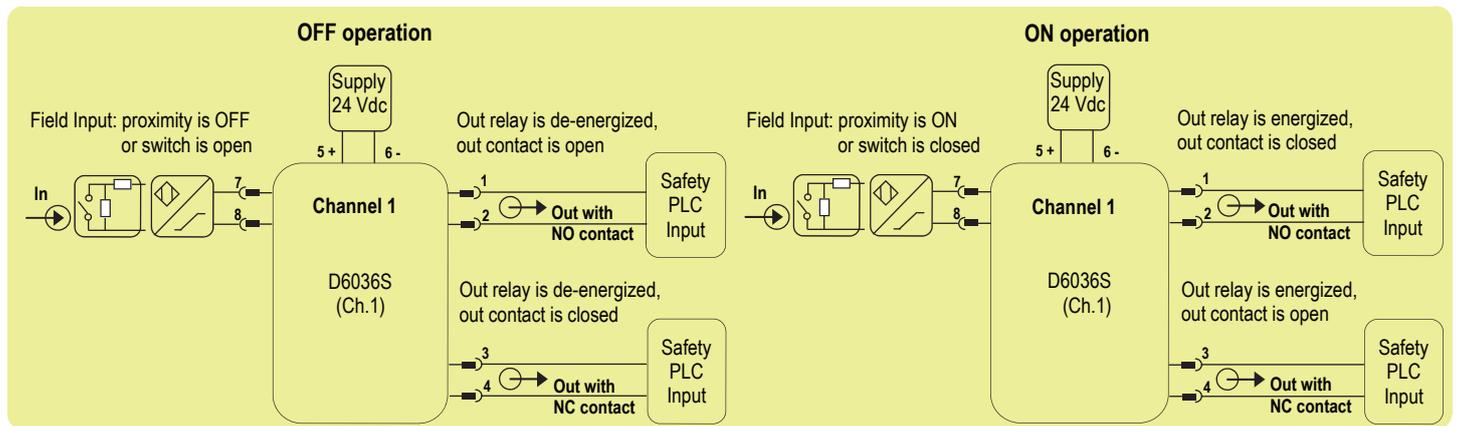
T[Proof] = 1 year	T[Proof] = 4 years
PFDavg = 2.25 E-04 Valid for SIL 2	PFDavg = 8.99 E-04 Valid for SIL 2

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 = 4.50 E-03 Valid for SIL 2

Systematic capability SIL 3.

Application for D6036S



Description:

For this application, enable input line fault (open or short) detection and direct input to output transfer function, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position	1	2	3	4
ON/OFF state	ON	OFF	Not used	Not used

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.

Input signal from field is applied to Pins 7-8 (In 1 - Ch.1).

Relay contact output Pins 1-2 is normally open or Pins 3-4 is normally closed (because relay is de-energized as safe state condition) for OFF operation, while Pins 1-2 is closed or Pins 3-4 is open (because relay is energized) for ON operation. The following table describes for Channel 1 the state (open or closed) of its output contacts when its input signal is in OFF or ON state, and it gives information about turn-on or turn-off of its channel status LED and channel fault LED:

Input signal state Pins 7-8	Out relay contact state Pins 1-2 (with NO contact)	Out relay contact state Pins 3-4 (with NC contact)	Channel status yellow LED state	Channel fault red LED state
Proximity is OFF or switch is open	Open (De-energize relay)	Closed (De-energize relay)	OFF	OFF
Proximity is ON or switch is closed	Closed (Energized relay)	Open (Energized relay)	ON	OFF
If the input line is break	Open (safe state condition)	Closed (safe state condition)	OFF	ON
If the input line is in short circuit	Open (safe state condition)	Closed (safe state condition)	OFF	ON

Safety Function and Failure behavior:

D6036S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behavior is described from the following definitions :

- Fail-Safe State: it is defined as the relay output being de-energized (so that the NO contact is open and the NC contact is closed);
- 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 (i.e. being unable to go to the defined Fail-Safe state), so that the relay output remains energized (the NO contact is blocked in closed position and the NC contact is blocked in open position);
- 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 that is not part of the Safety Function but that is 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	0.00
λ_{du} = Total Dangerous Undetected failures	51.22
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	124.62
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	175.84
MTBF (safety function, one channel) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	649 years
$\lambda_{no\ effect}$ = "No Effect" failures	128.26
$\lambda_{not\ part}$ = "Not Part" failures	23.50
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	327.60
MTBF (device, one channel) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	348 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	124.62 FIT	0.00 FIT	51.22 FIT	70.87%

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 = 2.25 E-04 Valid for SIL 2	PFDavg = 8.99 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 = 4.50 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.

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 K Ω typical (470 Ω to 2 K Ω range) resistor in series and R2=10 k Ω typical (5 K Ω to 15 K Ω range) resistor in parallel to the contacts.

The Proof test consists of the following steps:

Steps	Action
1	Bypass the Safety-related PLC or take any other appropriate action in order to avoid a false trip.
2	Vary the state conditions of the input sensors/contacts coming from field and verify that the relay outputs change from de-energized to energized and vice versa; then, check that the de-energized state condition corresponds to the required Safety-related function.
3	If input line fault detection is enabled for each channel by means of a dip-switches specific set up, disconnect the input wiring coming from the field sensor/contact and check that the correspondent relay output is de-energized. Then, put in short circuit condition the input connections and verify that the same output remains de-energized. In both cases, the related red alarm LEDs on the front panel will be turned on.
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.