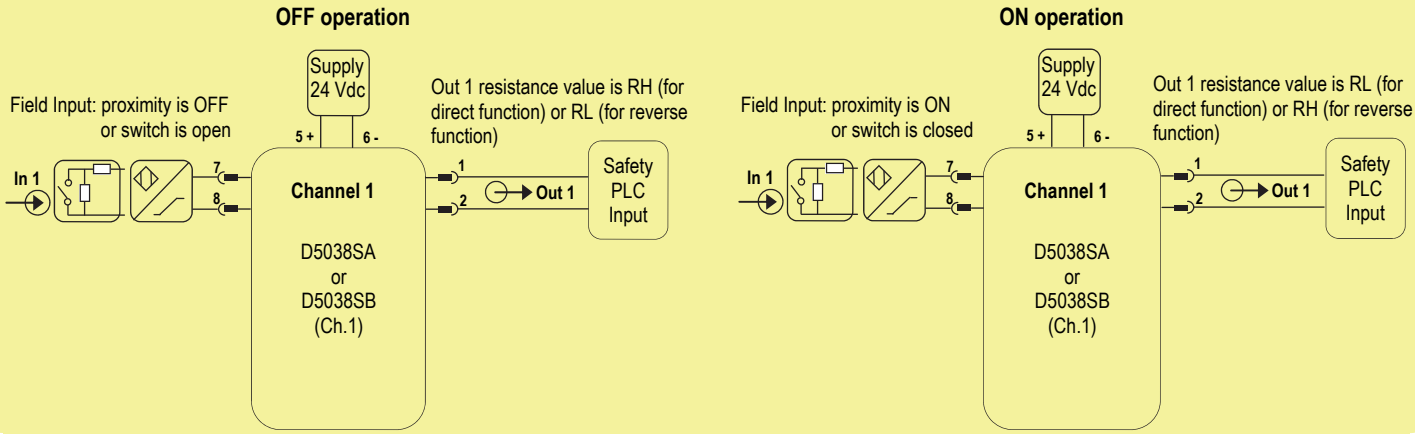
SAFETY MANUAL

I.S. SIL3 Line-Fault Transp. Switch/Prox. Repeater, DIN-Rail and Termination Board Models D5038S*, D5038D*, D5038X*

Reference must be made to the relevant sections within the instruction manual ISM0427, which contain basic guides for the installation of the equipment.

gmi technology for safety

Application for single channel D5038SA or D5038SB



Description:

For this application, enable input line fault (open or short) detection and choose direct or reverse input to output transfer function, by set the internal dip-switches in the following mode (for more information, please see the instruction manual ISM0427):

Dip-switch position	1	2	3	4
ON/OFF state	ON	OFF (direct) or ON (reverse)	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). Output Pins 1-2 (for Channel 1) has got RH (direct function) or RL (reverse function) resistance value for OFF operation, while it has got RL (direct function) or RH (reverse function) resistance value for ON operation. The following table describes for Channel 1 the output resistance value 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 1 signal state Pins 7-8 (In 1 - Ch.1)	Out 1 resistance value Pins 1-2 (Out 1 - Ch.1)	Channel 1 status yellow LED state	Channel 1 fault red LED state
Proximity sensor is OFF or switch is open	RH (direct function) or RL (reverse function)	OFF (direct function) ON (reverse function)	OFF
Proximity sensor is ON or switch is closed	RL (direct function) or RH (reverse function)	ON (direct function) OFF (reverse function)	OFF
Independently from proximity sensor or switch state, input line is broken	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON
Independently from proximity sensor or switch state, input line is short circuited	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON

Safety Function and Failure behavior:

D5038S 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: it is defined as two cases: 1st) the channel output being open, with output resistance equal or bigger than RH ; 2nd) the channel output being in short circuit, with output resistance equal to zero or very little than RL. The module output must be monitored by a Digital Input channel of a Safety PLC in order to detect open circuit (very high resistance) or short circuit (very low resistance) of output channel;
- □ 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 channel output is blocked in closed position, with output resistance equal or less than RL, but not equal to short circuit therefore not detectable by a Digital Input channel of a Safety PLC;
- □ fail "No Effect": failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure or 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. It is also not considered for the total failure rate (safety function) evaluation.

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	10.40
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	206.10
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**216.50**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**527 years**
$\lambda_{no\ effect}$ = "No Effect" failures	224.20
$\lambda_{not\ part}$ = "Not Part" failures	12.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**453.10**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**252 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	206.10 FIT	0.00 FIT	10.40 FIT	95.2%

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

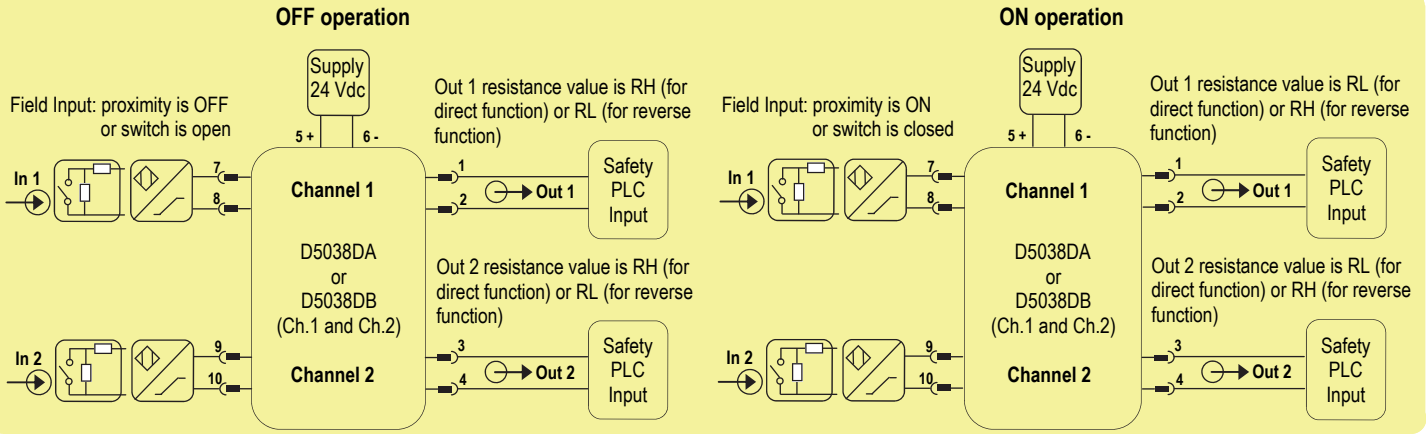
T[Proof] = 1 year	T[Proof] = 2 years
PFDavg = 4.56 E-05 Valid for **SIL 3**	PFDavg = 9.13 E-05 Valid for **SIL 3**

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] = 5 years
PFDavg = 2.28 E-04 Valid for **SIL 3**

SC3: Systematic capability SIL 3.

Application for double channel D5038DA or D5038DB



Description:

For this application, for each channel enable input line fault (open or short) detection and choose direct or reverse input to output transfer function, by set the internal dip-switches in the following mode (for more information, please see the instruction manual ISM0427), where dip 1 and 2 are related to Ch.1 and dip 3 and 4 are related to Ch.2:

Dip-switch position	1	2	3	4
ON/OFF state	ON	OFF (direct) or ON (reverse)	ON	OFF (direct) or ON (reverse)

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). Output Pins 1-2 (for Channel 1) and Output Pins 3-4 (for Channel 2) have got RH (direct function) or RL (reverse function) resistance value for OFF operation, while they have got RL (direct function) or RH (reverse function) resistance value for ON operation. The following table describes for each channel (Channel 1 or Channel 2) the output resistance value 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 1 or Input 2 signal state Pins 7-8 (In 1 - Ch.1) or Pins 9-10 (In 2 - Ch.2)	**Out 1 or Out 2 resistance value Pins 1-2 (Out 1 - Ch.1) or Pins 3-4 (Out 2 - Ch.2)**	**Ch.1 or Ch.2 status yellow LED state**	**Ch.1 or Ch.2 fault red LED state**
Proximity sensor is OFF or switch is open	RH (direct function) or RL (reverse function)	OFF (direct function) ON (reverse function)	OFF
Proximity sensor is ON or switch is closed	RL (direct function) or RH (reverse function)	ON (direct function) OFF (reverse function)	OFF
Independently from proximity sensor or switch state, input line is broken	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON
Independently from proximity sensor or switch state, input line is short circuited	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON

Safety Function and Failure behavior:

D5038D is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
For each channel, the failure behaviour is described from the following definitions :

- □ fail-Safe State: it is defined as two cases: 1st) the channel output being open, with output resistance equal or bigger than RH ; 2nd) the channel output being in short circuit, with output resistance equal to zero or very little than RL. The module output must be monitored by a Digital Input channel of a Safety PLC in order to detect open circuit (very high resistance) or short circuit (very low resistance) of output channel;
- □ 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 channel output is blocked in closed position, with output resistance equal or less than RL, but not equal to short circuit therefore not detectable by a Digital Input channel of a Safety PLC;
- □ fail "No Effect": failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure or 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. It is also not considered for the total failure rate (safety function) evaluation.

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	10.40
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	211.70
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**222.10**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**514 years**
$\lambda_{no\ effect}$ = "No Effect" failures	244.90
$\lambda_{not\ part}$ = "Not Part" failures	337.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**804.70**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**142 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	211.70 FIT	0.00 FIT	10.40 FIT	95.3%

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

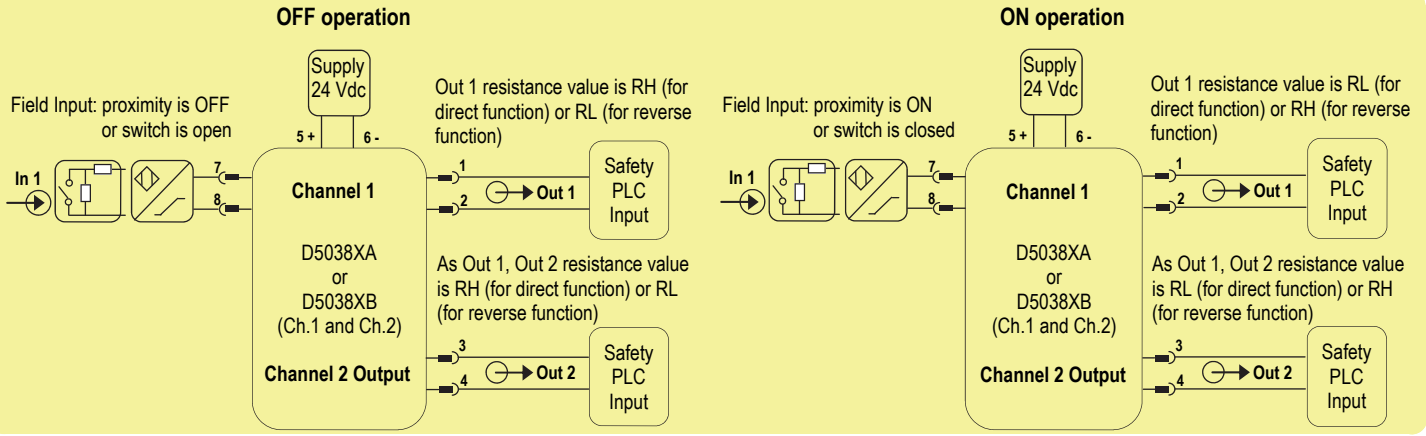
T[Proof] = 1 year	**T[Proof] = 2 years**
PFDavg = 4.56 E-05 Valid for **SIL 3**	PFDavg = 9.13 E-05 Valid for **SIL 3**

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] = 5 years
PFDavg = 2.28 E-04 Valid for **SIL 3**

SC3: Systematic capability SIL 3.

Application for duplicator D5038XA or D5038XB



Description:

For this application, for Channel 1 enable input line fault (open or short) detection and choose direct or reverse input to output transfer function, by set the internal dip-switches in the following mode (for more information, please see the instruction manual ISM0427):

Dip-switch position	1	2	3	4
ON/OFF state	ON	OFF (direct) or ON (reverse)	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). Output Pins 1-2 (for Channel 1) and Output Pins 3-4 (for Channel 2) have got RH (direct function) or RL (reverse function) resistance value for OFF operation, while they have got RL (direct function) or RH (reverse function) resistance value for ON operation. The following table describes for Channel 1 and Channel 2 the output resistance value when Channel 1 input signal is in OFF or ON state, and it gives information about turn-on or turn-off of Channel 1 status LED and Channel 1 fault LED:

Input 1 signal state Pins 7-8 (In 1 - Ch.1)	**Out 1 or Out 2 resistance value Pins 1-2 (Out 1 - Ch.1) or Pins 3-4 (Out 2 - Ch.2)**	**Ch.1 status yellow LED state**	**Ch.1 fault red LED state**
Proximity sensor is OFF or switch is open	RH (direct function) or RL (reverse function)	OFF (direct function) ON (reverse function)	OFF
Proximity sensor is ON or switch is closed	RL (direct function) or RH (reverse function)	ON (direct function) OFF (reverse function)	OFF
Independently from proximity sensor or switch state, input line is broken	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON
Independently from proximity sensor or switch state, input line is short circuited	RH (direct or reverse function) as safe state condition	OFF (direct or reverse function)	ON

Safety Function and Failure behavior:

D5038X is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
For each output channel, the failure behaviour is described from the following definitions :

- □ fail-Safe State: it is defined as two cases: 1st) the channel output being open, with output resistance equal or bigger than RH ; 2nd) the channel output being in short circuit, with output resistance equal to zero or very little than RL. The module output must be monitored by a Digital Input channel of a Safety PLC in order to detect open circuit (very high resistance) or short circuit (very low resistance) of output channel;
- □ 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 channel output is blocked in closed position, with output resistance equal or less than RL, but not equal to short circuit therefore not detectable by a Digital Input channel of a Safety PLC;
- □ fail "No Effect": failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure or 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. It is also not considered for the total failure rate (safety function) evaluation.

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	10.40
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	206.20
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**216.60**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**527 years**
$\lambda_{no\ effect}$ = "No Effect" failures	225.00
$\lambda_{not\ part}$ = "Not Part" failures	202.90
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**644.50**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**177 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	206.20 FIT	0.00 FIT	10.40 FIT	95.2%

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] = 1 year	**T[Proof] = 2 years**
PFDavg = 4.56 E-05 Valid for **SIL 3**	PFDavg = 9.13 E-05 Valid for **SIL 3**

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] = 5 years
PFDavg = 2.28 E-04 Valid for **SIL 3**

SC3: 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 detected 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 consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each channel, change the state conditions of the input sensors/contacts coming from field and verify, by ohmmeter connect to output terminals, that output resistance change value from RL to RH or vice versa (according to direct or reverse function setting up by Dip-switches). RL and RH measured values must be equivalent to RL and RH values within ±5% tolerance, defined on related product instruction manual .
3	For each channel, if input line fault detection is enable by Dip-switches specific set up, disconnect the input wiring coming from the field sensor/contact and check, by ohmmeter connect to output terminals, that output resistance goes to RH value. Then, put in short condition the input connections and verify again that output resistance goes to RH value. RH measured values must be equivalent to RH values within ±5% tolerance, defined on related product instruction manual. In both case the related channel alarm LED, on the front panel, must be turned on with red light.
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.