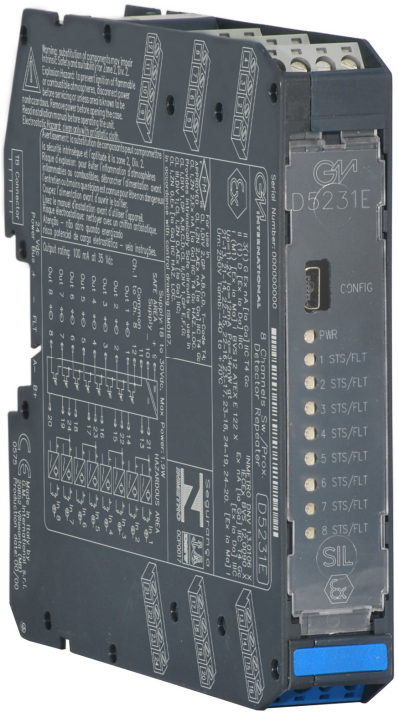


SAFETY MANUAL

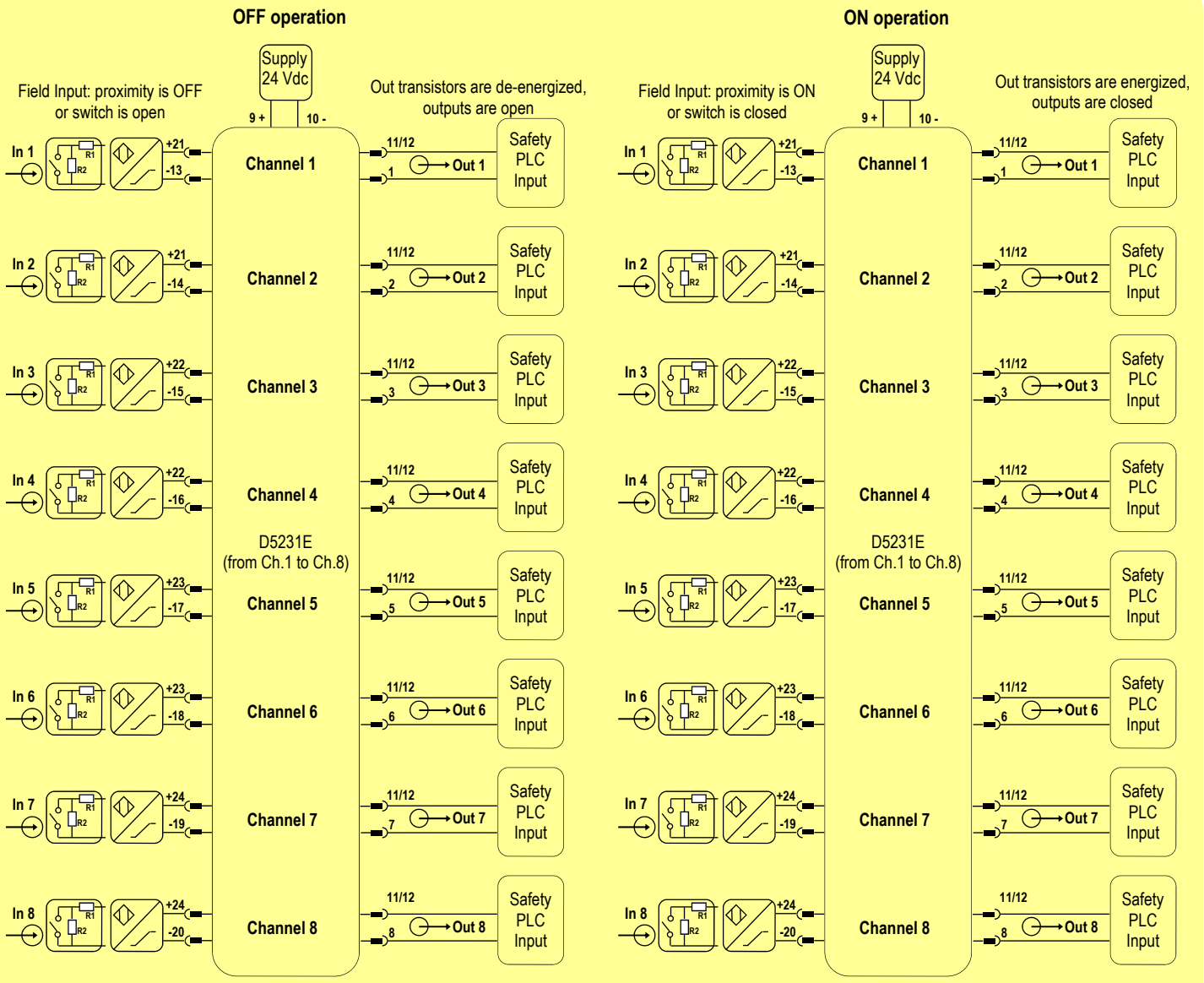
SIL 2 Switch / Proximity Detector Repeater, Open Collector Output DIN-Rail and Termination Board, Model D5231E

Approval: TÜV Certificate No. TUV IT 26 SIL 0725 A, 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 ISM0172 and ISM0154 (for SWC5090 Configuration Software instruction manual), which contain basic guides for the installation and configuration of the equipment.

gmi technology for safety

Application for D5231E



WARNING: R1 and R2 end of line resistors with voltage free contact are required for line fault detection

Description:

By means of SWC5090 Configuration Software, as user interface on a PC to comunicate with the module, select for 1 to 8 channels:

- Input - Sensor type = "proximity", also if switches are used;
- Output - Contact position when input is open = "open";
- Output - Contact position in case of fault = "open".

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.
Input signals from field are applied to Pins 21-13 (In 1 - Ch.1), Pins 21-14 (In 2 - Ch.2), Pins 22-15 (In 3 - Ch.3), Pins 22-16 (In 4 - Ch.4), Pins 23-17 (In 5 - Ch.5), Pins 23-18 (In 6 - Ch.6), Pins 24-19 (In 7 - Ch.7), Pins 24-20 (In 8 - Ch.8).
In case of 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 R1 and R2 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.
Transistor outputs Pins 1-11/12 (for Channel 1), Pins 2-11/12 (for Channel 2), Pins 3-11/12 (for Channel 3), Pins 4-11/12 (for Channel 4), Pins 5-11/12 (for Channel 5), Pins 6-11/12 (for Channel 6), Pins 7-11/12 (for Channel 7), Pins 8-11/12 (for Channel 8) are normally open (or transistor de-energized as safe state condition) for OFF operation, while they are closed (or transistor 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 21-13 (In 1 - Ch.1) or Pins 21-14 (In 2 - Ch.2) or Pins 22-15 (In 3 - Ch.3) or Pins 22-16 (In 4 - Ch.4) or Pins 23-17 (In 5 - Ch.5) or Pins 23-18 (In 6 - Ch.6) or Pins 24-19 (In 7 - Ch.7) or Pins 24-20 (In 8 - Ch.8)**	**Transistor output state** **Pins 1-11/12 (for Ch 1) or Pins 2-11/12 (for Ch 2) or Pins 3-11/12 (for Ch 3) or Pins 4-11/12 (for Ch 4) or Pins 5-11/12 (for Ch 5) or Pins 6-11/12 (for Ch 6) or Pins 7-11/12 (for Ch 7) or Pins 8-11/12 (for Ch 8)**	**Channel status / fault yellow / red LED state**
Proximity sensor is OFF or switch is open	Open (De-energize transistor)	OFF
Proximity sensor is ON or switch is closed	Closed (Energized transistor)	ON (yellow)
Independently from proximity sensor or switch state, the input line is break	Open (De-energized transistor as safe state condition)	ON (red)
Independently from proximity sensor or switch state, the input line is in short circuit	Open (De-energized transistor as safe state condition)	ON (red)

Safety Function and Failure behavior:

D5231E is considered to be operating in Low Demand mode, as a Type B 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 the output transistor being de-energized or 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 output transistor remains closed;
- □ fail Dangerous Detected: a dangerous failure which has been detected from module internal diagnostic so that output transistor is forced to be de-energized (that is to Fail-Safe state), so that it goes open;
- □ 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 is 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	108.78
λ_{du} = Total Dangerous Undetected failures	23.35
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	131.48
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**263.61**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**433 years**
$\lambda_{no\ effect}$ = "No effect" failures	218.07
$\lambda_{not\ part}$ = "Not Part" failures	393.90
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**875.58**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**130 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	131.48 FIT	108.78 FIT	23.35 FIT	82.33%	91.14%

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 = 82.33 % ≥ 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] = 9 years
PFDavg = 1.03 E-04 Valid for **SIL 2**	PFDavg = 9.30 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 = 2.07 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 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 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 PLC or take any other appropriate action to avoid a false trip.
2	Vary the state condition of the input switches/proximity detectors coming from field and verify that the related transistor outputs change from de-energized to energized and vice versa; then, check that the de-energized state condition corresponds to the required Safety Function.
3	If input line fault detection is enabled for each channel by means of the configuration software, disconnect the input wiring coming from the field sensor/contact and check that the corresponding transistor output is de-energized. Then, put in short circuit condition the input connections and verify that the same output remains de-energized.
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 switch/proximity repeater.