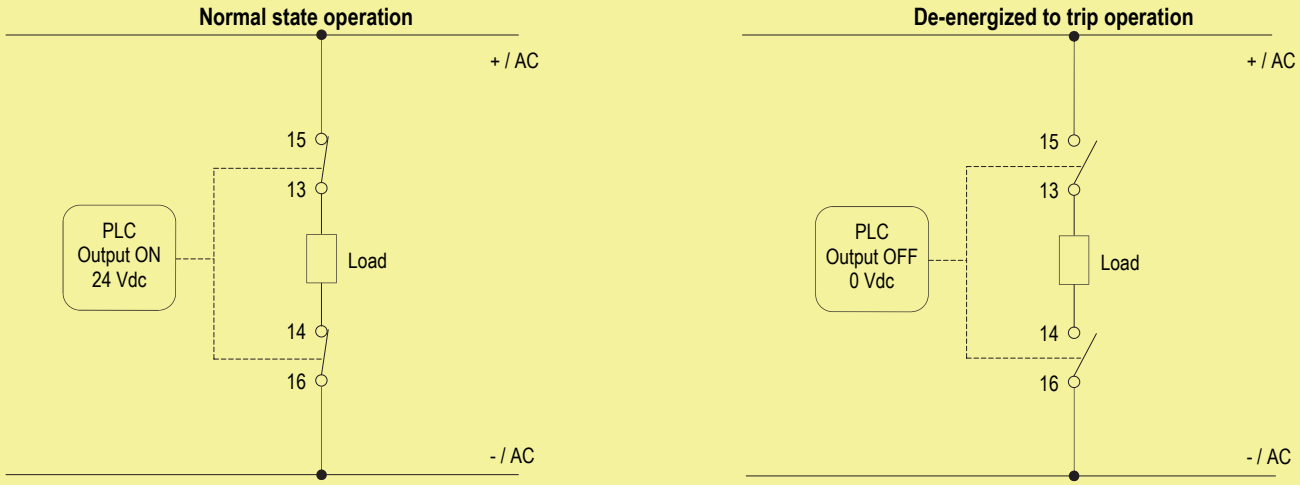
SAFETY MANUAL

5 A SIL 3 Relay Output Module for NE Load, with full diagnostic and Modbus, DIN-Rail, Power Bus and Termination Board, Model D5293S

Reference must be made to the relevant sections within the instruction manual ISM0122, which contain basic guides for the installation of the equipment.

gmi technology for safety

1) Application for D5293S - SIL 3 for NE Load with interruption of both load supply lines



Description:

Input Signal from PLC/DCS is normally High (24 Vdc) and is applied to pins 1-2 in order to Normally Energize (NE) the internal relays.
Input Signal from PLC/DCS is Low (0 Vdc) during "de-energized to trip" operation, in order to de-energize the internal relays.
The Load is Normally Energized (NE), therefore its safe state is to be de-energized.
Disconnection of the NE Load is done on both supply lines.
The following table describes the status (open or closed) of each output contact when the input signal is High or Low.

Operation	Input Signal Pins 1-2	Pins 15 - 13	Pins 16 - 14	NE Load (SIL3) Pins 13 - 14
Normal	High (24 Vdc)	Closed	Closed	Energized
Trip	Low (0 Vdc)	Open	Open	De-Energized

Safety Function and Failure behavior:

D5293S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
In this Functional Safety application, the normal state operation of relay module is energized, with NE (Normally Energized) load.
In case of alarm or request from process, the relay module is de-energized (safe state), de-energizing the load.
The failure behaviour of the relay module is described by the following definitions:

- □ fail-Safe State: it is defined as the output load being de-energized;
- □ fail Safe: this failure causes the system to go to the defined fail-safe state without a process demand;
- □ 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 load remains energized.
- □ fail "No effect": failure mode of a component that plays a part in implementing the safety function but 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	0.00
λ_{du} = Total Dangerous Undetected failures	1.72
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	130.74
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**132.46**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**861 years**
$\lambda_{no\ effect}$ = "No effect" failures	97.94
$\lambda_{not\ part}$ = "Not Part" failures	454.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**684.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**166 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	130.74 FIT	0.00 FIT	1.72 FIT	98.70%

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

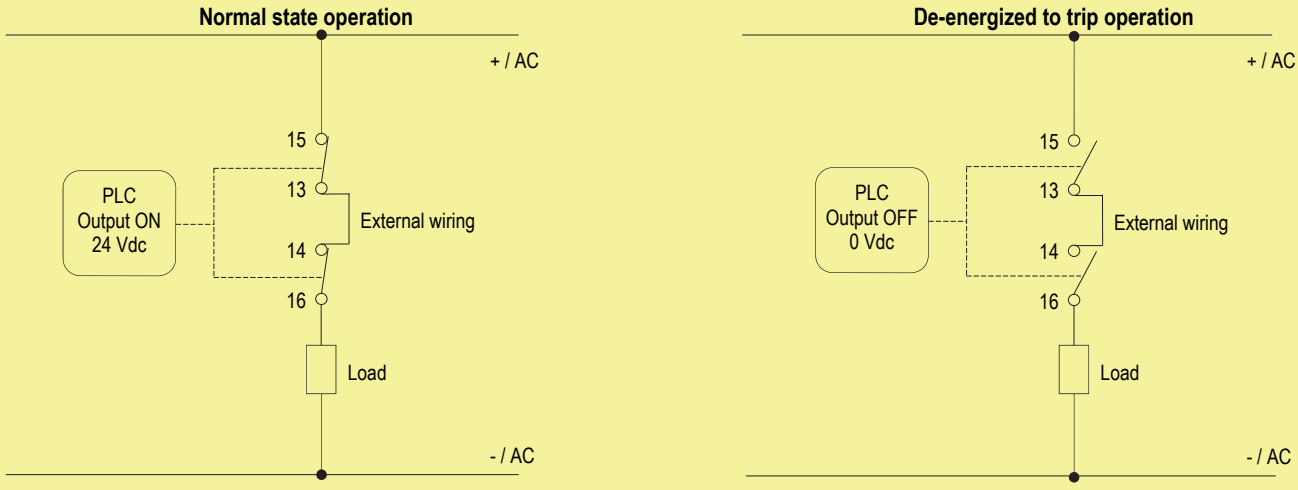
T[Proof] = 1 year	T[Proof] = 13 years
PFDavg = 7.55 E-06 - Valid for **SIL 3**	PFDavg = 9.81 E-05 - Valid for **SIL 3**

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] = 20 years
PFDavg = 1.51 E-04 - Valid for **SIL 3**

SC 3: Systematic capability SIL 3.

2) Application for D5293S - SIL 3 for NE Load with interruption of only one load supply line



Description:

Input Signal from PLC/DCS is normally High (24 Vdc) and is applied to pins 1-2 in order to Normally Energize (NE) the internal relays.
Input Signal from PLC/DCS is Low (0 Vdc) during "de-energized to trip" operation, in order to de-energize the internal relays.
The Load is Normally Energized (NE), therefore its safe state is to be de-energized.
Disconnection of the NE Load is done on only one load supply line. By SWC5090 Configuration & Monitoring Software set the following option to enable unipolar load interruption feature: "Module —> Advanced Options —> Load interruption —> Unipolar".
The following table describes the status (open or closed) of each output contact when the input signal is High or Low.

Operation	Input Signal Pins 1-2	Pins 15 - 13	Pins 16 - 14	NE Load (SIL3) Pins 13 - 14
Normal	High (24 Vdc)	Closed	Closed	Energized
Trip	Low (0 Vdc)	Open	Open	De-Energized

Safety Function and Failure behavior:

D5293S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
In this Functional Safety application, the normal state operation of relay module is energized, with NE (Normally Energized) load.
In case of alarm or request from process, the relay module is de-energized (safe state), de-energizing the load.
The failure behaviour of the relay module is described by the following definitions:

- □ fail-Safe State: it is defined as the output load being de-energized;
- □ fail Safe: this failure causes the system to go to the defined fail-safe state without a process demand;
- □ 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 load remains energized.
- □ fail "No effect": failure mode of a component that plays a part in implementing the safety function but 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	0.00
λ_{du} = Total Dangerous Undetected failures	1.72
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	130.74
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**132.46**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**861 years**
$\lambda_{no\ effect}$ = "No effect" failures	97.94
$\lambda_{not\ part}$ = "Not Part" failures	454.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**684.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**166 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	130.74 FIT	0.00 FIT	1.72 FIT	98.70%

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

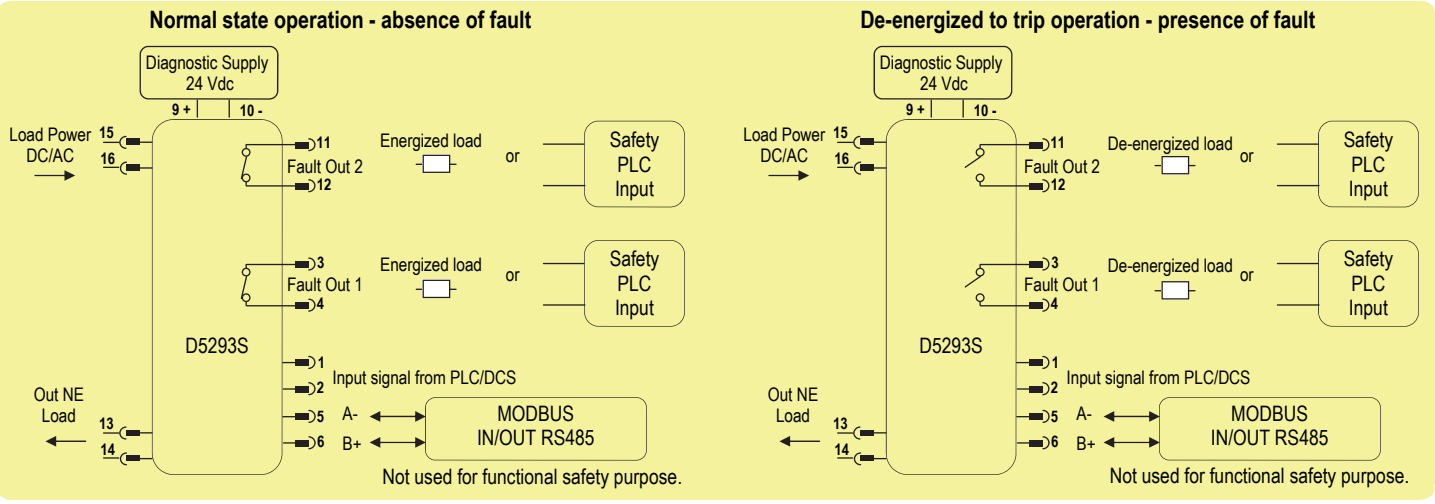
T[Proof] = 1 year	T[Proof] = 13 years
PFDavg = 7.55 E-06 - Valid for **SIL 3**	PFDavg = 9.81 E-05 - Valid for **SIL 3**

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] = 20 years
PFDavg = 1.51 E-04 - Valid for **SIL 3**

SC 3: Systematic capability SIL 3.

Diagnostic Application for D5293S - SIL 2 Fault Relay Outputs with NO contacts



Description:

In this application D5293S module monitors Load Power DC/AC line (Pins 15-16) and Out NE Load (Pins 13-14) by internal diagnostic circuits and uses Fault Out 1 or Fault Out 2 NO contact to signal presence of faults on them. See Instruction Manual "SWC5090 Configuration & Monitoring Software" section to configure and to monitor the diagnostic operation parameters (as fault conditions), by means of Modbus IN/OUT protocol with RS485 connection (Pins 5-6) or by PPC5092 adapter and SWC5090 related software.
When diagnostic supply is connected to Pins 9(+) - 10(-), the power green led is ON. NE load connected on Pins 13-14 is controlled by input signal Pins 1-2 from PLC/DCS.
As shown in the diagram, Fault Output (Out 1 or Out 2) contact can be connected to Safety PLC Input or used to (de-)energize a load by switching its supply lines.
Fault relay contact (Pins 3-4 for Fault Out 1 or 11-12 for Fault Out 2) is closed in normal state operation, that is absence of faults, energizing related load. This function is valid if "inverted fault relay" parameter is set to "0" or its field is not checked as explained on "SWC5090 Configuration & Monitoring Software" section. In case of faults detected by internal diagnostic circuits, de-energized to trip operation is applied to fault relay and its contacts become open, de-energizing related load.
The following table describes the status (open or closed) of each fault output contact in absence or presence of faults detected by internal diagnostic circuits:

Operation	Fault Out 1 contact (Pins 3-4)	Fault Out 2 contact (Pins 11-12)
Normal (absence of fault)	Closed	Closed
Trip (presence of fault)	Open	Open

Safety Function and Failure behavior:

D5293S is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of SPST fault relay output with NO contact and without "invert fault relay" condition by the following definitions:

- □ Fail-Safe State: it is defined as the fault relay output being de-energized, with open contact and de-energized fault output load;
- □ Fail Safe: this failure causes the system to go to the defined Fail-Safe state without a process demand;
- □ 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 fault relay remains energized or fault relay contact keeps closed (energizing fault output load) because of diagnostic measure error more than +/-20% of correct value or due to contact welding;
- □ 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; in particular, diagnostic measure error is less than +/-20% of correct value. 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 input and relay blocks failures are classified as "Not Part" failures.

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 date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	59.59
λ_{du} = Total Dangerous Undetected failures	39.54
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	161.70
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**260.83**
MTBF (safety function, fault relay outputs) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**437 years**
$\lambda_{no\ effect}$ = "No effect" failures	105.26
$\lambda_{not\ part}$ = "Not Part" failures	318.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**684.79**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**166 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	161.70 FIT	59.59 FIT	39.54 FIT	60.11%	84.84%

where DC means the dangerous diagnostic coverage for the Line and Load by internal diagnostic circuits. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 60.11 % ≥ 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] = 5 years	T[Proof] = 20 years
PFDavg = 1.74 E-04 - Valid for **SIL 2**	PFDavg = 8.70 E-04 - Valid for **SIL 2**	PFDavg = 3.48 E-03 - Valid for **SIL 1**

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] = 11 years
PFDavg = 1.91 E-03 - Valid for **SIL 2**

SC 3: Systematic capability SIL 3.

Testing procedure at T-proof for functional safety relay applications 1) or 2)

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostics. 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.
Before of specific Proof test, execute the following General proof test: connect the load supply lines to terminal blocks "15" (for +/AC) and "16" (-/AC) and the NE output load to terminal blocks "13" (as the positive terminal) and "14" (as the negative terminal); finally, connect the DCS/PLC signal to input channel terminal blocks "1" (as the positive terminal) and "2" (as the negative terminal). Then, verify the input to output functionality: the output NE load is Normally Energized by supplying the input channel, while shutdown of the input channel de-energizes (safe state) the load. The channel functionality must be verified for a min to max input voltage change (21.6 to 27.6 Vdc).

Then, disconnect the load supply lines from terminal blocks "15" - "16" and the output load from terminal blocks "13" - "14". Then, connect an ohmmeter (Ohm. A) between terminal blocks "15" - "13" and another one (Ohm. B) between terminal blocks "16" - "14". The Specific 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 when removing the unit for test.
2	1. Do not supply the input channel (terminals "1"-"2") of the unit under test and verify that ohmmeters Ohm. A and Ohm. B measure absence of ohmic continuity (i.e. both +/AC and -/AC load lines are interrupted because the NO contacts are open: **the 1st requisite is verified**). The presence of ohmic continuity measured by ohmmeter Ohm. A or Ohm. B implies that the related relay contact is blocked (for welding) in the closed position . 2. Supply the input channel (terminals "1"-"2") of the unit under test and verify that ohmmeters Ohm. A and Ohm. B measure presence of ohmic continuity (i.e. both +/AC and -/AC load lines are not interrupted because all NO contacts are closed: **the 2nd requisite is verified**). The absence of ohmic continuity measured by ohmmeter Ohm. A or Ohm. B implies that the related relay contact is blocked (for welding) in the open position.
3	Remove the bypass from the safety-related PLC or restore normal operation inserting the unit.

This test reveals almost 99 % of all possible Dangerous Undetected failures in the relay module.

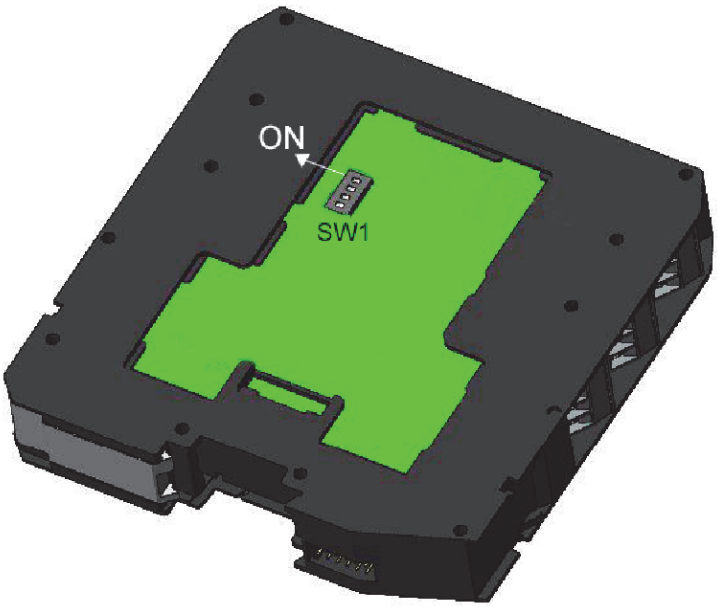
Testing procedure at T-proof for functional safety diagnostic application

The proof test will be performed to reveal dangerous faults which cannot be otherwise detected. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA analysis, can be revealed during the proof test.
When the diagnostic circuits of D5293S are used with the 1 +1 SPST fault relay output, the Proof Test consists of the following steps:

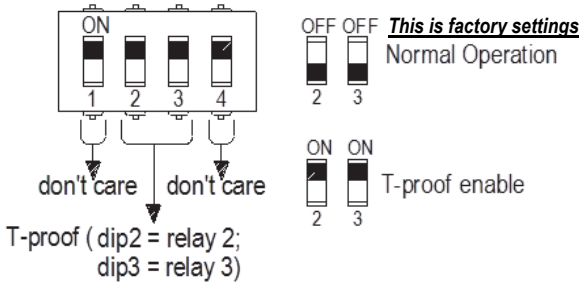
Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	By means of the configuration software, configure each fault relay output to be energized with closed contacts in normal operation and de-energized with open contacts when a fault condition occurs. Connect an ohmmeter to each couple of relay contacts and verify that, during the modules normal operation, the fault relay outputs are energized with presence of ohmic continuity between their contacts.
3	Impose a coil short circuit fault condition by means of the SW1 dip-switch (dip-2 or dip-3), which can simulate a short circuit of any the output relay coils, with the condition of enable the coil integrity by means of the module configuration software. Verify that, during fault condition, the fault relay outputs are de-energized with absence of ohmic continuity between their contacts. Finally, remove the output relay coil short circuit (by means of the SW1 dip-switch) and verify that the fault relay outputs are switched to the energized state with presence of ohmic continuity between their contacts.
4	Impose a fault condition to any of the analog measures (load supply voltage, load current, load resistance) performed by the modules. That means to impose a load supply voltage or a load current or a load resistance value outside up to 20% of the limit range (for each analog measure) set by means of the module configuration software. Verify that, during fault condition, the fault relay outputs are de-energized with absence of ohmic continuity between their contacts. Finally, remove the fault condition and verify that the fault relay outputs are switched to the energized state with presence of ohmic continuity between their contacts. Perform this test when the module output relays are both in the energized and de-energized states.
5	Restore the loop to full operation
6	Remove the bypass from the Safety-related PLC or restore normal operation.

This test will reveal approximately 99% of the possible Dangerous Undetected failures in the diagnostic circuits of D5293S when the fault relay output is considered.

For configuration of T-proof diagnostic circuits testing, some DIP Switches are located on component side of pcb.
These switches allow the T-proof diagnostic circuit test (SW1 dip-switch: 2 or 3 set "ON" and see "Testing procedure at T-proof for functional safety diagnostic application").



SW1 Dip switch configuration



WARNING: **after T-proof test, dip-switch 2-3 must be set to "OFF" position for normal operation.**