INSTRUCTION & SAFETY MANUAL

10 A SIL 3 Relay Output Module for NE Load, DIN-Rail and Termination Board, Model D5290S/SA for Safe Area only

technology for safety

Characteristics

General Description: The single channel Relay Output, D5290S/SA is a relay module suitable for the switching of safety related circuits, up to SIL 3 level according to IEC 61508:2010 Ed.2 for high risk industries. It provides isolation between input and output contacts.

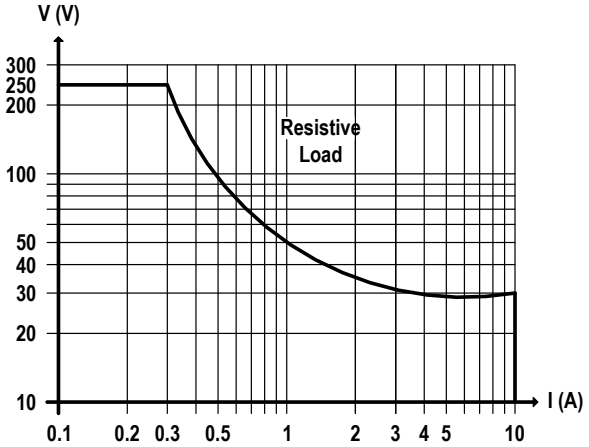
D5290S/SA provides two NO contacts for normally energized load and a NC contact for service purpose, in order to switch the NE load on both supply lines.
Compatibility with specific DO cards with pulse testing needs to be verified.
This relay module is not suitable for low-current consumption applications (system-to-system signalling, driving LEDs, etc.).
See the following pages for Functional Safety applications with related SIL value.

Mounting on standard DIN-Rail, installation in Safe Area.

Functional Safety Management Certification:
G.M. International is certified by TUV to conform to IEC61508:2010 part 1 clauses 5-6 for safety related systems up to and included SIL3.

Technical Data

Input: 24 Vdc nom (21.6 to 27.6 Vdc) reverse polarity protected, ripple within voltage limits ≤ 5 Vpp.
Current consumption @ 24 V: 40 mA with relay energized, typical.
Power dissipation: 1 W with 24 V input voltage, relay energized, typical.
Isolation (Test Voltage): Input / All Outputs 2.5 KV ; Out 1 / Out 2: 500 V.
Output: 1 voltage free SPDT relay contact identified with outputs: Out 1 (NO contact) terminals 13-21 and Service Load Out (NC contact) terminals 13-15;
1 voltage free SPST relay contact identified with output Out 2 (NO contact) terminals 14-22.
Terminals 13-21 (Out 1) and 14-22 (Out 2) are open when relay is de-energized, closed in energized relay condition.
Service load output (not SIL) at terminals 13-15 is normally close when relay is de-energized, open in energized relay condition.
Contact material: Ag Alloy (Cd free) or $AgSnO_2$.
Contact rating: 10 A 250 Vac 2500 VA, 10 A 250 Vdc 300 W (resistive load).
Contact inrush current: 16 A at 24 Vdc, 250 Vac.
Contact min. switching current: 100 mA.
DC Load breaking capacity:



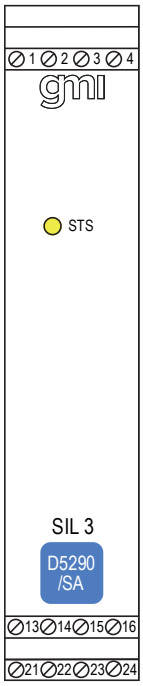
Mechanical / Electrical life: $10 * 10^6 / 5 * 10^4$ operation, typical.
Operate / Release time: 8 / 8 ms, typical.
Frequency response: 10 Hz maximum.
Compatibility:
CE mark compliant, conforms to Directive: 2014/30/EU EMC, 2014/35/EU LVD, 2011/65/EU RoHS.
Environmental conditions:
Operating: temperature limits – 40 to + 70 °C, relative humidity 95 %, up to 55 °C.
Storage: temperature limits - 45 to + 80 °C.
Approvals:.
TÜV Certificate No. C-IS-236198-04, SIL 3 conforms to IEC61508:2010 Ed.2.
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.
DNV No. TAA00001U0 and KR No. MIL20769-EL002 Certificates for maritime applications.
Mounting:
EN/IEC60715 TH 35 DIN-Rail or on customized Termination Board.
Weight: about 150 g.
Connection: by polarized plug-in disconnect screw terminal blocks to accommodate terminations up to 2.5 mm^2.
Location: installation in Safe Area.
Protection class: IP 20.
Dimensions: Width 22.5 mm, Depth 123 mm, Height 120 mm.

Ordering Information

Model: D5290S/SA

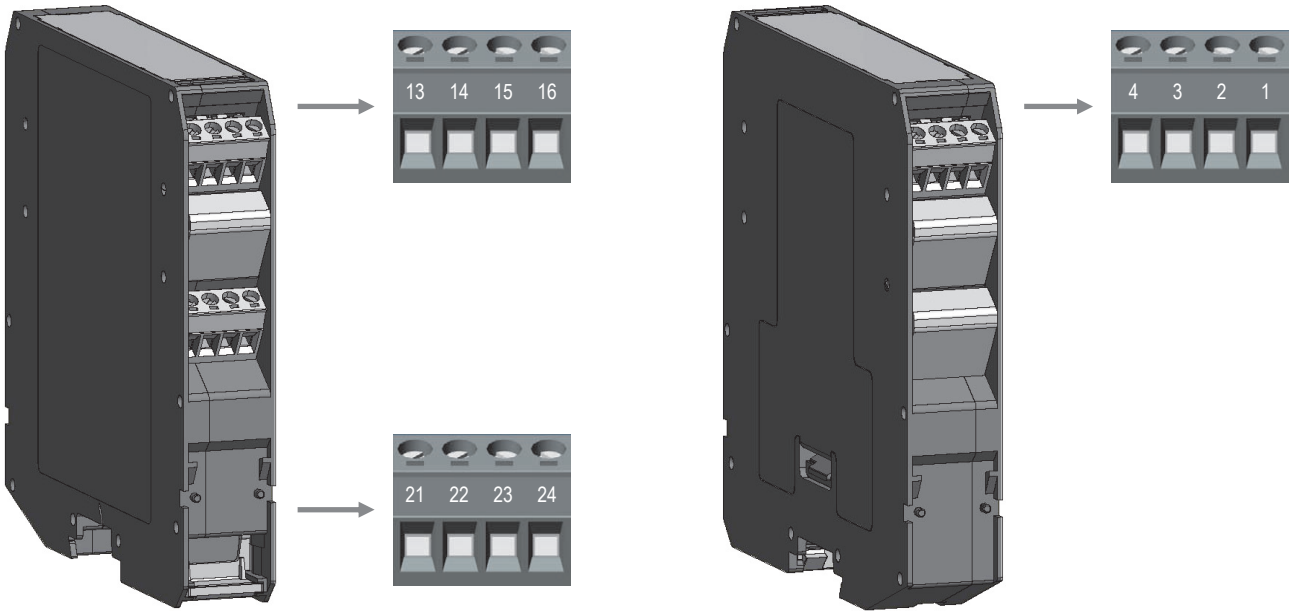
DIN-Rail accessories: Cover and fix MCHP196

Front Panel and Features



- SIL 3 according to IEC 61508:2010 Ed. 2 for Tproof = 14 / 20 yrs (≤10% / >10 % of total SIF).
- PFDavg (1 year) 7.01 E-06, SFF 98.38 % for NE Load.
- Systematic capability SIL 3.
- 10 A SIL 3 contact for NE load and contact for service purpose.
- 16 A inrush current at 24 Vdc / 250 Vac.
- Input/Output isolation.
- EMC Compatibility to EN61000-6-2, EN61000-6-4, EN61326-1, EN61326-3-1 for safety system.
- TÜV Certification.
- TÜV Functional Safety Certification.
- Type Approval Certificate DNV and KR for maritime applications.
- Simplified installation using standard DIN-Rail and plug-in terminal blocks or customized Termination Boards.

Terminal block connections



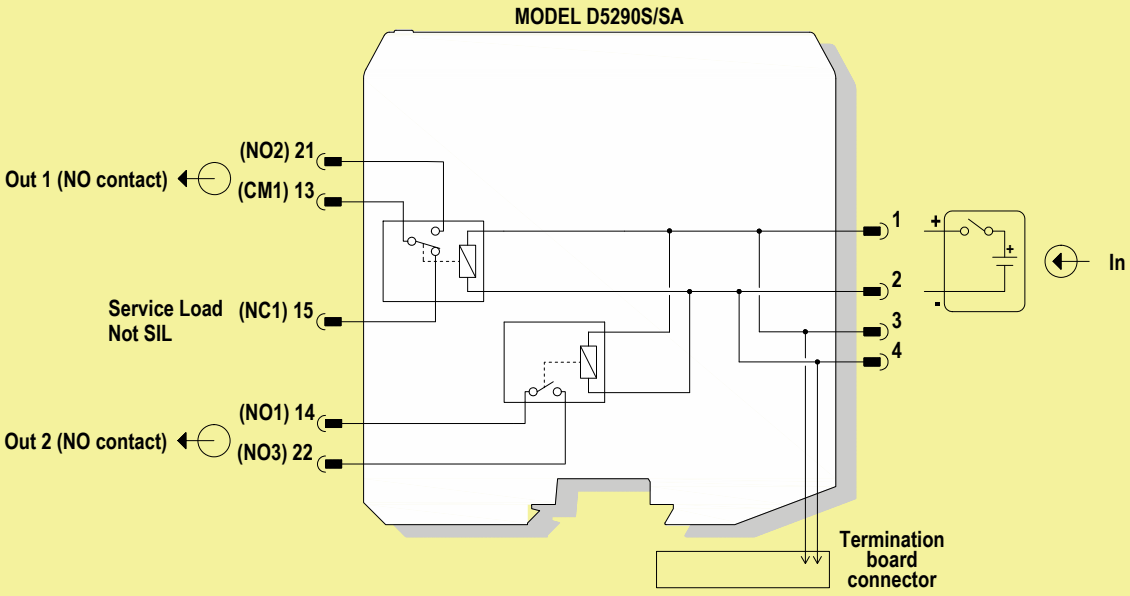
SAFE AREA

13	CM1 Common pole of: Normally Open contact (Out 1) and Normally Closed contact (Service Load (Not SIL) out)
14	NO1 pole of Normally Open contact (Out 2)
15	NC1 pole of Normally Closed contact (Service Load (Not SIL) out)
16	Not used
21	NO2 pole of Normally Open contact (Out 1)
22	NO3 pole of Normally Open contact (Out 2)
23	Not used
24	Not used

1	+ Input
2	- Input
3	+ Input
4	- Input

Function Diagram

SAFE AREA

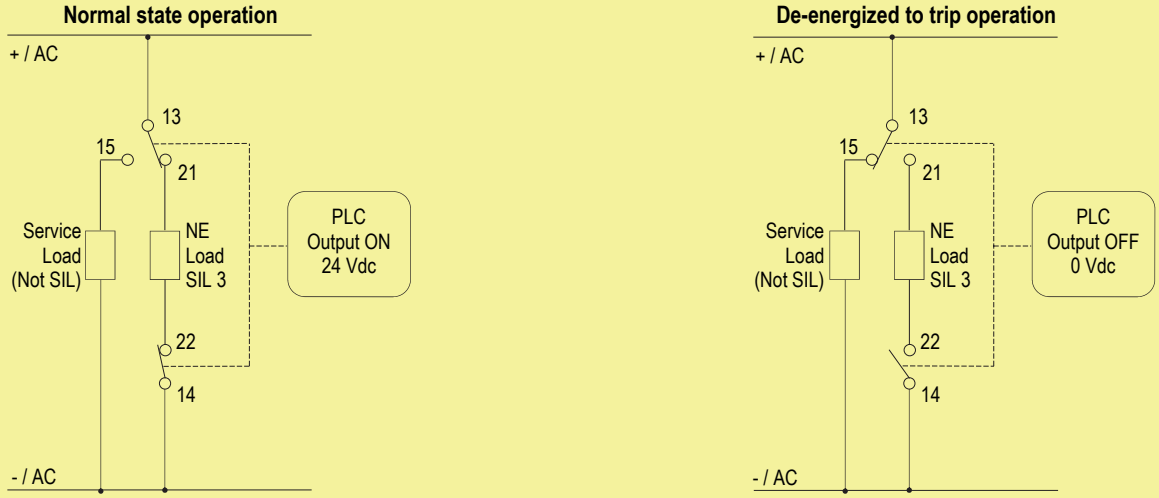


See the following pages for Functional Safety applications with related SIL value.

Relay contact shown in de-energized position.
Terminals 13-21 and 14-22 are open; terminal 13-15 is closed.

To prevent relay contacts from damaging, connect an external protection (fuse or similar), chosen according to the relay breaking capacity diagram.

1) Application D5290S/SA - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay, 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 or 3-4 in order to Normally Energize (NE) the internal relays.
Input Signal from PLC/DCS is Low (0 Vdc) during "de-energize to trip" operation, in order de-energize the internal relays.
The Load is Normally Energized (NE), therefore its safe state is to be de-energized; the Service Load is normally de-energized, therefore it energizes during "de-energized to trip" operation.
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 or 3-4	Pins 13- 21	Pins 14 - 22	Pins 13 - 15	NE Load (SIL3) Pins 21 - 22	Service Load (Not SIL) Pins 15 — - / AC Supply
Normal	High (24 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	Low (0 Vdc)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5290S/SA is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
In the 1st 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 data: 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	1.60
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	97.20
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**98.80**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1155 years**
$\lambda_{no\ effect}$ = "No effect" failures	88.40
$\lambda_{not\ part}$ = "Not Part" failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**187.20**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**609 years**
$MTTF_S$ (Total Safe) = 1 / ($\lambda_{sd} + \lambda_{su}$)	1174 years
$MTTF_D$ (Dangerous) = 1 / λ_{du}	71347 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	97.20 FIT	0.00 FIT	1.60 FIT	98.38%

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

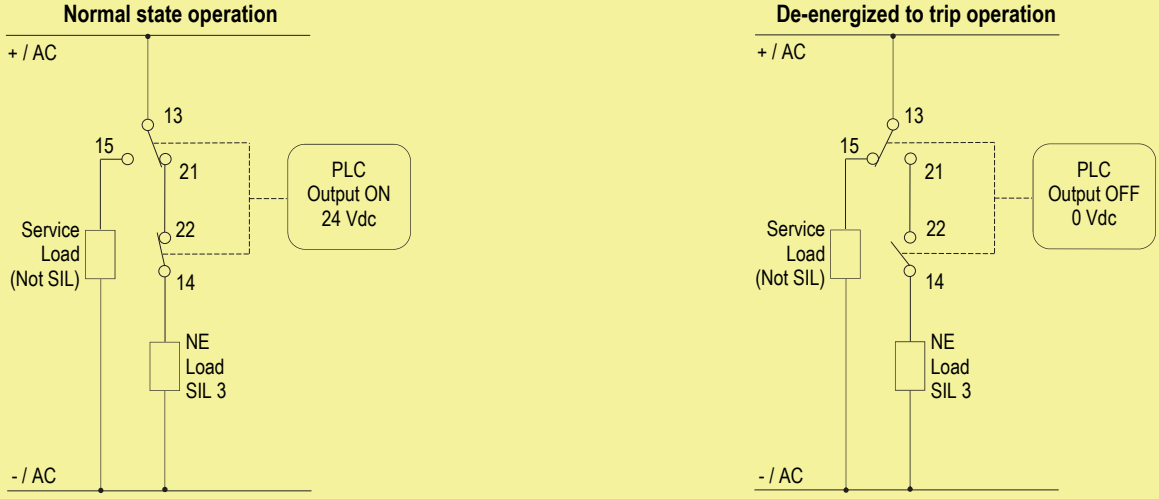
T[Proof] = 1 year	T[Proof] = 14 years
PFDavg = 7.01 E-06 - Valid for **SIL 3**	PFDavg = 9.81 E-05 - Valid for **SIL 3**

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 = 1.40 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

2) Application D5290S/SA - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay, 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 or 3-4 in order to Normally Energize (NE) the internal relays.
Input Signal from PLC/DCS is Low (0 Vdc) during "de-energize to trip" operation, in order de-energize the internal relays.
The Load is Normally Energized (NE), therefore its safe state is to be de-energized; the Service Load is normally de-energized, therefore it energizes during "de-energized to trip" operation.
Disconnection of the NE Load is done on only one load supply line.
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 or 3-4	Pins 13 - 21	Pins 14 - 22	Pins 13 - 15	NE Load (SIL3) Pins 14 — - / AC Supply	Service Load (Not SIL) Pins 15 — - / AC Supply
Normal	High (24 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	Low (0 Vdc)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5290S/SA is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
In the 2nd 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 data: 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	1.60
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	97.20
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**98.80**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1155 years**
$\lambda_{no\ effect}$ = "No effect" failures	88.40
$\lambda_{not\ part}$ = "Not Part" failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**187.20**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**609 years**
$MTTF_S$ (Total Safe) = 1 / ($\lambda_{sd} + \lambda_{su}$)	1174 years
$MTTF_D$ (Dangerous) = 1 / λ_{du}	71347 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	97.20 FIT	0.00 FIT	1.60 FIT	98.38%

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] = 14 years
PFDavg = 7.01 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 = 1.40 E-04 - Valid for **SIL 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 faults, which have been noted during the FMEDA, can be revealed during proof test. 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 when removing the unit for test.
2	For the single channel, verify the input-to-output functionality: the output load is normally energized by supplying the input channel, while shutdown of the input channel de-energizes the load (safe state). The channel functionality must be verified for a min to max input voltage change (21.6 to 27.6 Vdc). In addition, the use of two relays for the single output channel, where the contacts are connected in series, requires to control coil and contact of each relay, as described in the following procedure . 1. Do not supply the input channel (terminals "1"-"2" or "3"-"4") of the unit under test and verify that the ohmic continuity at the Out 1 and Out 2 contacts (terminals "13"-"21" and "14"-"22") is absent (i.e. both Out 1 and Out 2 contacts are open: **1st requisite is verified**). Instead, the presence of ohmic continuity at Out 1 or Out 2 implies that the relay contact 1 or 2 is blocked (for welding) into closed position. 2. Supply the input channel (terminals "1"-"2" or "3"-"4") of the unit under test and verify that the ohmic continuity at the Out 1 and Out 2 contacts (terminals "13"-"21" and "14"-"22") is present (both Out 1 and Out 2 contacts are closed: **2nd requisite is verified**). The absence of ohmic continuity at Out 1 or Out 2 implies that the relay contact 1 or 2 is blocked (for welding) into 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.

Warning

D5290S/SA is an electrical apparatus installed into standard EN50022 T35 DIN-Rail located in Safe Area within the specified operating temperature limits Tamb - 40 to +70 °C.
D5290S/SA must be installed, operated and maintained only by qualified personnel, in accordance to the relevant national/international installation standards, following the established installation rules.
Warning: de-energize main power source (turn off power supply voltage) and disconnect plug-in terminal blocks before opening the enclosure to avoid electrical shock when connected to live hazardous potential.
Failure to properly installation or use of the equipment may risk to damage the unit or severe personal injury.
The unit cannot be repaired by the end user and must be returned to the manufacturer or his authorized representative.
Any unauthorized modification must be avoided.

Operation

D5290S/SA relay module is suitable for the switching of safety related circuits, providing isolation between the input and output contacts.
D5290S/SA provides two NO contacts for normally energized load and a NC contact for service purpose, in order to switch the NE load on both supply lines.
See the previous pages for Functional Safety applications with related SIL value.
A "RELAY STATUS" yellow led lights when input is powered, showing that relay is energized.

Installation

D5290S/SA is a relay output module housed in a plastic enclosure suitable for installation on T35 DIN-Rail according to EN50022 or on customized Termination Board.
D5290S/SA unit can be mounted with any orientation over the entire ambient temperature range.
Electrical connection of conductors up to 2.5 mm² are accommodated by polarized plug-in removable screw terminal blocks which can be plugged in/out into a powered unit without suffering or causing any damage.
The wiring cables have to be proportionate in base to the current and the length of the cable.
On the section "Function Diagram" and enclosure side a block diagram identifies all connections.
Identify the function and location of each connection terminal using the wiring diagram on the corresponding section, as an example (interruption of both NE load supply lines):
Connect positive input at terminal "1" and negative input at "2" (positive input at terminal "3" and negative input at "4" are provided for daisy chain connection to the next module).
Connect positive or AC load supply line to CM1 Common pole (terminal "13" (for SIL 3 NE load and Not SIL Service Load)).
Connect SIL 3 Normally Energized (NE) Load at terminal "21" and "22".
Connect negative or AC load supply line at terminal "14" (for SIL 3 NE load).
Connect Not SIL Service Load at terminal "15" and to negative or AC load supply line.

Installation and wiring must be in accordance to the relevant national or international installation standards, make sure that conductors are well isolated from each other and do not produce any unintentional connection.
Connect SPST relay contacts checking the load rating to be within the contact maximum rating (10 A 250 Vac 2500 VA, 10 A 250 Vdc 300 W resistive load).
To prevent relay contacts from damaging, connect an external protection (fuse or similar), chosen according to the relay breaking capacity diagram on data sheet.
The enclosure provides, according to EN60529, an IP20 minimum degree of mechanical protection (or similar to NEMA Standard 250 type 1) for indoor installation, outdoor installation requires an additional enclosure with higher degree of protection (i.e. IP54 to IP65 or NEMA type 12-13) consistent with the effective operating environment of the specific installation.
Units must be protected against dirt, dust, extreme mechanical (e.g. vibration, impact and shock) and thermal stress, and casual contacts.
If enclosure needs to be cleaned use only a cloth lightly moistened by a mixture of detergent in water.
Any penetration of cleaning liquid must be avoided to prevent damage to the unit. Any unauthorized card modification must be avoided.
Relay output contact must be connected to load non exceeding category II overvoltage limits.
Warning: de-energize main power source (turn off power supply voltage) and disconnect plug-in terminal blocks before opening the enclosure to avoid electrical shock when connected to live hazardous potential.

Start-up

Before powering the inputs of unit check that all wires are properly connected, also verifying their polarity. Check conductors for exposed wires that could touch each other causing dangerous unwanted shorts. Enabling input, the "RELAY STATUS" yellow led must be lit and load circuit must be energized because relay output contacts (Out 1 and Out 2) are closed. Indeed, disabling input, the "RELAY STATUS" yellow led must be turned off and load circuit must be de-energized because relay output contacts (Out 1 and Out 2) are open.