
# INSTRUCTION MANUAL

## 10 A SIL 3 Relay Output Module for ND Load, with ND or NE Relay condition DIN-Rail and Termination Board, Model D5291S

GM INTERNATIONAL
TECHNOLOGY FOR SAFETY

## Characteristics

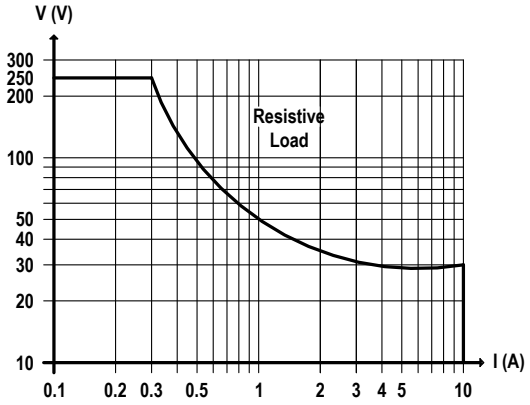
**General Description:** The single channel Relay Output, D5291S is a relay module suitable for the switching of safety related circuits, up to SIL 3 level according to IEC 61508 for high risk industries. It provides isolation between input and output contacts.
Two mutually exclusive (by DIP-Switch programming) monitoring circuits are provided:
1) line input monitoring, to allow DCS/PLC line monitoring function: when enabled, the module permits a wide compatibility towards different DCS/PLC. Driving line pulse testing, executed by DCS/PLC, is permitted by a dedicated internal circuit, to prevent relay and LED flickering.
2) low voltage input monitoring: when enabled, the module reflects a high impedance state to the control unit when the driving voltage is below the specified threshold.

D5291S provides 1 SPDT contact for two different safety functions:
1) SIL 3 Safety Function for Normally De-Energized load (energized in fail safe state) is available at Terminal Blocks 13-14. The driving signal is normally low (0 Vdc), the relay is normally de-energized, contact is open and load is de-energized. The safety function is met when the driving signal is high (24 Vdc), the relay is energized, contact is closed and load is energized. At Terminal Blocks 13-15 is also available a service contact (for service load) with opposite (not SIL) function.
2) SIL 3 Safety Function for Normally De-Energized load (energized in fail safe state) is available at Terminal Blocks 13-15. The driving signal is normally high (24 Vdc), the relay is normally energized, contact is open and load is de-energized. The safety function is met when the driving signal is low (0 Vdc), the relay is de-energized, contact is closed and load is energized. At Terminal Blocks 13-14 is also available a service contact (for service load) with opposite (not SIL) function.

Mounting on standard DIN-Rail or on customized Termination Boards, in Safe Area or in Zone 2.

## Technical Data

**Input:** 24 Vdc nom (21.6 to 27.6 Vdc) reverse polarity protected, ripple within voltage limits ≤ 5 Vpp.
***The following monitoring circuits are mutually exclusive:***
**1)** ***Line input monitoring (DIP-Switch selectable):*** to allow DCS/PLC line monitoring function (pulse test).
**2)** ***Voltage monitoring (DIP-Switch selectable):*** ≥ 21.6 Vdc for normal operation, ≤ 17 Vdc reflects a high impedance (≤ 10 mA consumption) to the control device.
***Current consumption @ 24 V:*** 60 mA with relay energized, typical.
***Power dissipation:*** 1.5 W with 24 V input voltage and relay energized, typical.
**Isolation (Test Voltage):** Input/Output 2.5 KV.
**Output:** voltage free SPDT relay contact.
Terminals 13-14, open when relay de-energized, close in energized condition. Terminals 13-15, close when relay de-energized, open in energized 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).
***DC Load breaking capacity:***



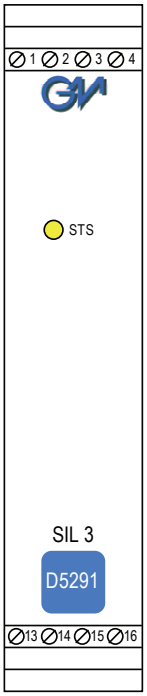

***Mechanical / Electrical life:*** 10 * $10^6$ / 5 * $10^4$ operation, typical.
***Bounce time NO / NC contact:*** 4 / 6 ms, typical.
***Frequency response:*** 10 Hz maximum.
**Compatibility:**
CE mark compliant, conforms to 94/9/EC Atex Directive and to 2004/108/CE EMC Directive.
**Environmental conditions:**
***Operating:*** temperature limits - 40 to + 60 °C, relative humidity 95 %, up to 55 °C.
***Storage:*** temperature limits - 45 to + 80 °C.
**Safety Description:**
***ATEX:*** II 3G Ex nA nC IIC T4 Gc
***IECEx:*** Ex nA nC IIC T4 Gc, non-sparking electrical equipment.
-40 °C ≤ Ta ≤ 60 °C.
***Approvals:*** BVS 10 ATEX E 114 conforms to EN60079-15,
IECEx BVS 10.0072 X conforms to IEC60079-15.
Russia according to GOST 12.2.007.0-75, R 51330.0-99, R 51330.10-99, R 51330.14-99 2ExnAnCIICT4 X.
Ukraine according to GOST 12.2.007.0, 22782.0, 22782.3, 22782.5 2ExsIIT4 X.
TUV Certificate No. C-IS-204194-01, SIL 2 / SIL 3 conforms to IEC61508.
**Mounting:** T35 DIN-Rail according to EN50022 or on customized Termination Board.
***Weight:*** about 145 g.
***Connection:*** by polarized plug-in disconnect screw terminal blocks to accomodate terminations up to 2.5 $mm^2$.
***Location:*** Safe Area/Non Hazardous Locations or Zone 2, Group IIC T4 installation.
***Protection class:*** IP 20.
***Dimensions:*** Width 22.5 mm, Depth 123 mm, Height 120 mm.

## Ordering Information

Model: D5291S

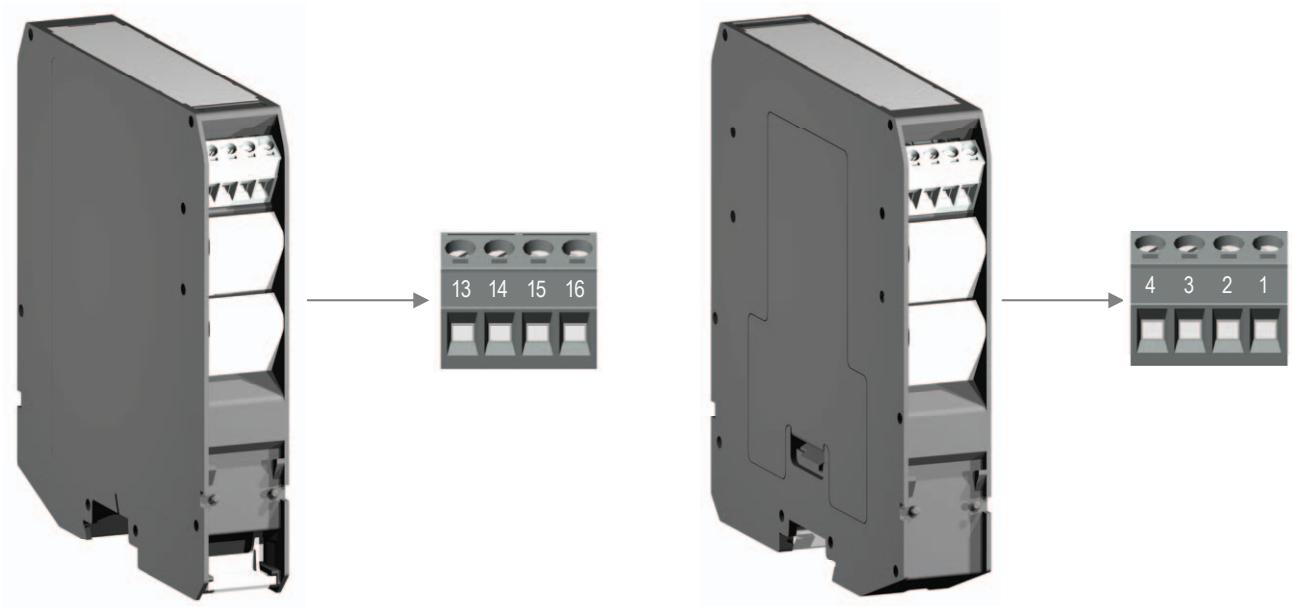
DIN-Rail accessories: Cover and fix MCHP196

## Front Panel and Features




- SIL 3 according to IEC 61508 for Tproof = 6 / 12 yrs (10 / 20 % of total SIF) for ND load with ND relay (terminals 13-14).
- SIL 3 according to IEC 61508 for Tproof = 10 / 20 yrs (10 / 20 % of total SIF) for ND load with NE relay (terminals 13-15).
- SIL 2 according to IEC 61508 for Tproof = 20 yrs (10 % of total SIF).
- PFDavg (1 year) 1.58 E-05, SFF 99.10 % for ND load with ND relay.
- PFDavg (1 year) 7.01 E-06, SFF 99.60 % for ND load with NE relay.
- Installation in Zone 2.
- 10 A SPDT contact for 2 different Safety Functions:
  1) SIL 3 for ND load (energized in fail safe state) with ND relay condition (energized in fail safe state)
  2) SIL 3 for ND load (energized in fail safe state) with NE relay condition (de-energized in fail safe state)
- Line input monitoring in-field DIP Switch selectable.
- Driving input voltage monitoring.
- Input/Output isolation.
- EMC Compatibility to EN61000-6-2, EN61000-6-4, EN61326-1, EN61326-3-1 for safety system.
- ATEX, IECEx, Russian and Ukrainian Certifications.
- Simplified installation using standard DIN-Rail and plug-in terminal blocks or customized Termination Boards.

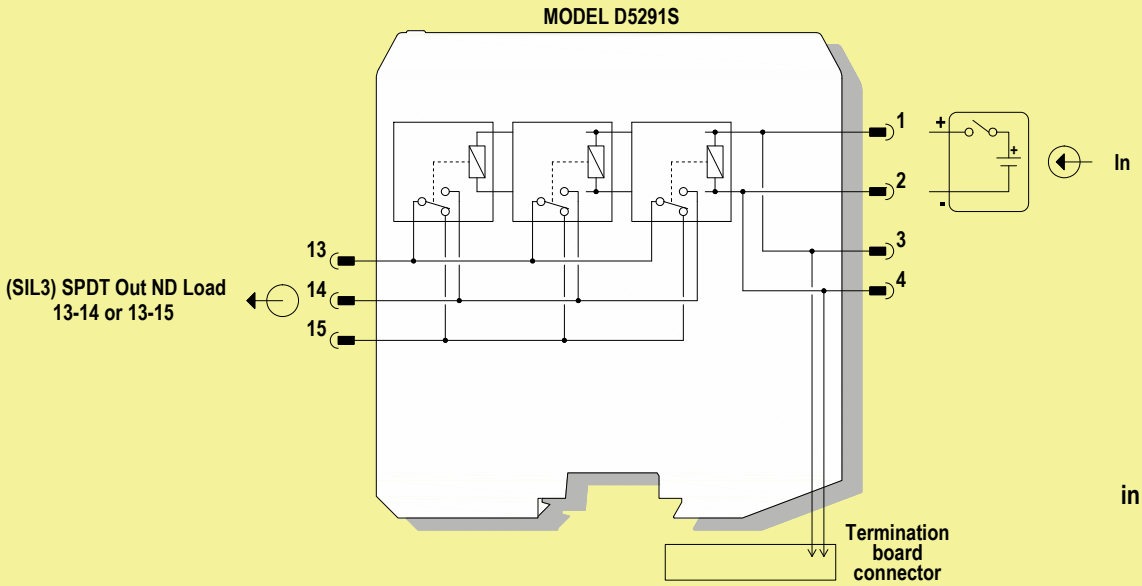
## Terminal block connections




## SAFE AREA

| | | | |
|---|---|---|---|
| **13** | SPDT Output Common | **1** | + Input |
| **14** | SPDT Output Normally Open Contact | **2** | - Input |
| **15** | SPDT Output Normally Close Contact | **3** | + Input |
| **16** | Not used | **4** | - Input |

SAFE AREA, ZONE 2 GROUP IIC T4




**Relay contact shown in de-energized position Terminals 13-14 open, terminals 13-15 close.**

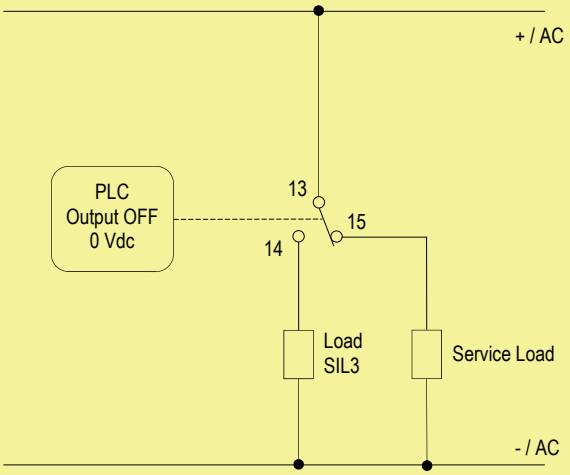
**SIL3 Safety Function for ND load (energized in fail safe state) is available at terminal blocks 13-14; In this case, the Safety Function is met when the relay is energized (closed contact).**

**SIL3 Safety Function for ND load (energized in fail safe state) is available at terminal blocks 13-15; In this case, the Safety Function is met when the relay is de-energized (closed contact).**

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

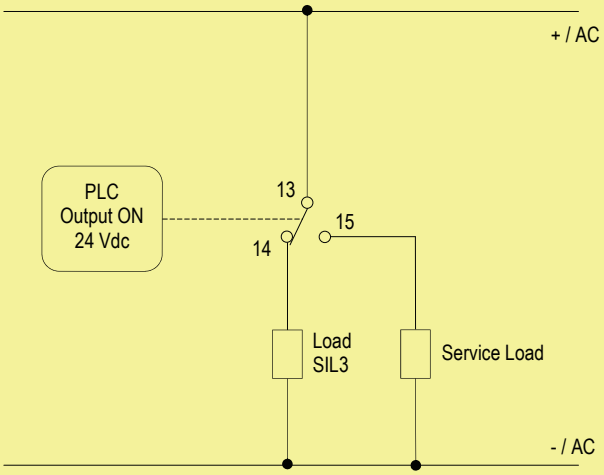
## Application for D5291S - SIL Load Normally De-Energized Condition (ND) and Normally De-Energized Relay

### Normal state operation




**Contact 13-14:** in normal operation the relay is de-energized, contact is open, load is de-energized
**Contact 13-15:** in normal operation the relay is de-energized, contact is closed, service load is energized.

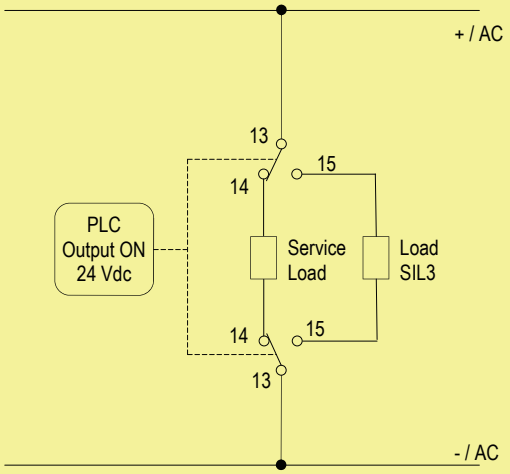
### Energized to trip operation




**Contact 13-14:** the SIL 3 Safety Function is met when the relay is energized, contact is closed, load is energized.
**Contact 13-15:** relay is energized, contact is open, service load is de-energized.

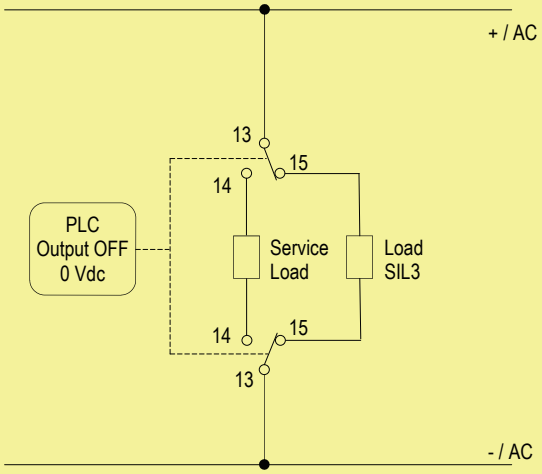
## Application for two D5291S - SIL Load Normally De-Energized Condition (ND) and Normally Energized Relay with common driving signal from PLC for the two relays

### Normal state operation




**Contacts 13-14:** in normal operation relays are energized, contacts are closed, service load is energized
**Contacts 13-15:** in normal operation relays are energized, contacts are open, load is de-energized.

### De-energized to trip operation

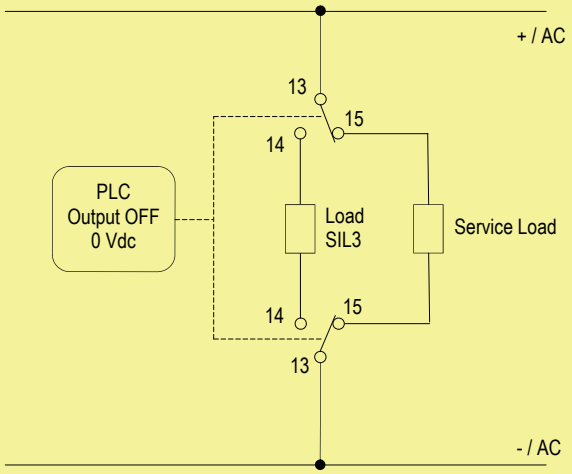



**Contacts 13-14:** relays are de-energized, contacts are open, service load is de-energized.
**Contacts 13-15:** the SIL 3 Safety Function is met when the relays are de-energized, contacts are closed, load is energized.

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

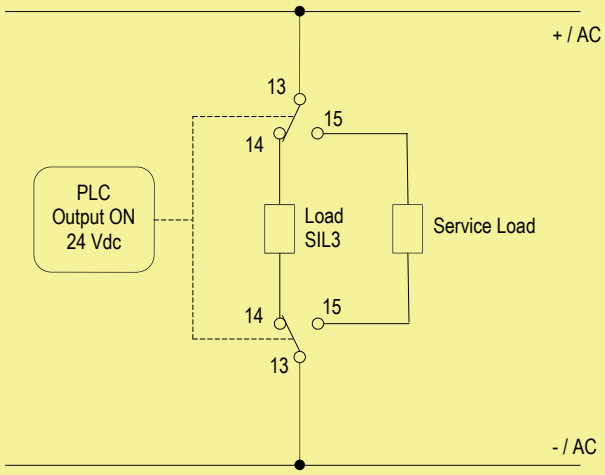
## Application for two D5291S - SIL Load Normally De-Energized Condition (ND) and Normally De-Energized Relay with one common driving signal from PLC for the two relays

### Normal state operation




**Contacts 13-14:** in normal operation relays are de-energized, contacts are open, load is de-energized
**Contacts 13-15:** in normal operation relays are de-energized, contacts are closed, service load is energized.

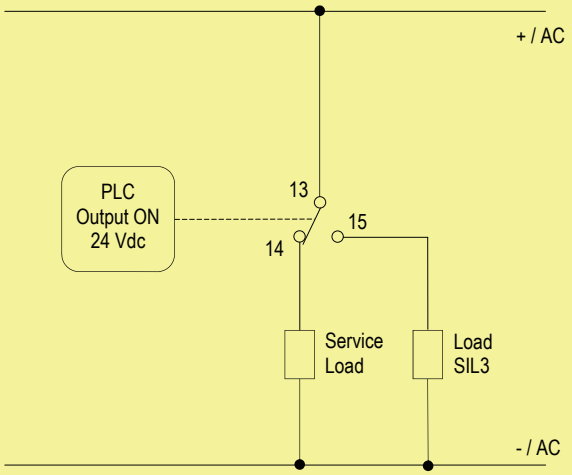
### Energized to trip operation




**Contacts 13-14:** the SIL 3 Safety Function is met when the relays are energized, contacts are closed, load is energized.
**Contacts 13-15:** relays are energized, contacts are open, service load is de-energized.

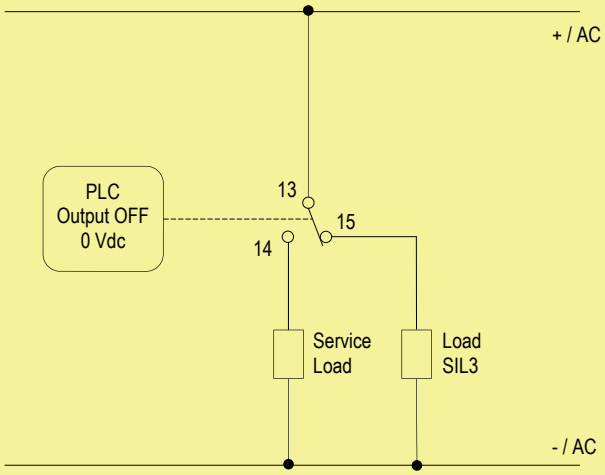
## Application for D5291S - SIL Load Normally De-Energized Condition (ND) and Normally Energized Relay

### Normal state operation




**Contact 13-14:** in normal operation the relay is energized, contact is closed, service load is energized
**Contact 13-15:** in normal operation the relay is energized, contact is open, load is de-energized.

### De-energized to trip operation




**Contact 13-14:** relay is de-energized, contact is open, service load is de-energized.
**Contact 13-15:** the SIL 3 Safety Function is met when the relay is de-energized, contact is closed, load is energized.

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

## Warning

D5291S is an electrical apparatus installed into standard EN50022 T35 DIN-Rail located in Safe Area or Zone 2, Group IIC, Temperature Classification T4, Hazardous Area (according to EN/IEC60079-15) within the specified operating temperature limits Tamb - 40 to +60 °C.
D5291S must be installed, operated and maintained only by qualified personnel, in accordance to the relevant national/international installation standards (e.g. IEC/EN60079-14 Electrical apparatus for explosive gas atmospheres - Part 14: Electrical installations in hazardous areas (other than mines)), following the established installation rules.
De-energize power source (turn off power supply voltage) before plug or unplug the terminal blocks when installed in Hazardous Area or unless area is known to be nonhazardous.
**Warning: substitution of components may impair Intrinsic Safety and suitability for Zone 2.**
**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**.
**Explosion Hazard: to prevent ignition of flammable or combustible atmospheres, disconnect power before servicing or unless area is known to be nonhazardous.**
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

D5291S relay module is suitable for the switching of safety related circuits, providing isolation between the input and output contacts.
D5291S provides 1 SPDT contact for two different safety functions:

1) SIL 3 Safety Function for Normally De-Energized load (energized in fail safe state) is available at Terminal Blocks 13-14. The driving signal is normally low (0 Vdc), the relay is normally de-energized, contact is open and load is de-energized. The safety function is met when the driving signal is high (24 Vdc), the relay is energized, contact is closed and load is energized. At Terminal Blocks 13-15 is also available a service contact (for service load) with opposite (not SIL) function.
2) SIL 3 Safety Function for Normally De-Energized load (energized in fail safe state) is available at Terminal Blocks 13-15. The driving signal is normally high (24 Vdc), the relay is normally energized, contact is open and load is de-energized. The safety function is met when the driving signal is low (0 Vdc), the relay is de-energized, contact is closed and load is energized. At Terminal Blocks 13-14 is also available a service contact (for service load) with opposite (not SIL) function.

A “RELAY STATUS” yellow led lights when input is powered, showing that relay is energized.

## Installation

D5291S 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.
D5291S 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 **(for Zone 2 installations check the area to be nonhazardous before servicing).**
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 (application for a single D5291S):
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 SPDT Output Common pole (terminal “13”).
Connect SIL 3 Normally De-Energized load between negative or AC load supply line and the terminal “14” (when relays are normally de-energized) or the terminal “15” (when relays are normally energized), as previously shown in the Functional Safety applications.

Installation and wiring must be in accordance to the relevant national or international installation standards (e.g. IEC/EN60079-14 Electrical apparatus for explosive gas atmospheres Part 14: Electrical installations in hazardous areas (other than mines)), 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.
**Electrostatic Hazard: to avoid electrostatic hazard, the enclosure of D5291S must be cleaned only with a damp or antistatic cloth.**
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 corresponding “RELAY STATUS” yellow led must be lit and load circuit must be according to the connection required.
Indeed, disabling each input, the corresponding “RELAY STATUS” yellow led must be turned off and load circuit must change the status.

## Configuration

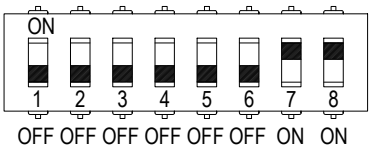
An eight position DIP Switch is located on component side of pcb in order to set four mutually exclusive configurations:

1) line input monitoring, to allow DCS/PLC line input monitoring function (driving line pulse testing);
2) low voltage input monitoring (UVLO—under voltage lock out): module reflects a high impedance state to the control unit when the driving voltage is below the specified threshold;
3) T-proof relay testing.

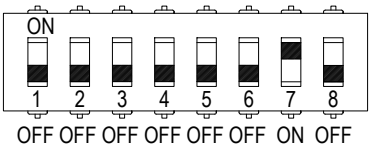

***WARNING:*** **dip-switch 2-4-6 must be set to “OFF” position for any configuration.**

DIP switch configurations:

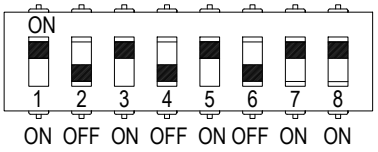
1) line input monitoring:



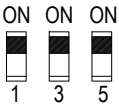

2) low voltage input monitoring:




3) T-proof relay testing:




T-proof relays (dip1 = relay1; dip3 = relay2; dip5 = relay3)




T-proof relays enable


Normal Operation

**Please, see next page for testing procedure at T-proof.**

***WARNING:*** **after T-proof test, dip-switch 1-3-5 must be set to “OFF” position for normal operation.**

## 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 detected 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:<br>1. For De-energized relays and open contacts, terminals "13"-"14", the output load is normally de-energized when the input channel is off, while the activation of the input channel energizes the load (safe state).<br>2. For Energized relays and open contacts, terminals "13"-"15", the output load is normally de-energized when the input is supplied, while the shutdown of the input channel energizes the load (safe state).<br>The channel functionality must be verified for a min to max input voltage change (21.6 to 27.6 Vdc).<br>In addition, the use of three relays for the single output channel, where the contacts are connected in parallel, requires to control the single coils by means of DIP-switch (n°1, 3, 5) and to check the ohmic continuity of the contacts, as described in the following procedures.<br>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 output contact terminals "13"-"14" is absent (i.e. the parallel connection of the 3 NO contacts is open: **1st requisite is verified**). But this condition could also be true if all contacts are normally open except one, which is blocked (for welding) into open position: this will be verified testing the channel when input is supplied (see **3rd requisite**). Instead, the presence of ohmic continuity implies that at least one relay contact is blocked (for welding) into closed position: this could only be verified disassembling and individually testing each relay.<br>2. 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 output contact terminals "13"-"15" is present (i.e. the parallel connection of the 3 NC contacts is closed: **2nd requisite is verified**). But this condition could also be true if only one contact is closed and others are blocked (for welding) into closed or open position: this will be verified testing the channel when input is supplied (see **4th requisite**). Instead, the absence of ohmic continuity implies that all relay contacts are blocked (for welding) into open position.<br>3. Supply the input channel (terminals "1"-"2" or "3"-"4") of the unit under test and verify that the ohmic continuity at the output contacts (terminals "13"-"14") is present (i.e. the parallel connection of the 3 NO contacts is closed: **3rd requisite is verified**). The absence of ohmic continuity implies that all relay contacts are blocked (for welding) into open position. Instead, to verify if a single contact is blocked (for welding) into open position, use the DIP-switches (n°1, 3, 5) to short circuit each possible couple among the 3 relay coils (starting with 1st & 2nd coils by DIP-switches n°1 & 3, then going with 1st & 3rd ones by DIP-switches n°1 & 5, and finally proceeding with 2nd & 3rd ones by DIP-switches n°3 & 5), verifying that ohmic continuity is always present between terminals "13"-"14". In this situation, the absence of ohmic continuity implies that a relay contact (the only one with energized coil because the others are de-energized) is blocked (for welding) into open position.<br>4. Supply the input channel (terminals "1"-"2" or "3"-"4") of the unit under test and verify that the ohmic continuity at the output contacts (terminals "13"-"15") is absent (i.e. the parallel connection of the 3 NC contacts is closed: **4th requisite is verified**). The presence of ohmic continuity implies that at least one relay contact is blocked (for welding) into closed position: this could only be verified after disassembling and individually testing each relay. Instead, to verify if a contact is blocked (for welding) into open position, use internal DIP-switches (n°1, 3, 5) to put in short circuit one relay coil at a time (starting with the 1st coil by DIP-switch n°1, then going on with the 2nd one by DIP-switch n°3, and finally proceeding with the 3rd one by DIP-switch n°5), verifying that the ohmic continuity is always present between terminals "13"-"15". In this situation, the absence of ohmic continuity implies that a relay contact (the only one with de-energized coil) 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 detects almost 100 % of all possible Dangerous Undetected failures in the relay module.

## D5291S Relay Output Module for ND load, with ND relay (terminals 7-8)

- Safety function

This first safety function for ND loads implies the following considerations:

- □ the three internal relays are normally de-energized and their NO contacts (in 1oo3 parallel architecture) are open, so that output load is normally de-energized;
- □ the safety function is met when the three internal relays are energized and their NO contacts (in 1oo3 parallel architecture) are closed, so that output load is energized;
- □ the remaining NC contacts (in 1oo3 parallel architecture) are not used here for this safety purpose but can only be used for service purpose with opposite (not SIL) function.

Therefore, the failure behaviour of module for this safety function is described from the following definitions:

- □ fail-Safe State: is defined as the output load being energized;
- □ fail Safe: failure mode that causes the module 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 load remains de-energized, because if required from the process the module tends to energize the three internal relays but it can't keep closed at least one of three NO contacts (in 1oo3 parallel architecture);
- □ fail "No Effect": failure mode of a component that is part of the safety function but that has no effect on the safety function. For the calculation of the SFF it is considered a safe undetected failure;
- □ 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 rates table:

| Failure category | Failure rates (FIT) |
|---|---|
| $\lambda_{dd}$ = Total Dangerous Detected failures | 0.00 |
| $\lambda_{du}$ = Total Dangerous Undetected failures | 3.60 |
| $\lambda_{sd}$ = Total Safe Detected failures | 0.00 |
| $\lambda_{su}$ = Total Safe Undetected failures | 398.40 |
| ↳ Safe Undetected failures | 299.64 |
| ↳ "No Effect" failures | 98.76 |
| **$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$** | **402.00** |
| $\lambda_{notpart}$ = "Not Part" failures | 0.00 |
| **$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$** | **402.00** |
| **MTBF (single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)** | **284 years** |
| $MTTF_S$ (Total Safe) = 1 / ($\lambda_{sd} + \lambda_{su}$) | 286 years |
| $MTTF_D$ (Dangerous) = 1 / $\lambda_{du}$ | 31710 years |

- Failure rates table according to IEC 61508:

| $\lambda_{sd}$ | $\lambda_{su}$ | $\lambda_{dd}$ | $\lambda_{du}$ | SFF |
|---|---|---|---|---|
| 0.00 FIT | 398.40 FIT | 0.00 FIT | 3.60 FIT | 99.10% |

- PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

| T[Proof] = 1 year | T[Proof] = 6 years | T[Proof] = 20 years |
|---|---|---|
| PFDavg = 1.58 E-05<br>Valid for **SIL 3** | PFDavg = 9.46 E-05<br>Valid for **SIL 3** | PFDavg = 3.15 E-04<br>Valid for **SIL 2** |

- PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

| T[Proof] = 1 year | T[Proof] = 12 years | T[Proof] = 20 years |
|---|---|---|
| PFDavg = 1.58 E-05<br>Valid for **SIL 3** | PFDavg = 1.89 E-04<br>Valid for **SIL 3** | PFDavg = 3.15 E-04<br>Valid for **SIL 2** |

## D5291S Relay Output Module for ND load, with NE relay (terminals 9-10)

- Safety function

This second safety function for ND loads implies the following considerations:

- □ the three internal relays are normally energized and their NC contacts (in 1oo3 parallel architecture) are open, so that output load is normally de-energized;
- □ the safety function is met when the three internal relays are de-energized and their NC contacts (in 1oo3 parallel architecture) are closed, so that output load is energized;
- □ the remaining NO contacts (in 1oo3 parallel architecture) are not used here for this safety purpose but can only be used for service purpose with opposite (not SIL) function.

Therefore, the failure behaviour of module for this safety function is described from the following definitions:

- □ fail-Safe State: is defined as the output load being energized;
- □ fail Safe: failure mode that causes the module 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 load remains de-energized, because if required from the process the module tends to de-energize the three internal relays but none of three NC contacts (in 1oo3 parallel architecture) can be closed;
- □ fail "No Effect": failure mode of a component that is part of the safety function but that has no effect on the safety function. For the calculation of the SFF it is considered a safe undetected failure;
- □ 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 rates table:

| **Failure category** | **Failure rates (FIT)** |
|---|---|
| $\lambda_{dd}$ = Total Dangerous Detected failures | 0.00 |
| $\lambda_{du}$ = Total Dangerous Undetected failures | 1.60 |
| $\lambda_{sd}$ = Total Safe Detected failures | 0.00 |
| $\lambda_{su}$ = Total Safe Undetected failures | 400.40 |
| ↳ Safe Undetected failures | 285.80 |
| ↳ "No Effect" failures | 114.60 |
| **$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$** | **402.00** |
| $\lambda_{notpart}$ = "Not Part" failures | 0.00 |
| **$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$** | **402.00** |
| **MTBF (single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)** | **284 years** |
| $MTTF_S$ (Total Safe) = 1 / ($\lambda_{sd} + \lambda_{su}$) | 285 years |
| $MTTF_D$ (Dangerous) = 1 / $\lambda_{du}$ | 71347 years |

- Failure rates table according to IEC 61508:

| $\lambda_{sd}$ | $\lambda_{su}$ | $\lambda_{dd}$ | $\lambda_{du}$ | SFF |
|---|---|---|---|---|
| 0.00 FIT | 400.40 FIT | 0.00 FIT | 1.60 FIT | 99.60% |

- PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

| **T[Proof] = 1 year** | **T[Proof] = 10 years** | **T[Proof] = 20 years** |
|---|---|---|
| PFDavg = 7.01 E-06<br>Valid for **SIL 3** | PFDavg = 7.01 E-05<br>Valid for **SIL 3** | PFDavg = 1.40 E-04<br>Valid for **SIL 2** |

- PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

| **T[Proof] = 20 years** |
|---|
| PFDavg = 1.40 E-04<br>Valid for **SIL 3** |