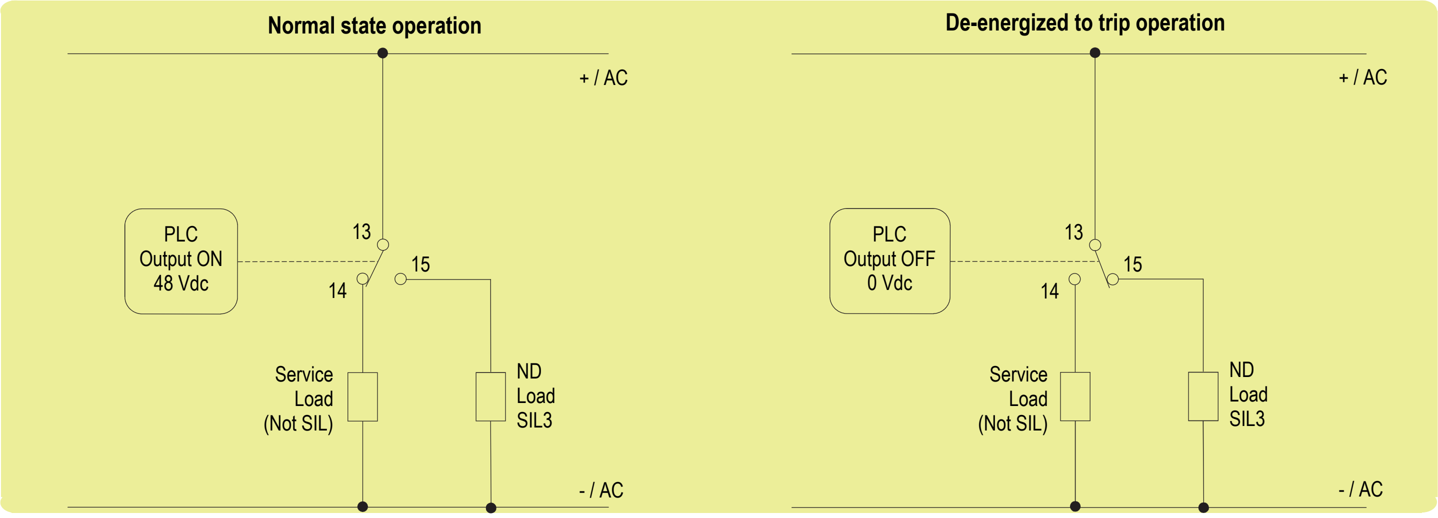
SAFETY MANUAL

10 A SIL 3 Relay Out Module for ND Load with NE Relay condition (48 Vdc coil voltage) DIN-Rail & Term. Board, Model D5291S-097

Reference must be made to the relevant sections within the instruction manual ISM0367, which contain basic guides for the installation of the equipment.

gm technology for safety

Application for D5291S-097 - SIL 3 Load Normally De-Energized Condition (ND) and Normally Energized Relay



Description:

Input Signal from PLC/DCS is normally High (48 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-energized to trip" operation, in order to de-energize the internal relays.
The Load is Normally De-Energized (ND), therefore its safe state is to be energized; instead, the Service Load is normally energized, therefore it de-energizes during "de-energized to trip" operation.
Disconnection of the ND Load is done on only one load line supply.
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- 14	Pins 13 - 15	ND Load (SIL3) Pins 15 — - / AC Supply	Service Load (Not SIL) Pins 14 — - / AC Supply
Normal	High (48 Vdc)	Closed	Open	De-Energized	Energized
Trip	Low (0 Vdc)	Open	Closed	Energized	De-Energized

Safety Function and Failure behavior:

D5291S-097 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 ND (Normally De-Energized) load.
In case of alarm or request from process, the relay module is de-energized (safe state), 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 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 de-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	1.60
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	145.44
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**147.04**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**776 years**
$\lambda_{no\ effect}$ = "No effect" failures	113.56
$\lambda_{not\ part}$ = "Not Part" failures	0.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**260.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**438 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.0 FIT	145.44 FIT	0.00 FIT	1.60 FIT	98.91%

When D5291S-097 drives ND Load and operates in Low Demand mode:

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 = 7.02 E-06 - Valid for **SIL 3**	PFDavg = 9.83 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**

When D5291S-097 drives ND Load and operates in High Demand mode (as a Type A module with HFT = 0 and SFF > 90%): PFH = λ_{du} = 1.60 E-09 h^{-1} - 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 any other appropriate action to avoid a false trip when removing the unit for test.
2	Verify the input-to-output functionality, considering the input signal and each relay output contact state: □ Functional Safety load output at terminals “13”-“15”: when input (terminals “1”-“2”, or “3”-“4”) is energized, this output must be open and FS load must be de-energized; while shutdown of the input channel, this output must be closed and FS load must be energized; □ Service load output at terminals “13”-“14”: when input (terminals “1”-“2”, or “3”-“4”) is energized, this output must be closed and service load must be energized; while shutdown of the input channel, this output must be open and service load must be de-energized. The channel functionality must be verified for a min to max input voltage change (42 to 54 VDC). In addition, the use of three relays for the single output channel, where the contacts are connected in parallel, requires to check the ohmic continuity of the contacts, as described in the following procedures: 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 FS output contact terminals “13”-“15” is present as **Safe State** (i.e. the parallel connection of the 3 NC contacts is closed: **1st requisite is verified**). But this condition could also be true if only one contact is closed and others are blocked (for welding) into: closed position which implies that FS output will always hold the Safe State independently by input channel status; open position which implies dangerous reduction of FS output contact redundancy and it can be verified by presence of ohmic continuity at the service output contact terminals “13”-“14”. Instead, the absence of ohmic continuity at the FS output contact terminals “13”-“15” implies that all three relay contacts are blocked (for welding) into dangerous open position because FS output cannot reach Safe Sate. 2. Supply the input channel (terminals “1”-“2”, or “3”-“4”) of the unit under test and verify that ohmic continuity at the FS output contact terminals “13”-“15” is absent as normal operation (i.e. the parallel connection of the 3 NC contacts is open: **2nd requisite is verified**). The presence of ohmic continuity implies that at least one relay contact is blocked (for welding) into closed position: this implies that FS output will always hold the Safe State independently by input channel status.
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.