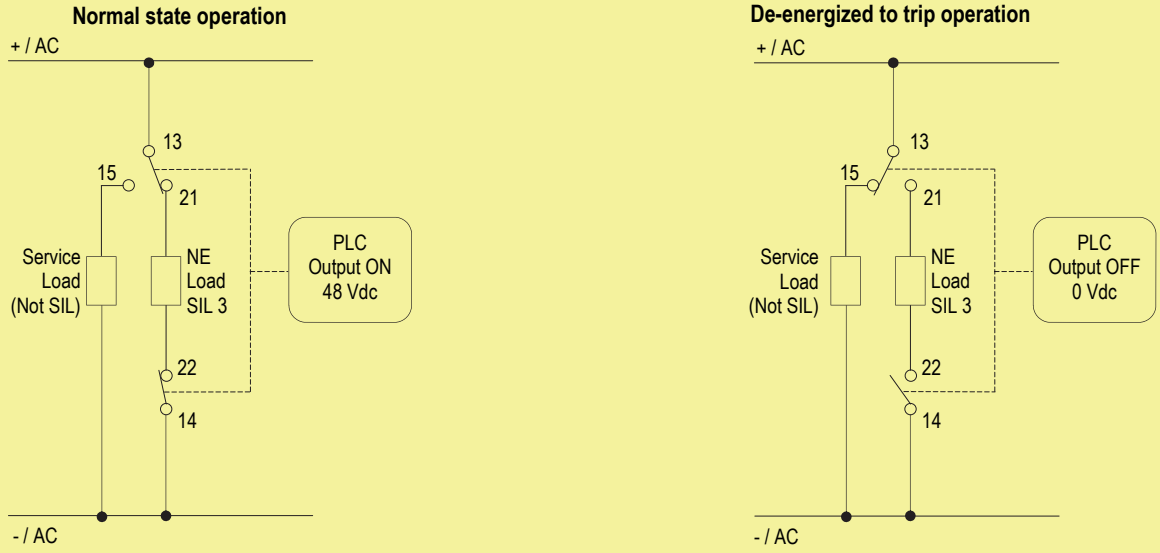
SAFETY MANUAL

10 A SIL 3 Relay Out Module for NE Load with NE Relay condition (48 Vdc coil voltage) DIN-Rail & Term. Board, Model D5290S-092

Reference must be made to the relevant sections within the instruction manual ISM0372, which contain basic guides for the installation of the equipment.

gmi technology for safety

1) Application D5290S-092 - 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 (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 Vac) 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) Pin 15 — -AC / Supply
Normal	High (48 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	Low (0 Vac)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5290S-092 is considered to be operating in Low or High 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) loads.
In case of alarm or request from process, the relay module is de-energized (safe state), de-energizing loads.
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 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 energized;
- □ 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 that 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
0.00 FIT	145.44 FIT	0.00 FIT	1.60 FIT	98.91%

When D5290S-092 drives NE 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:

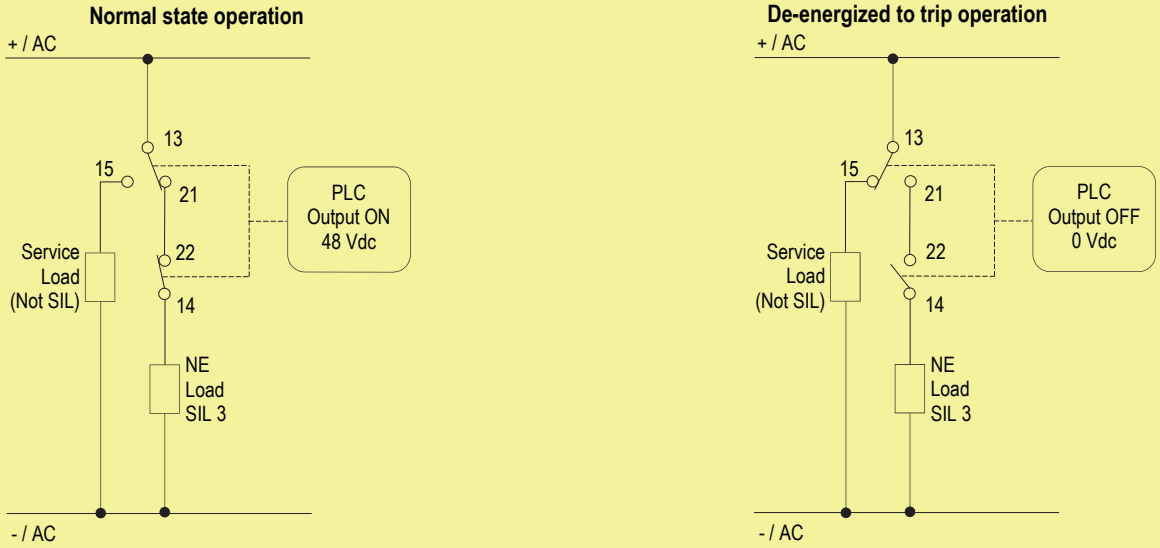
T[Proof] = 1 year	T[Proof] = 14 years
PFDavg = 7.02E-06 Valid for **SIL 3**	PFDavg = 9.83E-05 Valid for **SIL 3**

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

When D5290S-092 drives NE Load and operates in High Demand mode: PFH = λ_{du} = 1.60 E-09 h^{-1} - Valid for SIL 3.
Systematic capability SIL 3.

2) Application D5290S-092 - 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 (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 Vac) 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 by 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) Pin 14 — -AC / Supply	Service Load (Not SIL) Pin 15 — -AC / Supply
Normal	High (48 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	Low (0 Vac)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5290S-092 is considered to be operating in Low or High 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) loads.
In case of alarm or request from process, the relay module is de-energized (safe state), de-energizing loads.
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 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 energized;
- □ 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 that 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
0.00 FIT	145.44 FIT	0.00 FIT	1.60 FIT	98.91%

When D5290S-092 drives NE 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 = 7.02E-06 Valid for **SIL 3**	PFDavg = 9.83E-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 = 1.40E-04 Valid for **SIL 3**

When D5290S-092 drives NE Load and operates in High Demand mode: 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: □ Out 1 (NO contact CM1-NO2) at terminals "13"-"21": when input is energized Out 1 must be closed; while when the input is de-energized Out 1 must be open; □ Out 2 (NO contact NO1-NO3) at terminals "14"-"22": when input is energized Out 2 must be closed; while when the input is de-energized Out 2 must be open; □ Service load output (CM1-NC1) at terminals "13"-"15": when input is energized this output must be open; while when the input is de-energized this output must be closed. The channel functionality must be verified for a min to max input voltage change (42 to 54 VDC).
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.