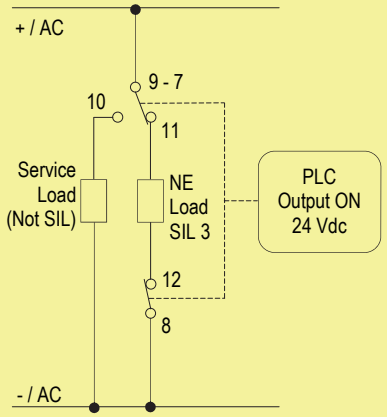
SAFETY MANUAL

SIL3 Relay Out Module for 5A NE Loads, DIN-Rail and Termination Board, Model D5090S-102

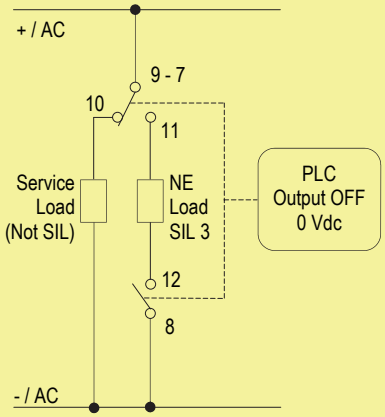
Reference must be made to the relevant sections within the instruction manual ISM0456, which contain basic guides for the installation of the equipment.

1) Application D5090S-102 - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay, with interruption of both load supply lines

Normal state operation



De-energized to trip operation



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.
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	Out 1 Pins 7 - 11	Out 2 Pins 8 - 12	NE Load (SIL3) Pins 11 - 12	Pins 9 - 10	Service Load (Not SIL) Pin 10 to -/AC
Normal	High (24 Vdc)	Closed	Closed	Energized	Open	De-Energized
Trip	Low (0 Vdc)	Open	Open	De-Energized	Closed	Energized

Safety Function and Failure behavior:

D5090S-102 is considered 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 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	191.64
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	193.24
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**590 years**
$\lambda_{no\ effect}$ = "No effect" failures	162.16
$\lambda_{not\ part}$ = "Not Part" failures	19.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**374.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**304 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	191.64 FIT	0.00 FIT	1.60 FIT	99.17%

When D5090S-102 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 = 7.02 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:

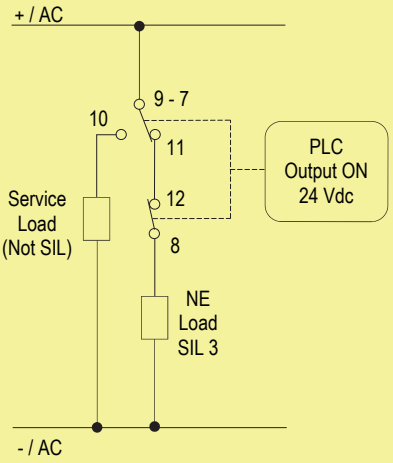
T[Proof] = 20 years
PFDavg = 1.40 E-04 - Valid for **SIL 3**

When D5090S-102 drives NE Load and operates in High Demand mode: PFH = λ_{du} = 1.60 E-09 h^{-1} - Valid for SIL 3.

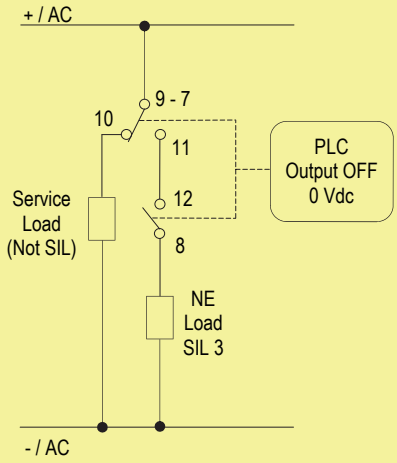
SC3: Systematic capability SIL 3.

2) Application D5090S-102 - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay, with interruption of only one load supply line

Normal state operation



De-energized to trip operation



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.
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 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	Out 1 Pins 7 - 11	Out 2 Pins 8 - 12	NE Load (SIL3) Pin 8 to -/AC	Pins 9 - 10	Service Load (Not SIL) Pin 10 to -/AC
Normal	High (24 Vdc)	Closed	Closed	Energized	Open	De-Energized
Trip	Low (0 Vdc)	Open	Open	De-Energized	Closed	Energized

Safety Function and Failure behavior:

D5090S-102 is considered 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 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	191.64
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	193.24
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**590 years**
$\lambda_{no\ effect}$ = "No effect" failures	162.16
$\lambda_{not\ part}$ = "Not Part" failures	19.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**374.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**304 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	191.64 FIT	0.00 FIT	1.60 FIT	99.17%

When D5090S-102 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 = 7.02 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 D5090S-102 drives NE Load and operates in High Demand mode: PFH = λ_{du} = 1.60 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

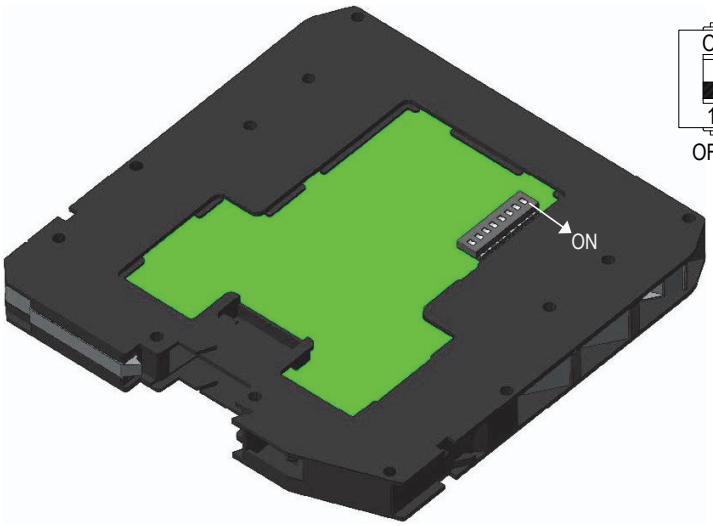
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during proof test. The Proof test consists of the following steps:

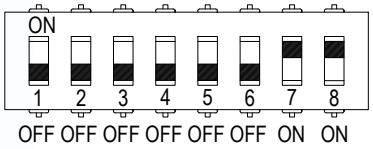
Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip when removing the unit for test.
2	For the single channel, verify the input-to-output functionality: the output load is normally energized by supplying the input channel, while shutdown of the input channel de-energizes the load (safe state). The channel functionality must be verified for a min to max input voltage change (20 to 28.8 Vdc). In addition, the use of three relays for the single output channel, where the contacts are connected in series, requires to control the single coil by means of DIP-switches (n°1, 3, 5) and to check the ohmic continuity of the contacts, as described in the following procedure. 1. Do not supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the Out 1 and Out 2 contacts (terminals "7"-"11" and "8"-"12") is absent (i.e. both the Out 1 contact (series connection of two relay contacts) and the Out 2 contact are open: **1st requisite is verified**). For Out 1 contact, this condition could also be true if only one of two relay contacts in series is open and other is blocked (for welding) into closed or open position: this will be verified by testing the channel when input is supplied, as described in the point 3 of the procedure. Instead, the presence of ohmic continuity at the Out 1 implies that both relay contacts in series are blocked (for welding) into closed position, while the presence of ohmic continuity at the Out 2 implies that the relay contact is blocked (for welding) into closed position. 2. Supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the Out 1 and Out 2 contacts (terminals "7"-"11" and "8"-"12") is present (i.e. both the Out 1 contact (series connection of two relay contacts) and the Out 2 contact are closed: **2nd requisite is verified**). The absence of ohmic continuity at the Out 1 contact implies that one of two relay contacts in series is blocked (for welding) into open position: this could only be verified disassembling and individually testing each of two relay contacts. Instead, the absence of ohmic continuity at the Out 2 contact implies this relay contact is blocked (for welding) into open position. 3. Always supplying the input channel (terminals "1"-"2") of the unit under test, to verify if one of two relay contacts in series (Out 1) is blocked (for welding) into closed position, use internal DIP-switches (n°1 and 3) 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), verifying that the ohmic continuity is always absent between terminals "7"-"11". The presence of ohmic continuity implies that a relay contact (the only one with de-energized coil) is blocked (for welding) into closed 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.

Configuration

An eight position DIP Switch is located on component side of pcb in order to set two mutually exclusive configurations:
1) short circuit fault detection: it allows DCS/PLC to detect short circuit fault of module;
2) T-proof relay testing.

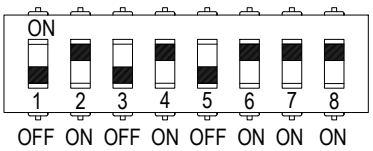




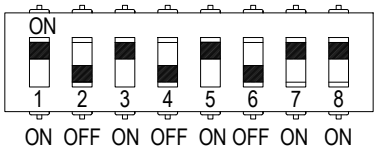
This is factory settings

DIP switch configurations:

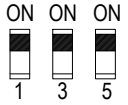
1) short circuit fault detection:



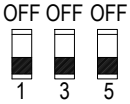
2) T-proof relay testing:



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



T-proof relays enable



Normal Operation

Please, see this page for section "Testing procedure at T-proof".

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