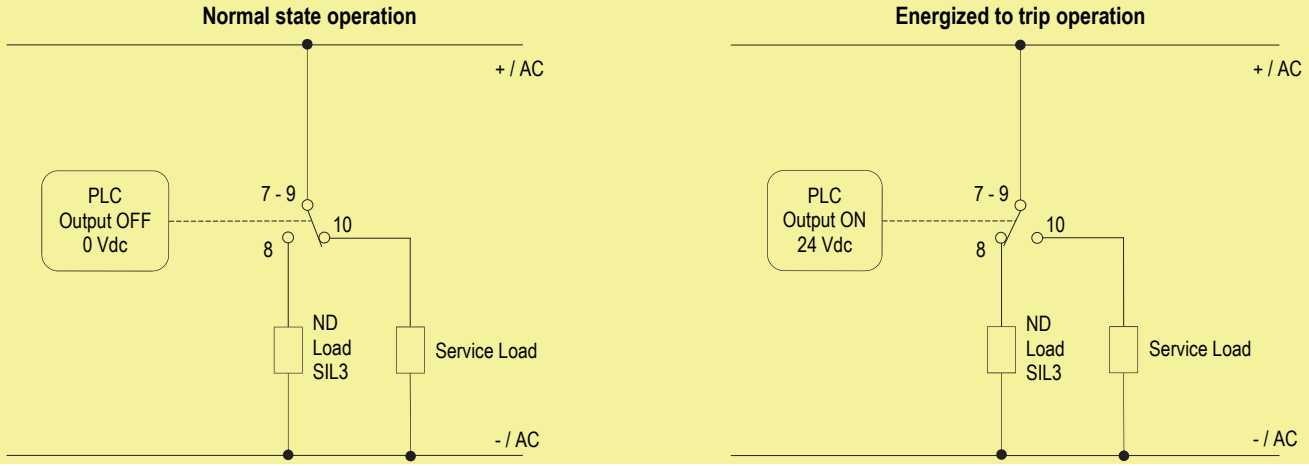
SAFETY MANUAL

SIL3 Relay Out Module for 5A ND Loads, DIN-Rail and Termination Board, Model D5091S-103

Reference must be made to the relevant sections within the instruction manual ISM0457, which contain basic guides for the installation of the equipment.

1) Application for D5091S-103 - SIL 3 Load Normally De-Energized Condition (ND) and Normally De-Energized Relay



Description:

Input Signal from PLC/DCS is normally Low (0 Vdc) and is applied to pins 1-2 in order to Normally De-Energize (ND) the internal relays.
Input Signal from PLC/DCS is High (24 Vdc) during "energized to trip" operation, in order to energize the internal relays.
The Load is Normally De-Energized (ND), therefore its safe state is to be energized.
The Service load is normally energized, therefore it de-energizes during "energized to trip" operation.
Disconnection of the ND 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	Pins 7 - 8	ND Load (SIL3) Pins 8 to - / AC	Pins 9 - 10	Service Load (Not SIL) Pin 10 to -/AC
Normal	Low (0 Vdc)	Open	De-Energized	Closed	Energized
Trip	High (24 Vdc)	Closed	Energized	Open	De-Energized

Safety Function and Failure behavior:

D5091S-103 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 de-energized, with ND (Normally De-Energized) load.
In case of alarm or request from process, the relay module is energized (safe state), 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 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	3.59
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	96.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**99.59**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1146 years**
$\lambda_{no\ effect}$ = "No effect" failures	266.61
$\lambda_{not\ part}$ = "Not Part" failures	9.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**375.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**303 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	96.00 FIT	0.00 FIT	3.59 FIT	96.40%

When D5091S-103 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] = 6 years
PFDavg = 1.58 E-05 - Valid for **SIL 3**	PFDavg = 9.48 E-05 - Valid for **SIL 3**

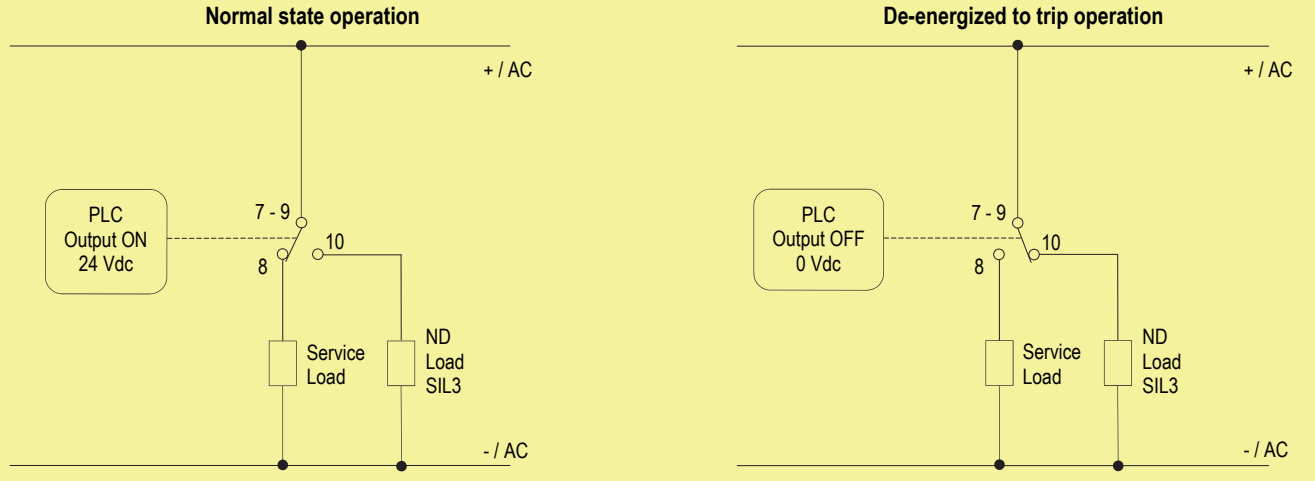
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes > 10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 3.16 E-04 - Valid for **SIL 3**

When D5091S-103 drives ND Load and operates in High Demand mode: PFH = λ_{du} = 3.59 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

2) Application for D5091S-103 - SIL 3 Load Normally De-Energized Condition (ND) and Normally Energized Relay



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 De-Energized (ND), therefore its safe state is to be energized.
The Service load is normally energized, therefore it de-energizes during "energized to trip" operation.
Disconnection of the ND 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	Pins 9 - 10	ND Load (SIL3) Pins 10 to - / AC	Pins 7 - 8	Service Load (Not SIL) Pin 8 to -/AC
Normal	High (24 Vdc)	Open	De-Energized	Closed	Energized
Trip	Low (0 Vdc)	Closed	Energized	Open	De-Energized

Safety Function and Failure behavior:

D5091S-103 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 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	191.37
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	192.97
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**591 years**
$\lambda_{no\ effect}$ = "No effect" failures	164.03
$\lambda_{not\ part}$ = "Not Part" failures	18.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**375.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**303 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	191.37 FIT	0.00 FIT	1.60 FIT	99.17%

When D5091S-103 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 D5091S-103 drives ND 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

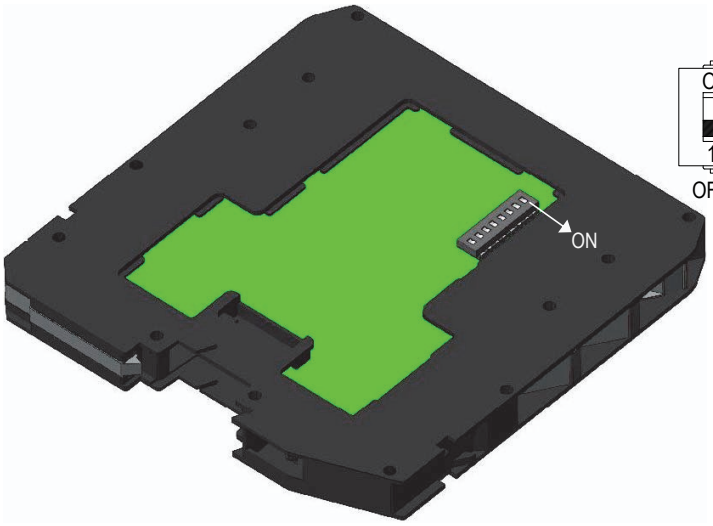
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during proof test. The Proof test consists of the following steps:

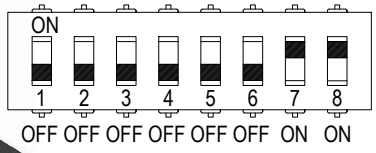
Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip when removing the unit for test.
2	For the single channel, verify the input-to-output functionality: 1. For De-energized relays and open contacts, terminals "7"-"8", the output load is normally de-energized when the input channel is off, while the activation of the input channel energizes the load (safe state). 2. For Energized relays and open contacts, terminals "9"-"10", the output load is normally de-energized when the input is supplied, while the shutdown of the input channel 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 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. 1. Do not supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the output contact terminals "7"-"8" 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. 2. Do not supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the output contact terminals "9"-"10" 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. 3. Supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the output contacts (terminals "7"-"8") 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 "7"-"8". 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. 4. Supply the input channel (terminals "1"-"2") of the unit under test and verify that the ohmic continuity at the output contacts (terminals "9"-"10") is absent (i.e. the parallel connection of the 3 NC contacts is open: **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 "9" & "10". 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 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 the following configuration:
1) T-proof relay testing.



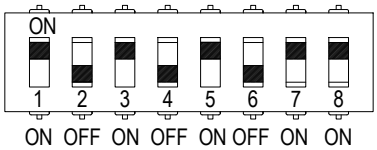


This is factory settings

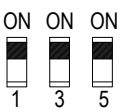
WARNING: **dip-switch 2-4-6 must be set to "OFF" position for any configuration.**

DIP switch configuration:

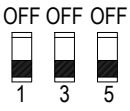
1) T-proof relay testing:



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.**