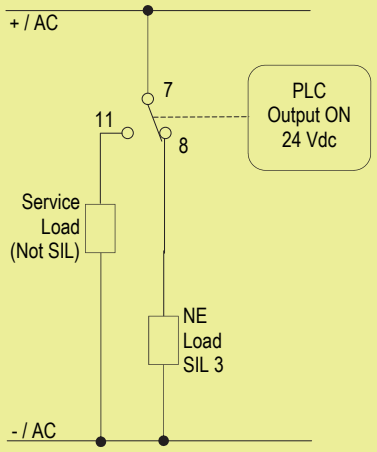
SAFETY MANUAL

5 A SIL 3 Relay Output Module for NE Load, DIN-Rail and Termination Board, Models D5098S, D5098D

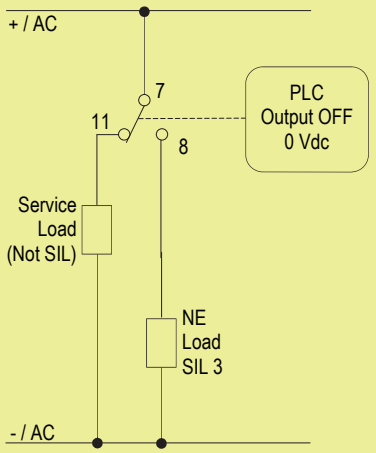
Reference must be made to the relevant sections within the instruction manual ISM0305, which contain basic guides for the installation of the equipment.

1) Application for D5098S - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay

Normal state operation



De-energized to trip operation



Description:

Input Signal from PLC/DCS is normally High (24 Vdc) and it 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 (for NE Load) is normally de-energized, while in safe state it is energized.
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 - 8	NE Load (SIL3) Pin 8 to -/AC	Pins 7 - 11	Service Load (Not SIL) Pin 11 to -/AC
Normal	High (24 Vdc)	Closed	Energized	Open	De-Energized
Trip	Low (0 Vdc)	Open	De-Energized	Closed	Energized

Safety Function and Failure behavior:

D5098S is considered 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) 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	122.50
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**124.10**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**919 years**
$\lambda_{no\ effect}$ = "No effect" failures	93.70
$\lambda_{not\ part}$ = "Not Part" failures	10.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**228.40**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**499 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	122.50 FIT	0.00 FIT	1.60 FIT	98.71%

When D5098S 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**

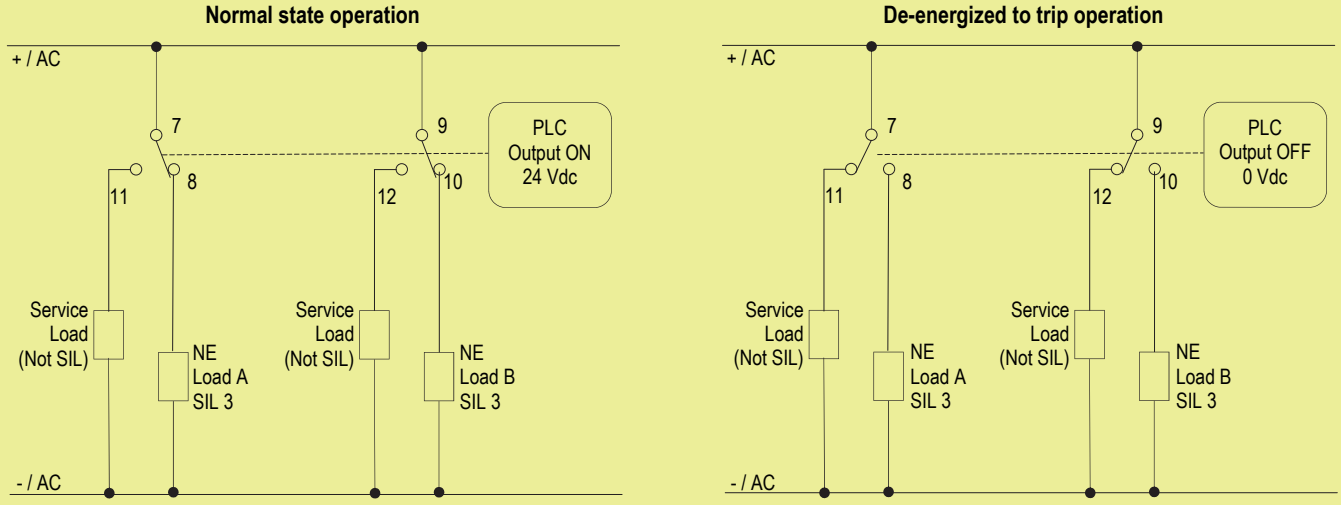
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes > 10% of total SIF dangerous failures:

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

When D5098S 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 for D5098D - SIL 3 Load Normally Energized Condition (NE) and Normally Energized Relay



Description:

For each load (A or B), input Signal from PLC/DCS is normally High (24 Vdc) and it is applied to pins 1-2 (for load A) or 3-4 (for load B) 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 (A or B) is Normally Energized (NE), therefore its safe state is to be de-energized.
The Service load (for NE Load A or B) is normally de-energized, while in safe state it is energized.
Disconnection of each 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 (Ch1), 3-4 (Ch2)	Out 1 Pins 7 - 8	NE Load A (SIL3) Pin 8 to -/AC	Out 2 Pins 9 - 10	NE Load B (SIL3) Pin 10 to -/AC	Pins 7 - 11	Service Load (Not SIL) Pin 11 to -/AC	Pins 9 - 12	Service Load (Not SIL) Pin 12 to -/AC
Normal	High (24 Vdc)	Closed	Energized	Closed	Energized	Open	De-Energized	Open	De-Energized
Trip	Low (0 Vdc)	Open	De-Energized	Open	De-Energized	Closed	Energized	Closed	Energized

Safety Function and Failure behavior:

D5098D is considered 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, one for each channel.
In case of alarm or request from process, the relay module is de-energized (safe state), de-energizing the loads.
For each channel, 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	122.50
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**124.10**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**919 years**
$\lambda_{no\ effect}$ = "No effect" failures	93.70
$\lambda_{not\ part}$ = "Not Part" failures	10.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**228.40**
MTBF (device, each channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**499 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	122.50 FIT	0.00 FIT	1.60 FIT	98.71%

When D5098D drives NE Loads 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 D5098D drives NE Loads 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

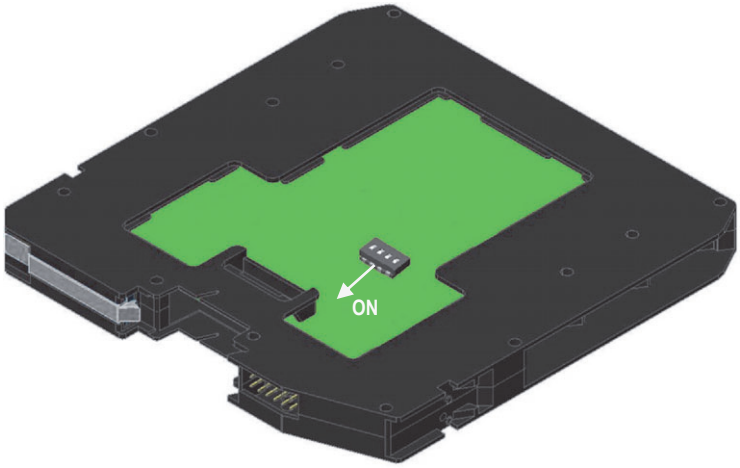
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during proof test.
The channel functionality of all modules here considered must be verified for a minimum to maximum input voltage change (from 21.6 Vdc to 27.6 Vdc).
For the single channel of D5098S and for both channels of D5098D, the output load must be normally energized when the input channel is supplied, while the shut-down of the input channel de-energizes the load (as the safe state). In addition, the use of two relays for each output channel requires to check the single coil by means of dip-switches (no. 1, 2, 3, 4) and to check the ohmic continuità (by ohmmeter) of the contacts, as described in the procedure here below.
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	1. Do not supply the input channel (terminals "1"-"2" for Channel 1 and "3"-"4" for Channel 2, only for D5098D) of the unit under test and verify that the ohmic continuity at the output contacts (terminals "7"-"8" for Channel 1 and "9"-"10" for Channel 2, only for D5098D) is absent, so that both NO contacts are open: the **1st requisite is verified**. For both output contacts, this requisite could also be true if only one of the two relay contacts in series is open and the other one is blocked (for welding) in the closed or open position: this can be verified by testing the channel when the input is supplied, as described in the point 3 of this step. On the other hand, the presence of ohmic continuity at the output contacts implies that both relay contacts are blocked (for welding) in the closed position. 2. Supply the input channel (terminals "1"-"2" for Channel 1 and "3"-"4" for Channel 2) of the unit under test and verify that the ohmic continuity at the output contacts (terminals "7"-"8" for Channel 1 and "9"-"10" for Channel 2) is present, so that both NO contacts are closed: the **2nd requisite is verified**. The absence of ohmic continuity at the output contacts implies that one relay contact is blocked (for welding) in the open position: this can only be verified by disassembling and individiually testing each relay. 3. Always supply the input channel (terminals "1"-"2" for Channel 1 and "3"-"4" for Channel 2) of the unit under test in order to verify if one of the two NO contacts connected in series is blocked (for welding) in the closed position. Set ON the internal dip-switches (no. 1 and 2 for Channel 1 and no. 3 and 4 for Channel 2) to put in short circuit one relay coil at a time (starting with the 1st coil by dip-switches no. 1 and no. 3, then going on with the 2nd coil by dip-switches no. 2 and no. 4), verifying that ohmic continuity is always absent between terminals "7"-"8" for Channel 1 and "9"-"10" for Channel 2. In this situation, the presence of ohmic continuity implies that one relay contact (the one with the de-energized coil) is blocked (for welding) in the closed position.
3	Remove the bypass from the safety-related PLC or restore normal operation inserting the unit.

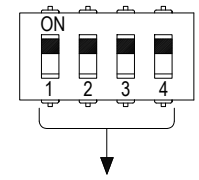
This test reveals almost 99 % of all possible Dangerous Undetected failures in the relay module.

Configuration

For configuration of T-proof relays testing, some DIP Switches are located on component side of pcb. These switches allow the T-proof relays test (SW1 dip-switch: 1-2-3-4 set "ON" and see "Testing procedure at T-proof" section for more information).



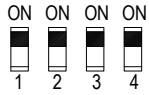
SW1 Dip switch configuration



T-proof relays (dip1 = relay1; dip2 = relay2; dip3 = relay3; dip4 = relay4)

This is factory settings

Normal Operation



T-proof relays enable

***WARNING:* after T-proof test, dip-switch 1-2-3-4 must be set to "OFF" position for normal operation.**