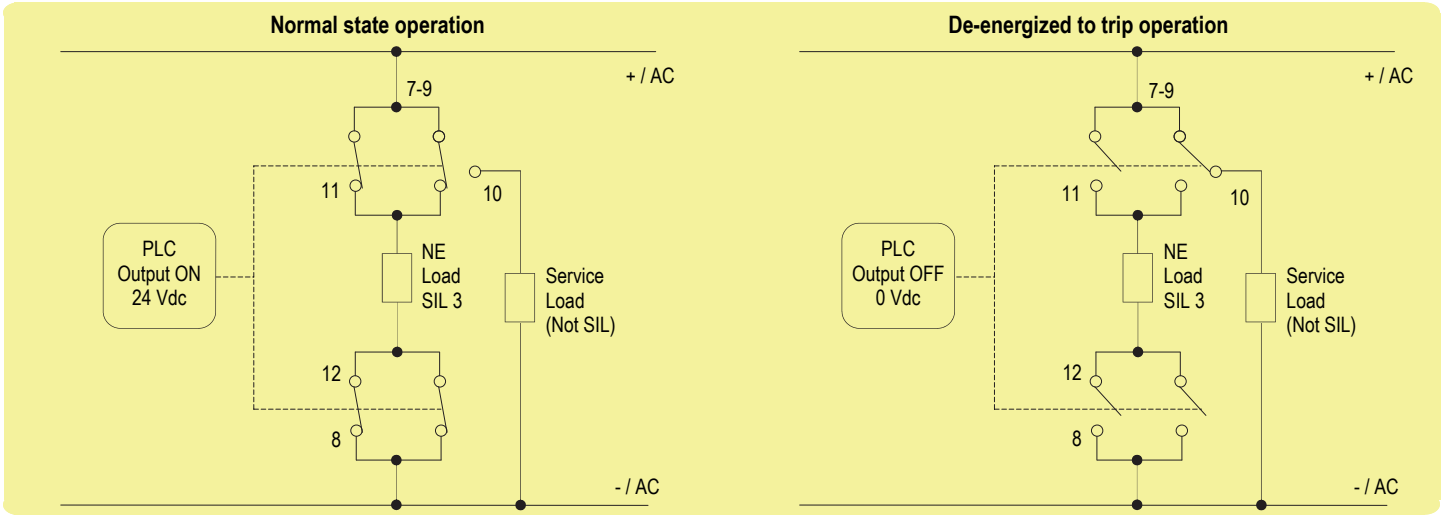
SAFETY MANUAL

5 A SIL 3/SIL 2 SC3 Relay Module for NE or F&G/ND Load, with Diagnostic & Universal Fault Mirroring DIN-Rail and Termination Board, Model D5096S-100

Reference must be made to the relevant sections within the instruction manual ISM0439, which contain basic guides for the installation of the equipment.

gmi technology for safety

1) Application for D5096S-100 - SIL 3 for NE Load with bipolar load interruption and universal fault mirroring to Safety PLC DO



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 (for NE Load) is normally de-energized, while in safe state it is energized.
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)	Pins 7 - 11	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:

D5096S-100 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	406.87
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**408.47**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**279 years**
$\lambda_{no\ effect}$ = "No effect" failures	373.72
$\lambda_{not\ part}$ = "Not Part" failures	110.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**892.59**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**127 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	406.87 FIT	0.00 FIT	1.60 FIT	99.61%

When D5096S-100 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**

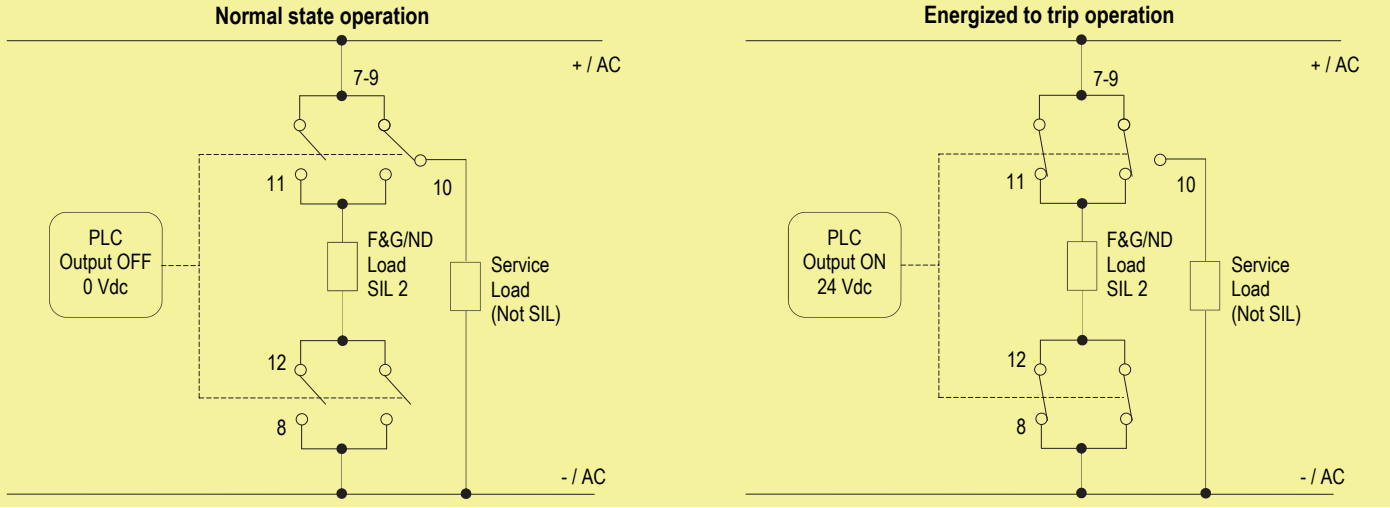
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes > 10% of total SIF dangerous failures:

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

When D5096S-100 drives NE Load and operates in High Demand mode: PFH = λ_{du} = 1.60 E-09 h^{-1} - Valid for SIL 3.

SC 3: Systematic capability SIL 3.

2) Application for D5096S-100 - SIL 2 for F&G/ND Load with bipolar load interruption and universal fault mirroring to Safety PLC DO



Description:

The Safety PLC/DCS Digital Output card must be configured to detect high impedance condition on D5096S-100 signal input, equivalent to detect an open input loop.

Indeed, the D5096S-100 internal diagnostic circuit opens the input loop in case of line and load short/open circuit, absence of load voltage or internal module fault condition.

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 (for ND Load) is normally energized, while in safe state it is de-energized.

Disconnection of the ND 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)	Pins 7 - 11	Pins 8 - 12	F&G/ND Load (SIL2) (Pins 11 - 12)	Pins 9 - 10	Service Load (Not SIL) (Pin 10 to -/AC)
Normal	Low (0 Vdc)	Open	Open	De-energized	Closed	Energized
Trip	High (24 Vdc)	Closed	Closed	Energized	Open	De-energized

Safety Function and Failure behavior:

D5096S-100 is considered to be **operating in Low Demand mode**, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

In the 2nd 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 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 Dangerous Detected: it's a dangerous failure which has been detected by Safety PLC/DCS DO (Digital Output) card because the input loop has been open by D5096S-100 internal diagnostic circuit as cause of line and load short/open circuit, absence of load voltage or internal module fault condition. The Safety PLC/DCS DO card must be configured to detect high impedance condition on D5096S-100 signal input, equivalent to detect an open input loop.
- □ 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.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.

Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2. Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	180.28
λ_{du} = Total Dangerous Undetected failures	3.35
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	133.80
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**317.43**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**359 years**
$\lambda_{no\ effect}$ = "No effect" failures	464.77
$\lambda_{not\ part}$ = "Not Part" failures	110.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**892.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**127 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	133.80 FIT	180.28 FIT	3.35 FIT	98.17%	98.94%

where DC means the diagnostic coverage by internal diagnostic circuit and safety PLC/DCS. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 98.17 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

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] = 20 years
PFDavg = 1.61 E-05 - Valid for **SIL 2**	PFDavg = 3.23 E-04 - Valid for **SIL 2**

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

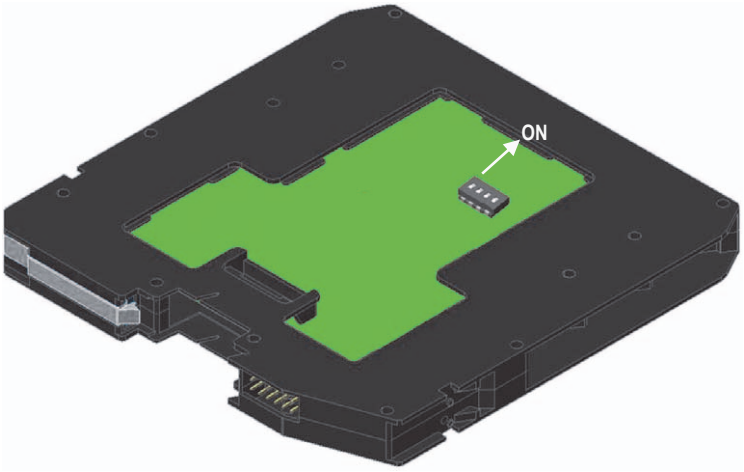
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during proof test.
Before of Specific Proof Test, execute the following General Proof Test: connect the load supply lines to terminal blocks "7" (for +/AC) and "8" (for -/AC) and the NE of F&G / ND load to terminal blocks "11" (as the positive terminal) and "12" (as the negative terminal); finally, connect the DCS/PLC signal to input channel terminal blocks "1" (as the positive terminal) and "2" (as the negative terminal). Then, verify the input to output functionality: the output NE load is normally energized by supplying the input channel, while shutdown of the input channel de-energizes (safe state) the load; on the other hand, the output F&G / ND load is normally de-energized by shutdown of the input channel, while supplying the input channel energizes (safe state) the load. The channel functionality must be verified for a minimum to maximum input voltage change (from 21.6 to 27.6 Vdc).
Then, connect a voltmeter in parallel to the NE of F&G / ND load, that is in parallel to terminal blocks "11" (as the positive terminal) and "12" (as the negative terminal). The use of four relays for a single channel requires to control each relay coil by means of the internal SW1 dip-switches (no. 1, 2, 3, 4) and to check relay contact positions (closed or open) by verifying presence or absence of supply voltage on load, as described in the following Specific Proof Test.
The Specific 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") of the unit under test and verify that there is absence of supply voltage on load (that is 0 V) because both +/AC and -/AC load lines are interrupted because all NO contacts are open: the **1st requisite is verified**. Absence of supply voltage on load could also be true if only one of the two relay contacts in parallel (on +/AC load lines or on -/AC load lines) is open and the other one is blocked (for welding) in the open position: this can be verified by testing the channel when the input is supplied, as described in point 3 of this procedure. On the other hand, the presence of supply voltage on load implies that at least two relay contacts (one for +/AC load lines and another for -/AC load lines) are blocked (for welding) in the closed position: this can be verified only by disassembling and individually testing each relay. 2. Supply the input channel (terminals "1" - "2") of the unit under test and verify that there is presence of supply voltage on load because both +/AC and -/AC load lines are connected to the load because the NO contacts are closed: the **2nd requisite is verified**. The absence of supply voltage on load implies that two relay contacts (both for +/AC load lines or both for -/AC load lines) are blocked (for welding) in the open position. In this condition, the D5096S-100 internal diagnostic circuit detects the fault and opens the input loop, so that the Safety PLC/DCS Digital Output card can detect this condition because configured to detect high impedance condition on D5096S-100 signal input. 3. Always supply the input channel (terminals "1" - "2") of the unit under test in order to verify if a single contact is blocked (for welding) in the open position. Considering the voltage measure on load, set ON the internal SW1 dip-switches (no. 1 or 2) to put in short circuit one relay coil at a time (starting with the 1st coil by dip-switch no. 1, then going on with the 2nd coil by dip-switch no. 2), verifying that supply voltage on load is always present. Then, set ON the internal SW1 dip-switches (no. 3 or 4) to put in short circuit one relay coil at a time (starting with the 3rd coil by dip-switch no. 3, then going on with the 4th coil by DIP-switch no. 4), verifying that supply voltage on load is always present. In these situations, the absence of supply voltage on load implies that a relay contact (the one with the energized coil because the other one is de-energized, being its dip-switch set ON) is blocked (for welding) in the open position. In this condition, the D5096S-100 internal diagnostic circuit detects the fault and opens the input loop, so that the Safety PLC/DCS Digital Output card can detect this condition because configured to detect high impedance condition on D5096S-100 signal input.
3	Remove the bypass from the safety-related PLC or restore normal operation inserting the unit.

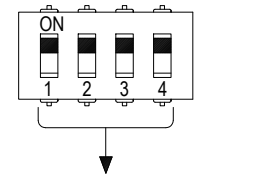
This test reveals almost 99 % of all possible Dangerous Undetected failures in the relay module.

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).

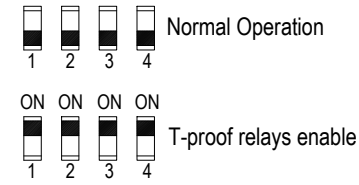


SW1 Dip switch configuration



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

This is factory settings



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