INSTRUCTION & SAFETY MANUAL

5 A SIL 3 Relay Output Module for NE Load, DIN-Rail and Termination Board, Model D5090S-086

technology for safety

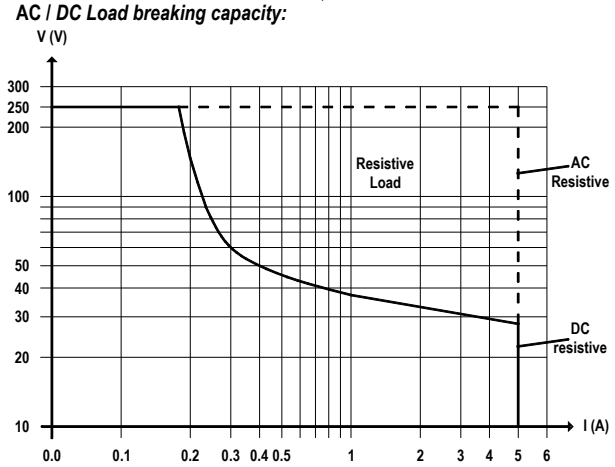
Characteristics

General Description: The single channel Relay Output, D5090S-086 is a relay module suitable for the switching of safety related circuits, up to SIL 3 level according to IEC 61508:2010 Ed.2 for high risk industries. It provides isolation between input and output contacts.
Two mutually exclusive (by DIP-Switch programming) monitoring circuits are provided:
1) line input monitoring, to allow DCS/PLC line monitoring function: when enabled, the module permits a wide compatibility towards different DCS/PLC. Driving line pulse testing, executed by DCS/PLC, is permitted by a dedicated internal circuit, to prevent relay and LED flickering;
2) low voltage input monitoring: when enabled, the module reflects a high impedance state to the control unit when the driving voltage is below the specified threshold;
D5090S-086 provides two NC contacts for normally energized load and a NO contact for service purpose, in order to switch the NE load on both supply lines.
See the following pages for Functional Safety applications with related SIL value.
Mounting on standard DIN-Rail or on customized Termination Boards, in Safe Area or in Zone 2.

Functional Safety Management Certification:
G.M. International is certified by TUV to conform to IEC61508:2010 part 1 clauses 5-6 for safety related systems up to and included SIL3.

Technical Data

Input: 24 Vdc nom (21.6 to 27.6 Vdc) reverse polarity protected, ripple within voltage limits ≤ 5 Vpp.
The following monitoring circuits are mutually exclusive:
1) ***Line input monitoring (DIP-Switch selectable):*** to allow DCS/PLC line monitoring function (pulse test).
2) ***Voltage monitoring (DIP-Switch selectable):*** ≥ 21.6 Vdc for normal operation, ≤ 17 Vdc reflects a high impedance (≤ 10 mA consumption) to the control device.
Current consumption @ 24 V: 40 mA with relay energized and line input monitoring disabled, 45 mA with relay energized and line input monitoring enabled, typical.
Power dissipation: 1.0 W with 24 V input voltage, relay energized and line input monitoring disabled, 1.1 W with 24 V input voltage, relay energized and line input monitoring enabled, typical.
Isolation (Test Voltage): Input / All Outputs 2.5 KV ; Out 1 / Out 2: 500V.
Output: 1 voltage free SPDT relay contact identified with outputs: Out 1 (NC contact) terminals 7-11 and Service Load Out (NO contact) terminals 9-10;
1 voltage free SPST relay contact identified with output Out 2 (NC contact) terminals 8-12.
Terminals 7-11 (Out 1) and 8-12 (Out 2) are closed when relay is de-energized, open in energized relay condition.
Service load output (not SIL) at terminals 9-10 is normally open when relay is de-energized, closed in energized relay condition.
Contact material: Ag Alloy (Cd free), gold plated.
Contact rating: 5 A 250 Vac 1250 VA, 5 A 250 Vdc 140 W (resistive load). Min. switching current 1 mA.
Contact inrush current: 6 A at 24 Vdc, 250 Vac.
AC / *DC Load breaking capacity:*



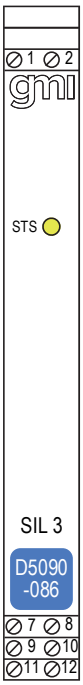
Mechanical / Electrical life: 5 * 10^6 / 3 * 10^4 operation, typical.
Operate / Release time: 50 / 40 ms, typical.
Frequency response: 10 Hz maximum.
Compatibility:
CE mark compliant, conforms to Directive: 2014/34/EU ATEX, 2014/30/EU EMC, 2014/35/EU LVD, 2011/65/EU RoHS.
Environmental conditions:
Operating: temperature limits - 40 to + 70 °C, relative humidity 95 %, up to 55 °C.
Storage: temperature limits - 45 to + 80 °C.
Safety Description:
ATEX: II 3G Ex ec nC IIC T4 Gc; ***IECEx / INMETRO:*** Ex ec nC IIC T4 Gc
EAC-EX: 2Ex ec nC IIC T4 Gc X.
CCC: Ex ec nC IIC T4 Gc
non-sparking electrical equipment.
-40 °C ≤ Ta ≤ 70 °C.
Approvals:
BVS 10 ATEX E 114 conforms to EN60079-0, EN60079-7, EN60079-15.
IECEx BVS 10.0072 X conforms to IEC60079-0, IEC60079-7, IEC60079-15.
INMETRO DNV 13.0109 X conforms to ABNT NBR IEC60079-0, ABNT NBR IEC60079-7, ABNT NBR IEC60079-15.
EAЭC RU C-IT.AA87.B.01310/24 conforms to GOST 31610.0, GOST 31610.7, GOST 31610.15.
CCC n. 2020322316000978 conforms to GB/T 3836.1, GB/T 3836.3, GB/T 3834.8
TÜV Certificate No. C-IS-236198-04, SIL 3 conforms to IEC61508:2010 Ed.2.
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.
DNV Type Approval Certificate No. TAA00001U0 and KR No.MIL20769-EL002 Certificates for maritime applications.
Mounting:
EN/IEC60715 TH 35 DIN-Rail or on customized Termination Board.
Weight: about 125 g.
Connection: by polarized plug-in disconnect screw terminal blocks to accommodate terminations up to 2.5 mm^2.
Location: installation in Safe Area or Zone 2, Group IIC T4.
Protection class: IP 20.
Dimensions: Width 12.5 mm, Depth 123 mm, Height 120 mm.

Ordering Information

Model: D5090S-086

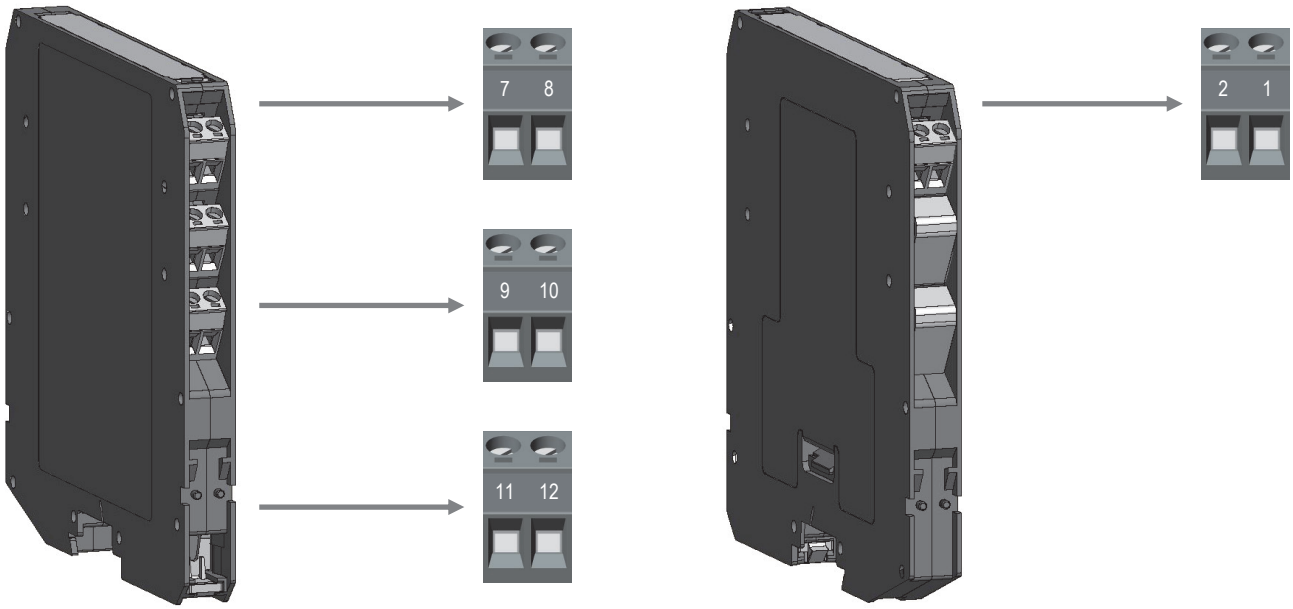
DIN-Rail accessories: Cover and fix MCHP196

Front Panel and Features



- SIL 3 according to IEC 61508:2010 Ed.2 for Tproof = 6 / 20 yrs (≤10% / >10 % of total SIF).
- PFDavg (1 year) 1.44 E-05, SFF 96.70% for NE Load.
- Systematic capability SIL 3.
- Installation in Zone 2.
- SIL 3 contact for NE load and contact for service purpose.
- 6 A inrush current at 24 Vdc / 250 Vac.
- Line input monitoring in-field DIP Switch selectable.
- Driving input voltage monitoring.
- Input/Output isolation.
- EMC Compatibility to EN61000-6-2, EN61000-6-4, EN61326-1, EN61326-3-1 for safety system.
- ATEX, IECEx, INMETRO, EAC-EX, CCC, TÜV Certifications.
- TÜV Functional Safety Certification.
- Type Approval Certificate DNV and KR for maritime applications.
- Simplified installation using standard DIN-Rail and plug-in terminal blocks or customized Termination Boards.

Terminal block connections



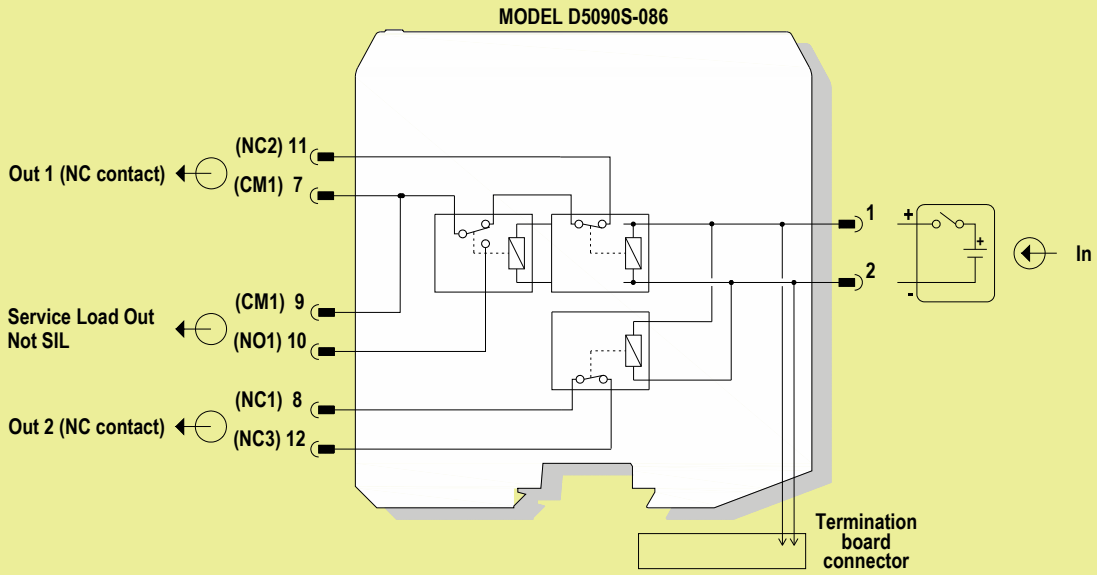
SAFE AREA

7	CM1 Common pole of Normally Closed contact (Out 1)
8	NC1 pole of Normally Closed contact (Out 2)
9	CM1 Common pole of Normally Open contact (Service Load (Not SIL) out)
10	NO1 pole of Normally Open contact (Service Load (Not SIL) out)
11	NC2 pole of Normally Closed contact (Out 1)
12	NC3 pole of Normally Closed contact (Out 2)

1	+ Input
2	- Input

Function Diagram

SAFE AREA, ZONE 2 GROUP IIC T4

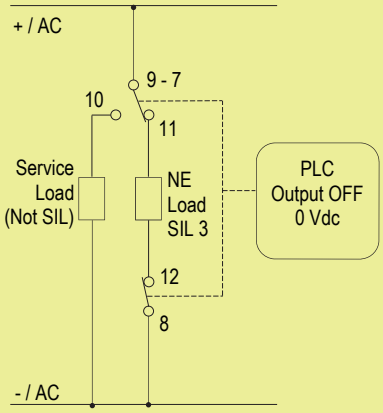


See the following pages for Functional Safety applications with related SIL value.

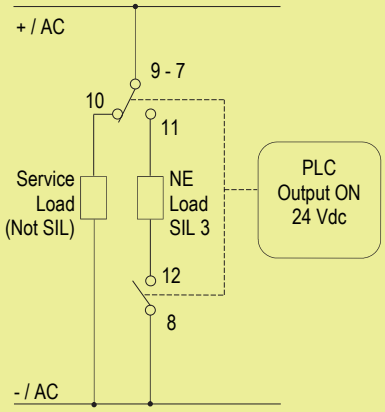
Relay contact shown in de-energized position.
Terminals 7-11 and 8-12 are CLOSED; terminals 9-10 are OPEN.

1) Application D5090S-086 - SIL 3 Load Normally Energized Condition (NE) and Normally De-Energized Relay, with interruption of both load supply lines

Normal state operation



Energized to trip operation



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 "energize to trip" operation, in order to 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 "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	Pins 7/9- 11	Pins 8 - 12	Pins 7/9 - 10	NE Load (SIL3) Pins 11-12	Service Load (Not SIL) Pins 10 — AC / - Supply
Normal	Low (0 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	High (24 Vdc)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5090S-086 is considered to be operating in Low Demand mode, as 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 NE (Normally Energized) load.
In case of alarm or request from process, the relay module is 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 data: 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	3.28
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	96.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**99.28**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1149 years**
$\lambda_{no\ effect}$ = "No effect" failures	260.72
$\lambda_{not\ part}$ = "Not Part" failures	42.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**402.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**283 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	3.28 FIT	96.70%

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 = 1.44 E-05 - Valid for **SIL 3**	PFDavg = 8.64 E-05 - Valid for **SIL 3**

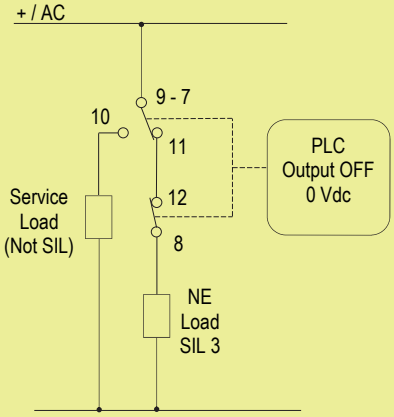
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 2.88 E-04 - Valid for **SIL 2**

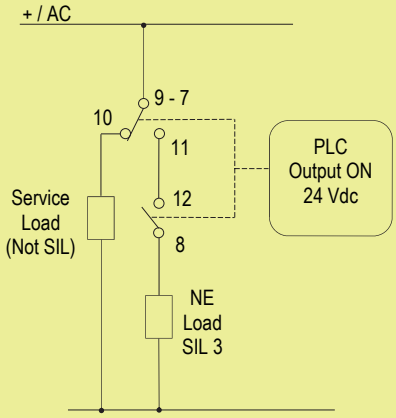
Systematic capability SIL 3.

2) Application D5090S-086 - SIL 3 Load Normally Energized Condition (NE) and Normally De-Energized Relay, with interruption of only one load supply line

Normal state operation



Energized to trip operation



Description:

Input Signal from PLC/DCS is normally Low (0 Vdc) and is applied to pins 1-2 in order to Normally De-energize (NE) the internal relays.
Input Signal from PLC/DCS is High (24 Vdc) during "energize to trip" operation, in order to 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 "energized to trip" operation.
Disconnection of the NE 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 7/9- 11	Pins 8 - 12	Pins 7/9 - 10	NE Load (SIL3) Pins 11-12	Service Load (Not SIL) Pins 10 — AC / - Supply
Normal	Low (0 Vdc)	Closed	Closed	Open	Energized	De-Energized
Trip	High (24 Vdc)	Open	Open	Closed	De-Energized	Energized

Safety Function and Failure behavior:

D5090S-086 is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
In the 2nd Functional Safety application, the normal state operation of relay module is de-energized, with NE (Normally Energized) load.
In case of alarm or request from process, the relay module is 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 data: 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	3.28
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	96.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**99.28**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1149 years**
$\lambda_{no\ effect}$ = "No effect" failures	260.72
$\lambda_{not\ part}$ = "Not Part" failures	42.60
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**402.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**283 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	3.28 FIT	96.70%

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 = 1.44 E-05 - Valid for **SIL 3**	PFDavg = 8.64 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 = 2.88 E-04 - Valid for **SIL 2**

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: the output load is de-energized (safe state) by supplying the input channel, while shutdown of the input channel normally energizes the load. The channel functionality must be verified for a minimum to maximum input voltage change (from 21.6 to 27.6 Vdc). In addition, the use of three relays for the single output channel, whose 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 present (so that both the Out 1 contact, as the series connection of two relay contacts, and the Out 2 contact are closed: the **1st requisite is verified**). The absence of ohmic continuity at the Out 1 contact implies that at least one of the two relay contacts in series is blocked (for welding) in the open position: this can only be verified by disassembling and individually testing each of the two relay contacts. On the other hand, the absence of ohmic continuity at the Out 2 contact implies that this relay contact is blocked (for welding) in the open 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 absent (so that both the Out 1 contact, as the series connection of two relay contacts, and the Out 2 contact are closed: the **2nd requisite is verified**). For the Out 1 contact, this condition could also be true if only one of the two relay contacts in series is open and other one is blocked (for welding) in the closed or open position: this can be verified only by testing the channel when the input is supplied, as described in point 3 of this procedure. On the other hand, the presence of ohmic continuity at the Out 1 contact implies that both relay contacts in series are blocked (for welding) in the closed position, while the presence of ohmic continuity at the Out 2 implies that the relay contact is blocked (for welding) in the closed position. 3. Always supply the input channel (terminals "1"-"2") of the unit under test, to verify if one of the two relay contacts in series (Out 1) is blocked (for welding) in the closed position; use the 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 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.

Warning

D5090-086 series is an electrical apparatus installed into standard EN/IEC60715 TH 35 DIN-Rail located in Safe Area or Zone 2, Group IIC, Temperature Classification T4, Hazardous Area within the specified operating temperature limits Tamb - 40 to +70 °C.
D5090-086 series must be installed, operated and maintained only by qualified personnel, in accordance to the relevant national/international installation standards (e.g. IEC/EN60079-14 Electrical apparatus for explosive gas atmospheres - Part 14: Electrical installations in hazardous areas (other than mines)), following the established installation rules.
De-energize power source (turn off power supply voltage) before plug or unplug the terminal blocks when installed in Hazardous Area or unless area is known to be nonhazardous.
Warning: substitution of components may impair suitability for Zone 2.
Warning: de-energize main power source (turn off power supply voltage) and disconnect plug-in terminal blocks before opening the enclosure to avoid electrical shock when connected to live hazardous potential.
Explosion Hazard: to prevent ignition of flammable or combustible atmospheres, disconnect power before servicing or unless area is known to be nonhazardous.
Failure to properly installation or use of the equipment may risk to damage the unit or severe personal injury.
The unit cannot be repaired by the end user and must be returned to the manufacturer or his authorized representative.
Any unauthorized modification must be avoided.

Operation

D5090S-086 relay module is suitable for the switching of safety related circuits, providing isolation between the input and output contacts.
D5090S-086 provides two NC contacts for normally energized load and a NO contact for service purpose, in order to switch the NE load on both supply lines.
See the previous pages for Functional Safety applications with related SIL value.
A "RELAY STATUS" yellow led lights when input is powered, showing that relay is energized.

Installation

D5090-086 series is a relay output module housed in a plastic enclosure suitable for installation on EN/IEC60715 TH 35 DIN-Rail or on customized Termination Board.
D5090-086 series can be mounted with any orientation over the entire ambient temperature range.
Electrical connection are accommodated by polarized plug-in removable screw terminal blocks which can be plugged in/out into a powered unit without suffering or causing any damage **(for Zone 2 installations check the area to be nonhazardous before servicing)**. Connect only one individual conductor per each clamping point, use conductors up to 2.5 mm² (13 AWG) and a torque value of 0.5-0.6 Nm. The wiring cables have to be proportionate in base to the current and the length of the cable.
In case of installation in zone 2, the connecting cables of non-intrinsically safe circuits must be safely routed in a cable duct or similar. The distance between the pluggable connection terminal and the cable duct should not exceed 500 mm cable length.
On the section "Function Diagram" and enclosure side a block diagram identifies all connections.
Identify the function and location of each connection terminal using the wiring diagram on the corresponding section, as an example (interruption of both NE load supply lines):
Connect positive input at terminal "1" and negative input at "2".
Connect positive or AC load supply line to CM1 Common pole (terminal "7" (for SIL 3 NE load) or "9" (for Not SIL Service Load)).
Connect SIL 3 Normally Energized (NE) Load at terminal "11" and "12".
Connect negative or AC load supply line at terminal "8" (for SIL 3 NE load).
Connect Not SIL Service Load at terminal "10" and to negative or AC load supply line.

Installation and wiring must be in accordance to the relevant national or international installation standards (e.g. IEC/EN60079-14 Electrical apparatus for explosive gas atmospheres Part 14: Electrical installations in hazardous areas (other than mines)), make sure that conductors are well isolated from each other and do not produce any unintentional connection.
Connect SPST relay contacts checking the load rating to be within the contact maximum rating (5 A 250 Vac 1250 VA, 5 A 250 Vdc 140 W resistive load).
To prevent relay contacts from damaging, connect an external protection (fuse or similar), chosen according to the relay breaking capacity diagram on data sheet.
The enclosure provides, according to EN60529, an IP20 minimum degree of protection (or similar to NEMA Standard 250 type 1). The equipment shall only be used in an area of at least pollution degree 2, as defined in IEC 60664-1. When installed in EU Zone 2, the unit shall be installed in an enclosure that provides a minimum ingress protection of IP54 in accordance with IEC 60079-0.
Units must be protected against dirt, dust, extreme mechanical (e.g. vibration, impact and shock) and thermal stress, and casual contacts.
If enclosure needs to be cleaned use only a cloth lightly moistened by a mixture of detergent in water.
Electrostatic Hazard: to avoid electrostatic hazard, the enclosure of D5090-086 series must be cleaned only with a damp or antistatic cloth.
Any penetration of cleaning liquid must be avoided to prevent damage to the unit. Any unauthorized card modification must be avoided.
All circuits connected to D5090-086 series must comply with the overvoltage category II (or better) according to EN/IEC60664-1.
Warning: de-energize main power source (turn off power supply voltage) and disconnect plug-in terminal blocks before opening the enclosure to avoid electrical shock when connected to live hazardous potential.

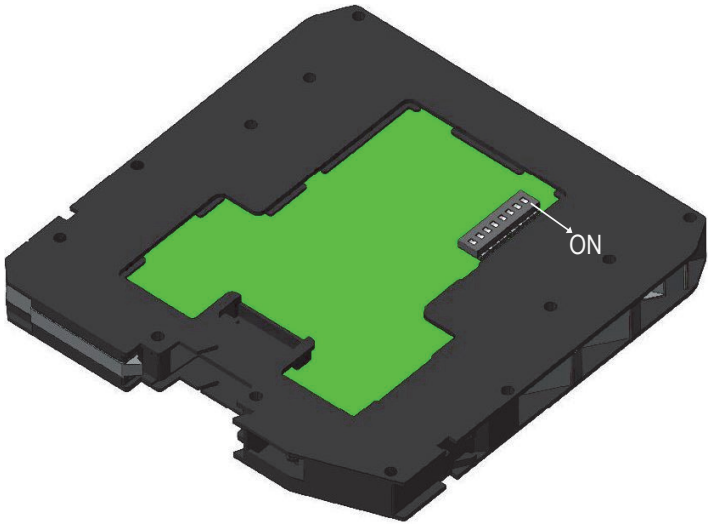
Start-up

Before powering the inputs of unit check that all wires are properly connected, also verifying their polarity. Check conductors for exposed wires that could touch each other causing dangerous unwanted shorts. Enabling input, the “RELAY STATUS” yellow led must be lit and load circuit must be de-energized because relay output contacts (Out 1 and Out 2) are open. Indeed, disabling input, the “RELAY STATUS” yellow led must be turned off and load circuit must be energized because relay output contacts (Out 1 and Out 2) are closed.

Configuration

An eight position DIP Switch is located on component side of pcb in order to set four mutually exclusive configurations:

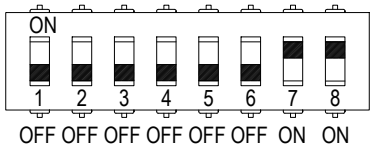
1) line input monitoring, to allow DCS/PLC line input monitoring function (driving line pulse testing);
2) low voltage input monitoring (UVLO—under voltage lock out): module reflects a high impedance state to the control unit when the driving voltage is below the specified threshold;
3) T-proof relay testing.



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

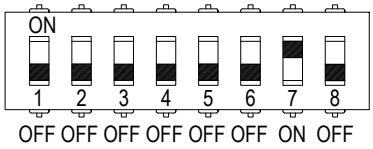
DIP switch configurations:

1) line input monitoring:

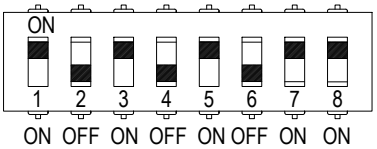


This is factory settings

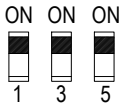
2) low voltage input monitoring:



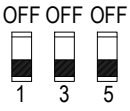
3) T-proof relay testing:



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



T-proof relays enable



Normal Operation

Please, see previous page for testing procedure at T-proof.

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