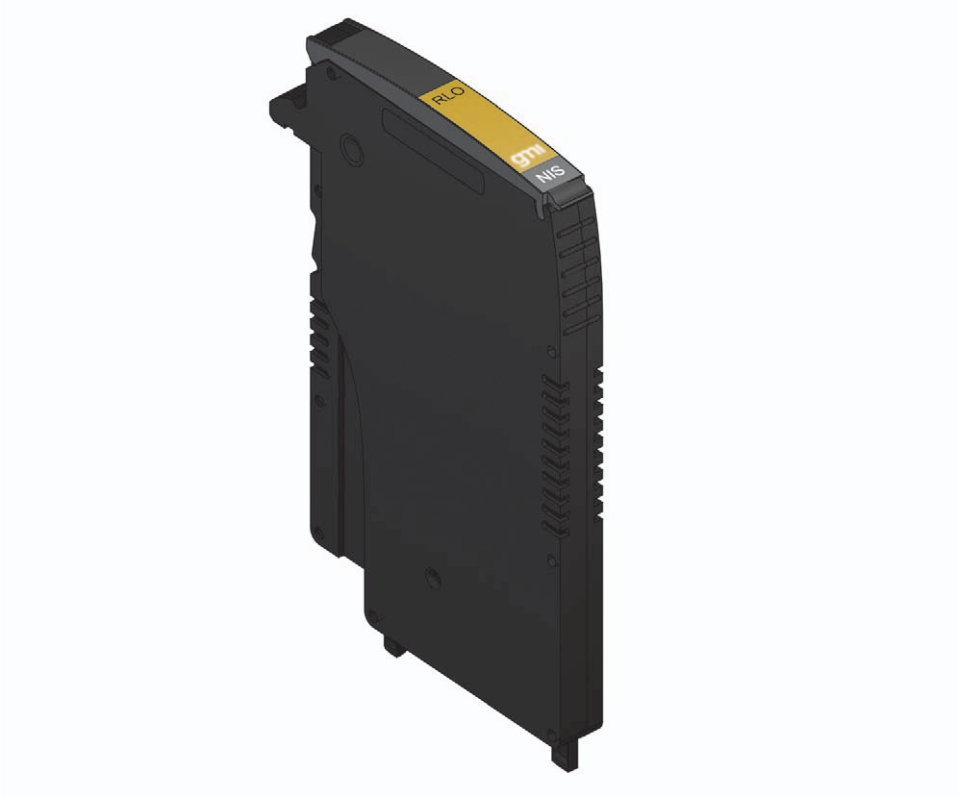


SAFETY MANUAL

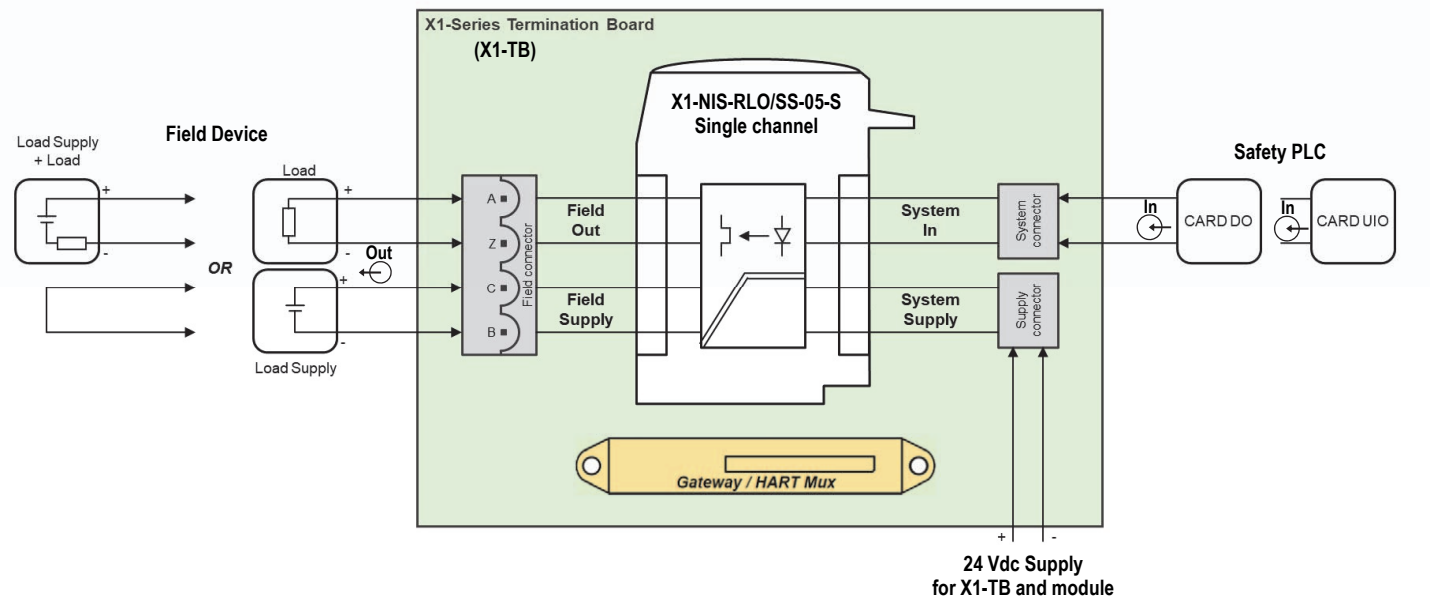
SIL3 Solid-State Relay Out Module for 2A ND/F&G Loads with Diagnostics Model X1-NIS-RLO/SS-05-S

Approval: TÜV Certificate No. TUV IT 25 SIL 0531 A, 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.

Reference must be made to the relevant sections within the instruction manual ISM0629, which contain basic guides for the installation and configuration of the equipment.

gmi technology for safety

X1-NIS-RLO/SS-05-S with ND/F&G load



Description:

The module requires a X1 Series Termination Board (X1-TB) to operate and to connect to field device and to safety-related PLC system.
By X1-TB Supply connector, the 24 Vdc Supply is given to X1-TB and module.
The load supply and load are connected to the module by X1-TB Field connector in two different modes:
- load supply on C-B pins and load on A-Z pins;
- load supply in series to load on A-Z pins and short circuit on C-B pins.

The module is connected to the safety-related PLC system by X1-TB System connector, which is specific for each type of X1-TB and related to PLC System.
For more information on X1-TB System connector, please see related instruction manual of X1-TB.
Line and load short/open circuit detection with programmable limits (by the Gateway) and load voltage monitoring are provided by RLO module, both when the load is de-energized and when the load is energized. The Gateway module is also necessary to execute testing procedure at T-proof.

Safety Function and Failure behavior:

X1-NIS-RLO/SS-05-S is considered to be operating in High or Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour of relay channel is described by the following definitions:
□ fail-Safe State: it is defined as the output load being energized (that is, when three relays are energized and their NO contacts (in 1oo3 parallel architecture) are closed);
□ fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
□ 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, because if required from the process the module tends to energize three relays but it can't keep closed at least one of three NO contacts (in 1oo3 parallel architecture);
□ fail Dangerous Detected: failure mode that causes channel and output load de-energization because system input loop is open or short circuited. With Safety PLC Digital Output (DO) card (connected to channel module by X1-TB) configured to detect very high or low impedance condition of open or short circuited system input loop, this dangerous failure is detected (DD).
□ 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	3.27
λ_{du} = Total Dangerous Undetected failures	2.92
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.02
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**100.21**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1139 years**
$\lambda_{no\ effect}$ = "No effect" failures	207.39
$\lambda_{not\ part}$ = "Not Part" failures	540.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**847.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**135 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	94.02 FIT	3.27 FIT	2.92 FIT	97.09%

When X1-NIS-RLO/SS-05-S 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] = 7.5 years	T[Proof] = 20 years
PFDavg = 1.28 E-05 Valid for **SIL 3**	PFDavg = 9.63 E-05 Valid for **SIL 3**	PFDavg = 2.57 E-04 Valid for **SIL 2**

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 = 2.57 E-04 Valid for **SIL 3**

When X1-NIS-RLO/SS-05-S operates in High Demand mode:

PFH = λdu = 2.92 E-09 h-1 - Valid for SIL 3 (supposing module contributes ≤10% of total SIF dangerous failures).

SC 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 the proof test.

The **Proof test** on X1-NIS-RLO/SS-05-S module with input to output direct signal transfer and input line fault detection enabled:

Steps	Action
1	The module requires a X1 Series Termination Board (X1-TB) to operate and to connect to field device and to safety-related PLC system. In addition, X1 Gateway module (X1-GW) must be present to X1-TB and it must be connected to Workstation/PC by (USB or Ethernet or Modbus RS485) to configure and monitor the RLO module under test by SWCX1 software installed on Workstation/PC. By Safety PLC, take appropriate action to avoid detection of a malfunctioning on the SIF where RLO module is operating. Change the field load with an equivalent one (in terms of resistance and voltage / current / power operating).
2	Considering that equivalent field load is normally de-energized (because Safety PLC de-energizes system input loop to RLO module), on SWCX1 main window choose "Advanced options" entry, then "T-proof" selection to start the Proof test by pressing "Test" button of related RLO module. The T-proof procedure tests independently all solid state relay contacts and it releases a T-proof test report with PASS or FAIL result as test validation. With PASS result, RLO module operates correctly and passes step 2 of Proof test. Instead, with FAIL result, RLO module is not correctly operating according to a demand from the process (presence of dangerous failure) and it must be changed with a new RLO module.
3	If RLO module passes the step 2 of Proof test, disconnect the equivalent field load and restore normal field load. By Safety PLC, re-establish normal operation (including detection of malfunctioning) on the SIF where RLO module is operating.

This test detects approximately 99 % of possible Dangerous Undetected failures in the RLO module.