SIL Safety Manual

Manual Safety Relay SCS 24VDC P1SIL3DS I

Weidmüller

Content

Revision history

Version	Date	Change
00	09/2017	First Edition
01	11/2017	Chapter 2.2, editorial change
02	05/2018	Page 11, Technical safety values updated

Contact address

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold
Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

1 Scope and definitions

1.1 Scope

This safety manual applies to the safety relay

SCS 24VDC P1SIL3 I 2500980000

from the Weidmüller SAFESERIES product family.

Manufacturer:

Weidmüller Interface GmbH & Co KG
Klingenbergstraße 16
32758 Detmold
Germany

Certification body:

TÜV NORD CERT GmbH
Zertifizierungsstelle
Maschinen
Benannte Stelle 0044
Langemarckstraße 20
45141 Essen
Germany

The safety relay fulfils the safety integrity level 3 (SIL 3) for low and high demand modes of operation. The device is certified according to EN 61508:2010 and may bear the following TÜV certification mark.

Certificate Registration No
44 207 13773712

1.2 Terms and abbreviations

Safety Integrity Level (SIL):

Four discrete levels (SIL1 to SIL4). The higher the safety integrity level of a safety-related system, the lower the probability that it will not perform the required safety functions.

Average Probability of Failure on Demand (PFD_{avg}):

Average probability of failure of a safety function working in low demand mode of operation.

Probability of Failure per Hour (PFH):

VAverage probability of failure of a safety function working in high demand or continuous mode of operation.

Safe Failure Fraction (SFF):

Percentage part of safe failures and dangerous detected failures of a safety function or a sub-system related to all failures.

Hardware Fault Tolerance (HFT):

HFT = n means, that n+1 faults could cause a loss of the safety function.

Low demand mode of operation:

Frequency of demands on a safety-related system no greater than one per year and no greater than twice the proof-test frequency.

High demand or continuous mode of operation:

Frequency of demands on a safety-related system greater than one per year or greater than twice the proof-test frequency.

Device type A (simple subsystem):

The failure modes of all constituent components are well defined and the behaviour under fault conditions can be completely determined.

FMEDA (Failure Mode, Effects and Diagnostic Analysis):

Systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document a system in consideration.

Failure rates λ:

- λ_{SD} Total failure rate for safe detected failures
- λ_{SU} Total failure rate for safe undetected failures
- λ_{DD} Total failure rate for dangerous detected failures
- λ_{DU} Total failure rate for dangerous undetected failures

MTTF (Mean Time To Failure):

Mean time between two failures. MTTF is a basic measure of reliability for non-repairable systems.

Proof-test interval (T_{proof}):

Interval between periodic tests performed to detect failures in a safety-related system.

De-energised To Safe (DTS):

Safety-related switch-off

Energised To Safe (ETS):

Safety-related switch-on

2 Intended use and device description

2.1 Intendes use

The safety relay SCS 24VDC P1SIL3 I serves the purpose of safety-related switch-off of process industry systems (DTS = de-energised to safe).

The safety relay is intended to be used together with Triconex® safety controllers from the Schneider Electric company. A certificate of compatibility is available for the systems Tricon™, Trident™ and Tri-GP™.

The device fulfils the safety integrity level 3 (SIL 3) for low and high demand modes of operation according to EN 61508.

2.2 Device description

The input of the safety relay uses a test pulse filter and three relays connected in parallel. The relay contacts in the output are connected in series. Therefore, the safety-related switch-off is ensured even in case of sticking contacts. The relay contact circuit at the connection terminals 13 and 15 is protected against overload and short-circuit with a 5 A fuse.

Connection terminals 14 and 15 are to be used for implementing external fusing.

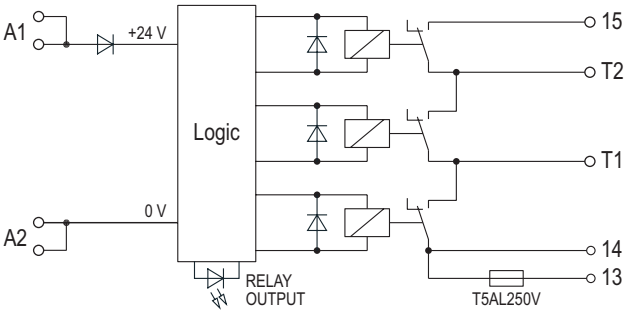
Connection terminals T1 and T2 must only be used for checking the relay contacts. In order to do this, the device must be released and the test current must be limited to max. 500 mA.

The front of the device features a status LED “RELAY OUTPUT”. The LED lights yellow when the input circuit (connection terminals A1 and A2) of the device is actuated.

The status LED does not indicate the electrical switching state at the device output.

The status change at the device output is executed with a certain delay after the status LED indication has changed.

2.3 Block diagram



3 Notes on configuration

3.1 Low demand mode of operation

The safety relay is used with a low demand rate (low demand mode) when the demand rate of the relay does not exceed 5x per year and when it does not exceed double the frequency of the repeat test (proof test).

The associated technical parameter is the value PFD_{avg} that applies to the duration of the test interval T_{proof}.

3.2 High demand mode of operation

If the low demand rate mode is not applicable, the safety relay is to be used as a safety-relevant subsystem with a high or continuous demand rate (high demand mode or continuous mode).

The associated technical parameter is the value PFH that applies to the duration of the test interval T_{proof}.

3.3 Types of malfunctions

A safe failure is not able to render a technical safety system dangerous or non-functional. The safety relay passes to a predefined safe state.

A dangerous, undetected failure has the potential to render a technical safety system dangerous or non-functional. The safety relay does not pass to a predefined safe state.

3.4 Test interval

The test interval is the period of time in which tests are conducted in full and are repeated.

Errors are detected within the framework of the proof test.

4 Commissioning and maintenance

The following operating instructions must be available for the safety relay.

Designation:	IS SCS 24VDC P1SIL3DS I
Order number:	2530250000

It contains notes, boundary conditions and limit values that must be factored into the installation and operation of the safety relay.

The safety relay must be checked for proper functioning prior to commissioning and after every change in wiring, see chapter 5.1 „Functional testing“.

The output circuit is protected with a miniature device fuse (GS fuse).

The fuse is accessible on the front side of the housing. It can be swapped out without opening the housing.

If there is a short circuit, you must make sure that the cause of the short circuit has been fixed. A functional test should be carried out after the fuse has been replaced.

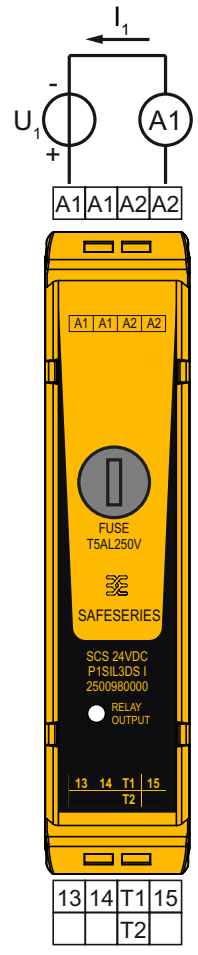
5 Proof test

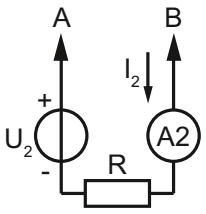
The purpose of the proof test is to detect any dangerous faults that cannot be detected by means of self-diagnostics. Therefore, the functionality of the safety relay must be tested in appropriate intervals.

The selection of the type and intervals of the tests is the responsibility of the operator. The test intervals are, among other factors, determined by the calculation of each individual safety circuit in a system (PFD values).

Testing must be carried out in such a way that proper functionality of the safety function is proven during interaction of all components.

5.1 Functional testing





Dimensioning recommendation:
U_2 = 12 V DC
R = 1200 Ω

Functional testing	A	B
Internal fuse and relay contact circuit	13	15
Contact set 1	14	T1
Contact set 2	T1	T2
Contact set 3	T2	15

Input circuit active

- U_1 = 24 V DC, input voltage at the connection terminals A1(+) and A2(-) is switched on
  - current consumption is I_1 = 45...55 mA (ammeter A1)
  - the “RELAY OUTPUT” LED lights up
  - Functional testing of internal fuse and relay contact circuit:
    the connection terminals 13 and 15 are electrically connected, current consumption is I_2 = 10 mA (ammeter A2)

Input circuit inactive

- U_1 = 0 V DC, input voltage at the connection terminals A1(+) and A2(-) is switched off
  - current consumption is I_1 = 0 mA (ammeter A1)
  - the “RELAY OUTPUT” LED does not light up
  - Functional testing contact set 1:
    the connection terminals 14 and T1 are not electrically connected, current consumption is I_2 = 0 mA (ammeter A2)
  - Functional testing contact set 2:
    the connection terminals T1 and T2 are not electrically connected, current consumption is I_2 = 0 mA (ammeter A2)
  - Functional testing contact set 3:
    the connection terminals T2 and 15 are not electrically connected, current consumption is I_2 = 0 mA (ammeter A2)

6 Technical safety values

Safety basic data	
Safety category	SIL 3
Safety standard	EN 61508
Device type	A
HFT	2
T_{proof} in years	12

Safety parameters “low demand mode”	
Frequency of demands	5 per year
λ_{DD} in FIT	0
λ_{DU} in FIT	0.4
$\lambda_{SD} + \lambda_{SU}$ in FIT	1936.2
λ_{Total} in FIT	1936.6
SFF in %	50
PFD_{avg} (complete)	4.30×10^{-6}
MTTF in years	400

Safety parameters “high demand mode”			
Frequency of demands	Once per month	Once per week	Once per day
λ_{DD} in FIT	0	0	0
λ_{DU} in FIT	0.8	3.00	21.1
$\lambda_{SD} + \lambda_{SU}$ in FIT	1936.6	1938.8	1956.9
λ_{Total} in FIT	1937.4	1941.9	1978.0
SFF in %	50	50	50
PFH in h^{-1} (complete)	1.02×10^{-10}	2.14×10^{-10}	1.12×10^{-9}
MTTF in years	396	379	279

Requirements

- The maximum allowable ambient temperature is 50 °C.
- The environmental conditions correspond to the average industrial environment.
- The specifications in the data sheet and the operating instructions should not be exceeded.

www.weidmueller.com

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold
Germany
T +49 5231 140
F +49 5231 14292083
www.weidmueller.com

Order number:
2555600000/02/05-2018