SIL Safety Manual

Manual SCS 24VDC P1SIL3DS

Weidmüller

Revision History

Version	Date	Change
0.0	05/2012	First Edition
1.0	08/2015	Page 13, chapter 6.2 updated
2.0	06/2017	Page 5, TÜV logo updated Page15, deleted

Contact Address

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold
Germany

Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-292083
info@weidmueller.com
www.weidmueller.com

Content

1. Scope and standards

1.1 Scope

This safety manual applies to SIL3 relays from Weidmüller's SAFESERIES for the following items produced after 03/2012:

SCS 24VDC P1SIL3DS	1303890000
SCS 24VDC P1SIL3DS M	1303760000
SCS 24VDC P1SIL3DS MG3	1304040000

SIL3 relays in the SCS 24VDC P1SIL3DS series from

Weidmüller Interface GmbH & Co KG
Klingenbergstrasse 16
32758 Detmold
Germany

have been certified by

TÜV NORD CERT GmbH
Am TÜV 1
30519 Hannover
Germany

according to EN 61508 SIL3. They are certified as “Safety Approved” for use in “low demand mode” and “high demand mode” systems.

Certificate Registration No:
44 207 12 405992

1.2 Abbreviations

Safety Integrity Level (SIL):
Four discrete levels (SIL1 to SIL4). The higher the SIL 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):
Average 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.

2. Device description and application

2.1 General

Our SAFESERIES line of safety relays are used for safety-related shutdowns (DTS = de-energized to safe) of facilities in the process industry.

All products in this series comply with the requirements found in EN 61508, SIL 3 for “low demand mode” and “high demand mode”. The “M” and “M G3” types also feature a monitoring circuit for receiving signals from the field. The “M G3” types also feature a special coating over the electronics that protects them from harsh industrial conditions, as described in the standard ISA S71.04-1985, Class G3.

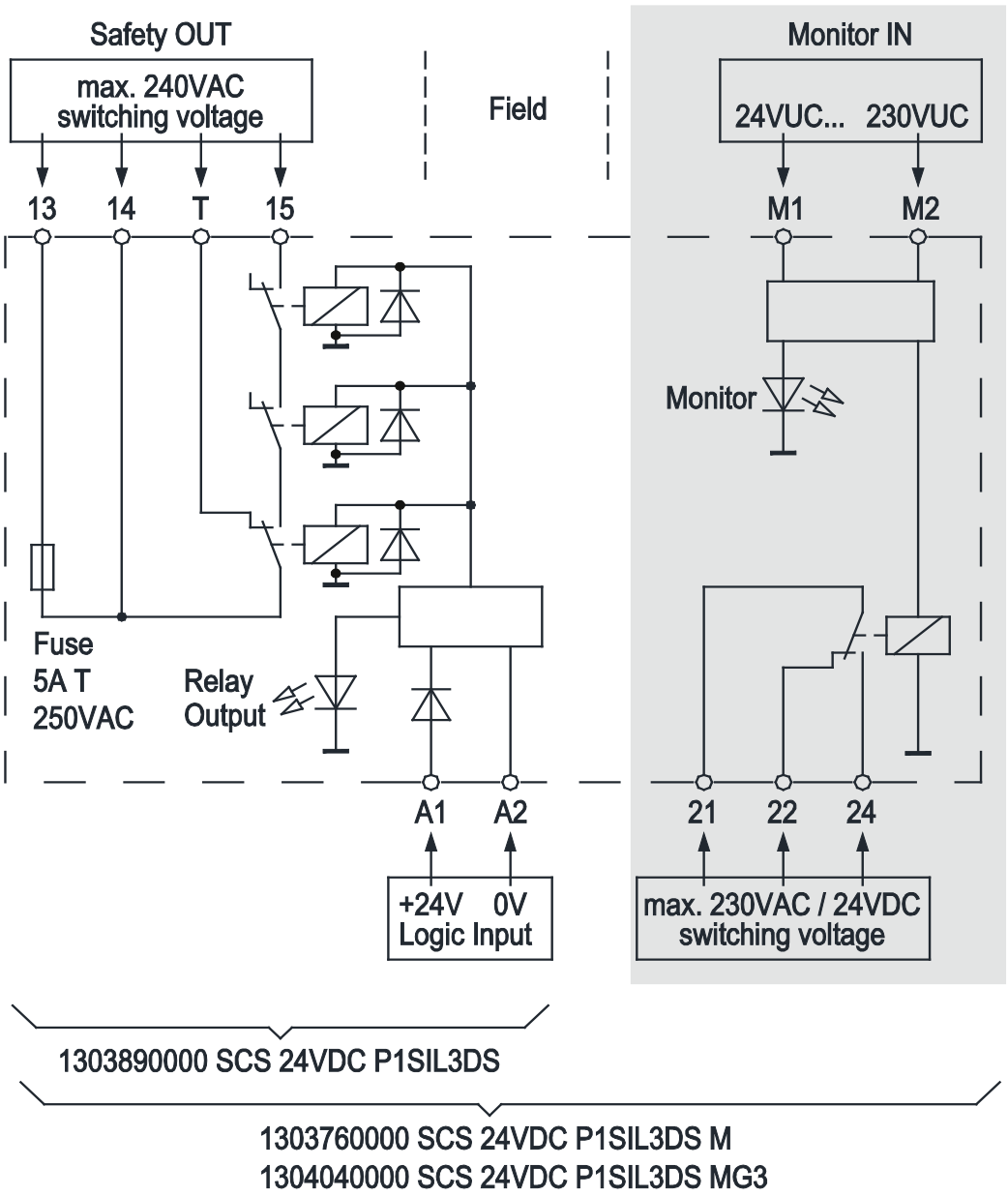
2.2 Design and function

Three relays are connected in parallel in the input circuit (A1/A2). The relay’s output contacts (terminals 13 and 15) are wired in series. Thus, safety-related shutdowns are ensured even where there is a welding contact. The output is protected with a 5 A fuse against overloads and short circuits. The output contacts (terminals 14 and 15) are used when using external fuse protection or when checking the fuse. It is also possible to check the switching status of a relay in the safety circuit by using the output (NC) contact at terminal T.

The relay coils are energised when the nominal voltage of 24 V DC is applied between the input terminals A1 and A2.

The switch function is signalled with the “RELAY OUTPUT” LED display.

2.3 Block diagram



3. Notes on configuring

3.1 Low demand mode of operation

The SIL3 relays from the SAFESERIES are used in low demand mode, when their demand frequency is no more than five times per year and no more than double the repeated testing frequency (refer to DIN EN 61508-4, 3.5.12).

The corresponding parameter is the value $PFD_{avg} = 3.07 \cdot 10^{-6}$, which is valid for a testing interval T_{proof} of 12 years.

3.2 High demand mode of operation

If the “low demand mode of operation” usage cannot be applied, then the SIL3 relay should be used as a safety-critical sub-system operating at high demand mode or continuous mode (DIN EN 61508-4, 3.5.12). The following values are valid for the frequency of demand and the corresponding PFH value:

Once per month	$PFH = 6,83 \cdot 10^{-11}\ h^{-1}$
Once per week	$PFH = 1,83 \cdot 10^{-10}\ h^{-1}$
Once per day	$PFH = 1,08 \cdot 10^{-9}\ h^{-1}$

3.3 Types of malfunctions

A safe failure is not able to render a technical safety system dangerous or non-functional. The SIL3 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 SIL3 relay does not pass to a predefined safe state.

3.4 Test intervals

The test interval is the time between complete repeated tests.

Incidental hardware errors can be detected within this time period (T_{proof} = 12 years).

4. Mounting and installation

The operating instructions for the SIL3 relay with the order number

IS SCS 24VDC P1SIL3DS 1345290000

must be made available.

The instructions, constraints and limitations contained in these instructions must be taken into consideration when installing and operating the SIL3 relay.

The SIL3 relay should be checked to see if it is functioning properly before it is first used and after any wiring change is make. Refer to section 5.1 “Functional check” for more details.

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.

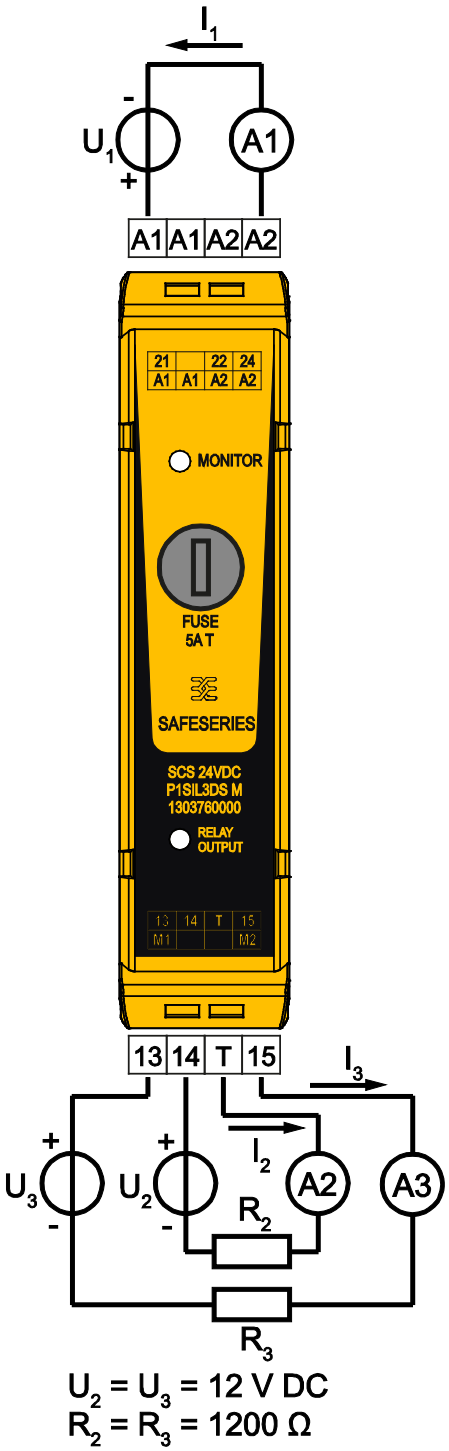
5. Periodic inspections

Periodic functional inspections are used to discover non-visible and dangerous faults which cannot be detected by the self-diagnostics. It is therefore important to check the functionality of the SIL3 relay with the proper frequency.

The operator must determine the type of tests and the proper time intervals. The time intervals are partly determined by the calculation of each individual safety circuit of the system (the PFD values).

The inspections should be carried out so that the flawless operation of the safety functions in conjunction with components can be proven.

5.1 Functional check



(The illustration shows the front view of the parts (order number) 1303760000 SCS 24VDC P1SIL3DS M and the 1304040000 SCS 24VDC P1SIL3DS MG3. The monitoring circuit is not applicable for the part 1303890000 SCS 24VDC P1SIL3DS).

Active input circuit

- Apply U_1 = 21.6 V DC to the connection terminals A1(+) and A2(-)
  - ◊ The current consumption is I_1 = 35 to 44.3 mA (current meter A1)
- The “RELAY OUTPUT” LED lights up
- No electrical connection between terminal 14 and terminal T
  - ◊ The current consumption is I_2 = 0 mA (current meter A2)
- Electrical connection between terminal 14 and terminal 15
  - ◊ The current consumption is I_3 = 10 mA (current meter A3)

Inactive input circuit

- Apply U_1 = 0 V DC to the connection terminals A1(+) and A2(-)
  - ◊ The current consumption is I_1 = 0 mA (current meter A1)
- The “RELAY OUTPUT” LED does not light up
- Electrical connection between terminal 14 and terminal T
  - ◊ The current consumption is I_2 = 10 mA (current meter A2)
- No electrical connection between terminal 13 and terminal 15
  - ◊ The current consumption is I_3 = 0 mA (current meter A3)

6. Technical safety values

6.1 Assumptions

- The monitoring circuit is used exclusively for detecting field signals and responding to the control unit throughout the range 24 to 230 V UC.
  The monitoring circuit should not be used for technical safety-critical operations.
- The max. 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.

6.2 Safety data

Safety basic data	
Safety category	SIL3
Safety standard	DIN EN 61508
Device type	A
HFT	2
T_{proof} in years	12

Safety parameters “low demand mode”		
Frequency of demands	5 per year	
Part of architecture	1oo1	1oo3
PFD_{avg}	$1.31 \cdot 10^{-6}$	$1.75 \cdot 10^{-6}$
λ_{DD} in FIT	0.00	0.00
λ_{DU} in FIT	0.03	1.00
$\lambda_{SD} + \lambda_{SU}$ in FIT	188.97	1.00
λ_{Total} in FIT	189.00	2.00
SFF in %	99.98	50.00
PFD_{avg} (complete)	$3.07 \cdot 10^{-6}$	

Safety parameters “high demand mode”						
Frequency of demands	Once per month		Once per week		Once per day	
Part of architecture	1oo1	1oo3	1oo1	1oo3	1oo1	1oo3
PFH in h^{-1}	$3.33 \cdot 10^{-11}$	$3.43 \cdot 10^{-11}$	$3.33 \cdot 10^{-11}$	$1.48 \cdot 10^{-10}$	$3.33 \cdot 10^{-11}$	$1.05 \cdot 10^{-9}$
λ_{DD} in FIT	0.00	0.00	0.00	0.00	0.00	0.00
λ_{DU} in FIT	0.03	0.69	0.03	2.97	0.03	21.00
$\lambda_{SD} + \lambda_{SU}$ in FIT	188.97	0.69	188.97	2.97	188.97	21.00
λ_{Total} in FIT	189.00	1.38	189.00	5.94	189.00	42.00
SFF in %	99.98	50.00	99.98	50.00	99.98	50.00
PFH in h^{-1} (complete)	$6.76 \cdot 10^{-11}$		$1.82 \cdot 10^{-10}$		$1.08 \cdot 10^{-9}$	

www.weidmueller.com

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold
Germany
Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-292083
info@weidmuller.com
www.weidmueller.com

Order number:
1373930000/02/06-2017