SIL Safety Manual

Manual Monitoring Safety Relay SCS 24VDC P2SIL3ES

Weidmüller

Contact address

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
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 11/2012:

SCS 24VDC P2SIL3ES	1319280000

SIL3 relays in the SCS 24VDC P2SIL3ES series from

Weidmüller Interface GmbH & Co KG
Klingenbergstraße 26
32758 Detmold
Germany

have been certified by

Certification Body TÜV NORD CERT GmbH
Notified Body 0044
Am TÜV 1
45307 Essen
Germany

according to EN 61508 SIL3. They are certified as "EC type-examination" for use in "low demand mode" and "high demand mode" systems.

Certificate Registration No:
44 207 13773715

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 Special product features

- Stop category 0 according to EN 60204-1
- Application up through control category 4 according to EN ISO 13849-1
- Reset button monitoring
- Single- and dual-channel activation
- Cross-connection detection
- 2 enable current paths, 1 signal current path

2.2 General

The safety relay in the SAFESERIES product family is certified according to DIN EN 61508 / SIL3.

It is used for the safety-related switch-off (DTS = de-energised to safe) of system components in the processing industry segment such as combustion plants (according to EN 746-2 and EN 50156) and for the protection of personnel and machinery (emergency stop).

2.3 Design and function

For safety-related switch-off, there are 2 monitoring inputs with cross-connection detection, 2 enable outputs (NO) and an acknowledgement output (NC) with positively-driven contacts.

The output must be protected externally with maximum 5 A T.

The unit can be put into operation with either a falling edge at S33/S34 or with a rising edge at S33/S35 (auto start). The response time for switching on and off at A1/A2 can be reduced from > 50 ms to < 20 ms by removing a bridge at C1/C2.

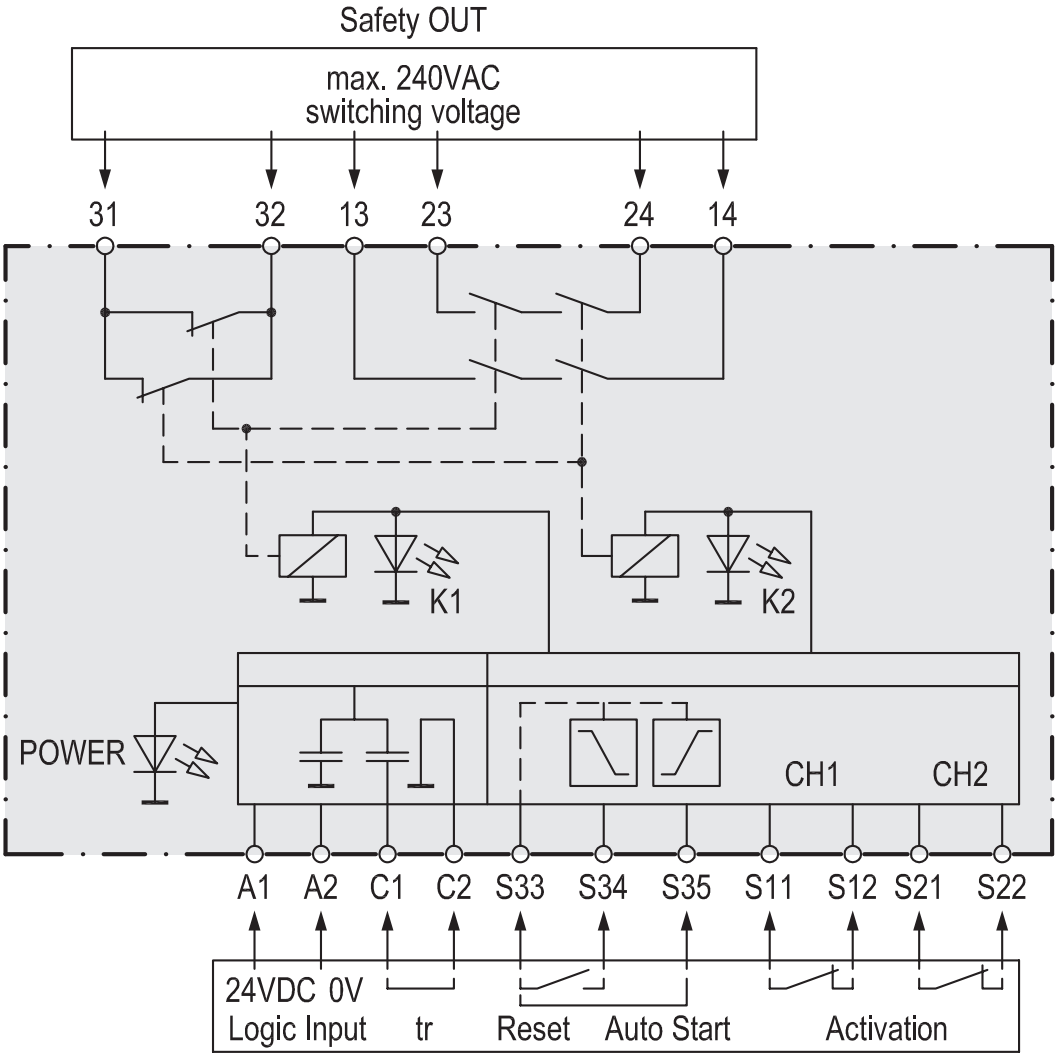
Activation of the safety circuit is done in the field through a PLC with a 24 V digital output at A1/A2 (bridged between S11/S12 and S21/S22) or with corresponding safety contacts (protective curtain, emergency stop button) at S11/S12 and S21/S22 with a fixed operating voltage at A1/A2.

A reset is possible only by opening and closing both monitoring circuits or by turning the operating voltage on and off.

Minimal current consumption of 35 mA at 24 V DC -10 % at the input is guaranteed.

Test pulses (typ < 1 ms) from a PLC for wire-break recognition at A1/A2 do not result in the output relay contacts switching on or off.

2.4 Block diagram



3 Notes on configuring

3.1 Low demand mode of operation according to EN 61508

The SIL3 relays from the SAFESERIES are used in low demand mode, when their demand frequency is no more than one times per year and no more than double the repeated testing frequency (refer to DIN EN 61508-4, 3.5.12).
For the demand rate and the associated PFD parameters at an inspection interval Tproof of 12 years, the values indicated in Table 2 apply.

3.2 High demand mode of operation according to EN 61508

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). For the demand rate and the associated PFH parameters, the values indicated in the following table 3 apply:

3.3 High demand mode of operation according to EN ISO 13849-1

For the demand rate and the associated PFH parameters, the values indicated in Table 4 apply.

3.4 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.

3.5 Test intervals

The test interval or inspection interval T_{proof} is the timeframe in which tests are conducted in full and are repeated.
All hardware failures are recognised within this period of time.

Table 1

Safety basic data	
Safety category	SIL3
Safety standard	DIN EN 61508
Device type	A
HFT	1

Table 2

Safety parameters “low demand mode” according to EN 61508							
Switching cycle	**PFH**	**SFF**	**λ_{SD}**	**λ_{SU}**	**λ_{DD}**	**λ_{DU}**	**SIL**
1× per year	$2{,}3 \times 10^{-12}\ h^{-1}$	99,99 %	$1{,}13 \times 10^{-1}$ FIT	$1{,}6 \times 10^{+1}$ FIT	$1{,}13 \times 10^{-1}$ FIT	$1{,}14 \times 10^{-3}$ FIT	3

FIT = $10^{-9}\ h^{-1}$ (Failure in time)

Table 3

Safety parameters “high demand mode” according to EN 61508							
Switching cycle	**PFH**	**SFF**	**λ_{SD}**	**λ_{SU}**	**λ_{DD}**	**λ_{DU}**	**SIL**
1× per day	$7{,}87 \times 10^{-10}\ h^{-1}$	99,58 %	$4{,}11 \times 10^{+1}$ FIT	$1{,}64 \times 10^{+1}$ FIT	$4{,}11 \times 10^{+1}$ FIT	$4{,}15 \times 10^{-1}$ FIT	3
10× per day	$8{,}41 \times 10^{-9}\ h^{-1}$	99,51 %	$4{,}12 \times 10^{+2}$ FIT	$2{,}02 \times 10^{+1}$ FIT	$4{,}12 \times 10^{+2}$ FIT	4,17 FIT	3

FIT = $10^{-9}\ h^{-1}$ (Failure in time)

Table 4

Safety parameters “high demand mode” according to EN ISO 13849-1						
Switching cycle	**PFH**	**MTTFD**	**λ_{SD}**	**λ_{SU}**	**λ_{DD}**	**λ_{DU}**
1× per year	$2{,}3 \times 10^{-12}\ h^{-1}$	2500	$1{,}13 \times 10^{-1}$ FIT	$1{,}6 \times 10^{+1}$ FIT	$1{,}13 \times 10^{-1}$ FIT	$1{,}14 \times 10^{-3}$ FIT
10× per day	$8{,}41 \times 10^{-9}\ h^{-1}$	270	$4{,}12 \times 10^{+2}$ FIT	$2{,}02 \times 10^{+1}$ FIT	$4{,}12 \times 10^{+2}$ FIT	4,17 FIT

FIT = $10^{-9}\ h^{-1}$ (Failure in time)
Diagnostic coverage (DC): 99%
Hardware category: 4
Performancelevel (PL): e

4 Mounting and installation

The operating instructions for the SIL3 relay with the order number

IS SCS 24VDC P2SIL3ES 1412550000

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 chapter 5.1 „Functional check“ for more details.

The device may be operated only with an external fuse.

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

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

Functional testing is done in three steps according to the following tables.

5.1.1 “Reset” functional test

Input voltage: 24 V DC

Connection: S33/S34

Reset	Monitoring		Indication		Output		Acknowl-edgement
S33/S34	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
0→1→0	open	open	OFF	OFF	open	open	closed
0→1→0	closed	open	OFF	OFF	open	open	closed
0→1→0	open	closed	OFF	OFF	open	open	closed
0→1→0	closed	closed	ON	ON	closed	closed	open

5.1.2 “Auto Start” functional test

Input voltage: 24 V DC

Connection: S33/S35

Control input	Monitoring		Indication		Output		Acknowl-edgement
A1/A2	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
0→1	open	open	OFF	OFF	open	open	closed
0→1	closed	open	OFF	OFF	open	open	closed
0→1	open	closed	OFF	OFF	open	open	closed
0→1	closed	closed	ON	ON	closed	closed	open

5.1.3 “Monitoring” functional test

Input voltage: 24 V DC

Connection: S33/S35

Test step	Monitoring		Indication		Output		Acknowl-edgement
	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
1.	closed	closed	ON	ON	closed	closed	open
2.	open	closed	OFF	ON	open	open	closed
3.	closed	closed	OFF	ON	open	open	closed
4.	closed	open	OFF	OFF	open	open	closed
5.	closed	closed	ON	ON	closed	closed	open
6.	open	open	OFF	OFF	open	open	closed

6 Technical safety values

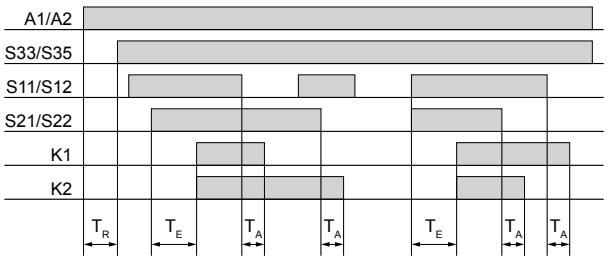
6.1 Assumptions

- The max. allowable ambient temperature is 55 °C.
- The environmental conditions correspond to the average industrial environment.
- The specifications in the data sheet and the operating instructions should not be exceeded.

7 Functional diagrams

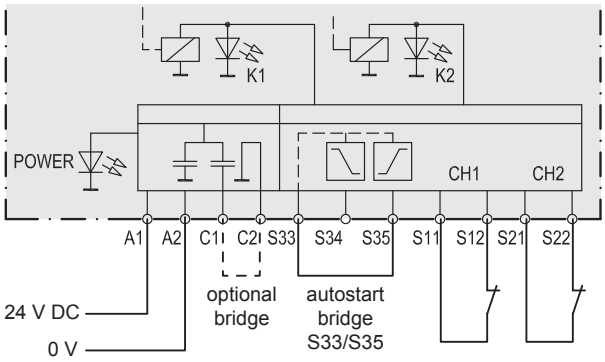
7.1 Auto start

Reset input S33 is connected to S35. Supply voltage is applied to A1/A2. The unit starts with a rising edge of the signal at safety inputs S11/S12 and S12/S22.



T_E = 30 ms (switch-on time K1 and K2)
T_A = 15 ms (switch-off time K1 and K2)

T_R = typ. 50 ms (reaction time with bridge over C1/C2)
T_R = typ. 20 ms (reaction time without bridge over C1/C2)

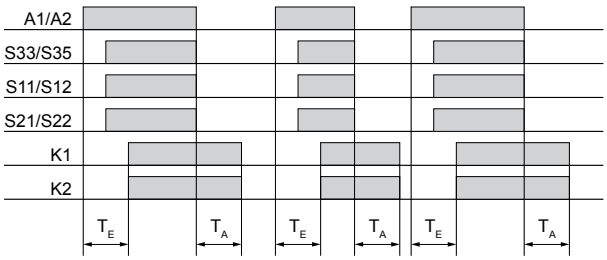


Attention

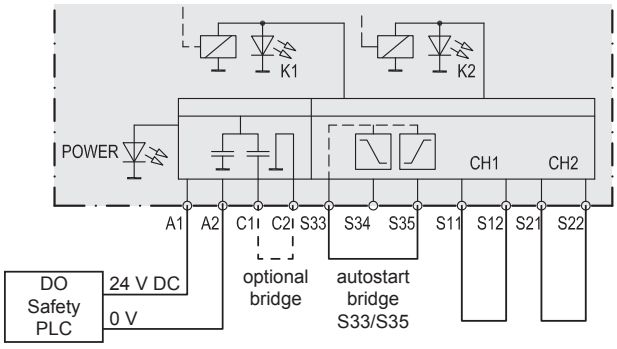
Make absolutely certain that there is no unexpected start-up after there has been an interruption in the supply voltage.

7.2 Start through A1/A2

Reset input S33 is connected to S35. Safety inputs S11/S12 and S12/S22 are bridged. After application of supply voltage at A1/A2, the enable current paths are closed.



T_E = 55 ms (switch-on time K1 and K2 with bridge over C1/C2)
T_A = 55 ms (switch-off time K1 and K2 with bridge over C1/C2)

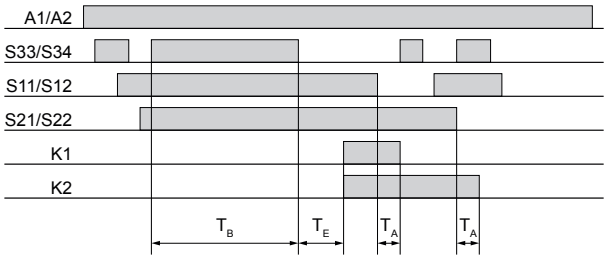


Attention

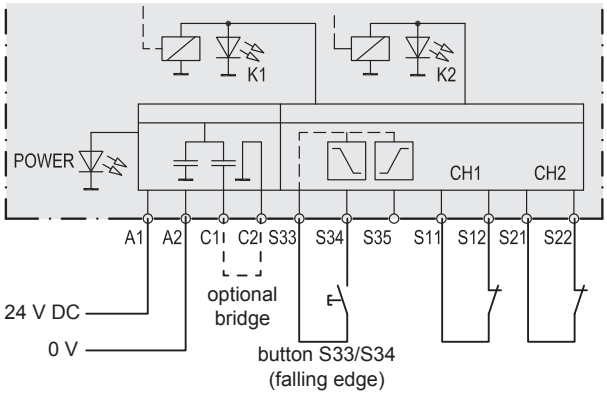
Make absolutely certain that there is no unexpected start-up after there has been an interruption in the supply voltage.

7.3 Manual start – triggering on a falling edge

When the safety inputs are closed, the reset input S34 is opened using a button (triggering on a falling edge)

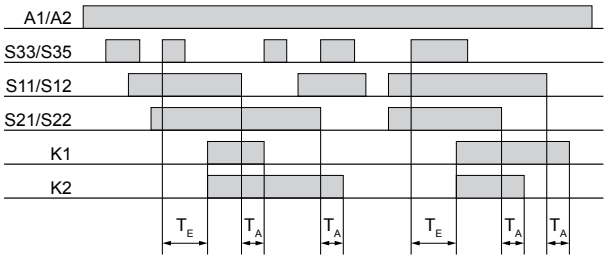


T_B = 100 ms (recovery time)
T_E = 30 ms (switch-on time K1 and K2)
T_A = 15 ms (switch-off time K1 and K2)

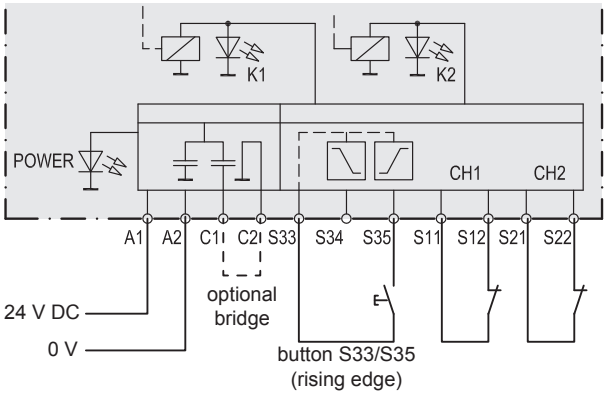


7.4 Manual start – triggering on a rising edge

When the safety inputs are closed, the reset input S35 is closed using a button (triggering on a falling edge)



T_E = 30 ms (switch-on time K1 and K2)
T_A = 15 ms (switch-off time K1 and K2)



8 Modes of operation / notes

- Single- or dual-channel activation
  - For single-channel activation, there is no cross-connection detection.

- Restart lockout
  - There is no restart after the safety inputs have been opened and closed.
    A restart can be accomplished only by activating the Reset button.
    For the restart lockout, the reset inputs are to be activated with a button as in the “Manual start” mode of operation.

www.weidmueller.com

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

1438130000/03/03-2023