SIL-Slam 2021

Sichere Fehler – EN 62061 kontra EN 61508

SAFE ≠ SAFE ?

Stephan Aschenbrenner

About the presenter

- Stephan H. Aschenbrenner, CFSE
  - Dipl. Ing. (Univ) for Electrical Engineering and Automation of the Technical University of Munich (TUM)
  - Start as a software and hardware developer of programmable electronic systems
  - At TÜV Product Service GmbH responsible for machinery safety components later at TÜV Product Service Inc. in the USA responsible for setting up a functional safety department for the Americas
  - Business Unit Manager at TÜV Product Service
  - Since 2001 at *exida.com* GmbH involved in both product analysis and design process improvements in the process industry, the machinery industry, as well as in the automotive and semiconductor industry
  - Responsible for *exida's* FMEDA tool SILcal
  - Since 2007 Certified Functional Safety Expert (CFSE)
  - Since 2013 Managing Partner at *exida.com* GmbH
  - Since 2017 Head of AK 914.0.4 (German IEC 61508-1/-2 committee)
  - Since 2017 Active member of MT 61508-1/-2
  - Since 02.2020 CEO at *exida.com* GmbH
  - Over twenty-six years of experience and extensive knowledge in the safety and reliability field

Background

- IEC 61508
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 62061
  - Safety of machinery – Functional safety of safety-related control systems
- IEC TS 63394
  - Safety of machinery – Guidelines on functional safety of safety-related control system

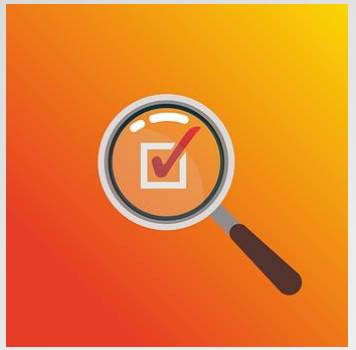
Definitions “safe failure”

IEC 61508

3.6.8
safe failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state



IEC 62061

3.2.53
safe failure
failure of an SCS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:2010, 3.6.8, modified – terminology adapted to machinery]

IEC TS 63394

3.2.48
safe failure
failure of an SCS or SRP/CS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:2010, 3.6.8, modified – terminology adapted to machinery]

Definitions

- **IEC 61508**

3.6.14
no effect failure
failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function

NOTE 1 The no effect failure has by definition no effect on the safety function so it cannot contribute to the failure rate of the safety function.

NOTE 2 The no effect failure is not used for SFF calculations.

- **IEC 62061**

  N/A

IEC TS 63394

N/A

Identification of failure modes (here SAFE)

- B.4.2.2 of IEC 62061

Identification of failure modes:

A fault of an electromechanical component generally represents a situation (state) that can lead to a failure. Assuming that the safe state is an open circuit:

– the contact remains open: safe state;
– the contact remains closed: dangerous state.

The theoretical failure effects of the position switch are:

– the contact will not (anymore) open: dangerous failure (unintended closed);
– the contact will open "by itself": safe failure
– the contact will not (anymore) close: safe failure
– the contact will close "by itself": dangerous failure (unintended closed).

NOTE See also failure modes in IEC 60947-4-1.

Failure mode SAFE

B.4.2.2 of IEC 62061

Identification of failure modes:

A fault of an electromechanical component generally represents a situation (state) that can lead to a failure. Assuming that the safe state is an open circuit:

- the contact remains open: safe state;
- the contact remains closed: dangerous state.

The theoretical failure effects of the position switch are:

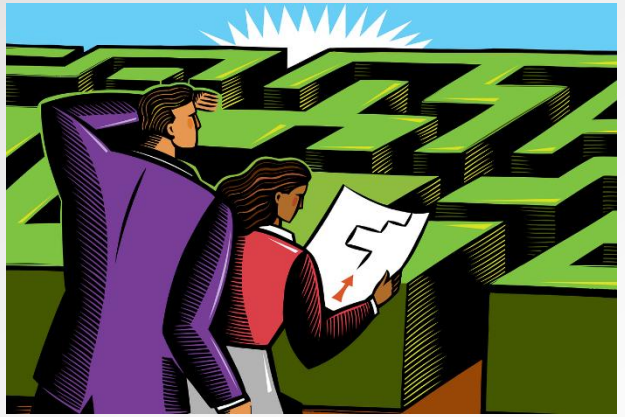
- the contact will not (anymore) open: dangerous failure (unintended close
- the contact will open "by itself": safe failure (unintended op ned dered as very unlikely for an electromechanical device);
- the contact will not (anymore) close: safe failure which ot have any influence of the safety function (unintended opened);
- the contact will close "by itself": dangerous failure (unintended closed).

NOTE See also failure modes in IEC 60947-4-1.

3.6.8
safe failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe tate or maintain a safe state; or

b) s the probability of the spurious operation of the safety function to put the EUC (or t reof) into a safe state or maintain a safe state



Source: Pixabay revzck, Pixabay license

SAFE = no effect ?

B.4.2.2 of IEC 62061

Practical considerations:

The opening of the guard door defines the failure modes of the position switch to be considered. That means that practically no safe failures of the position switch related to this safety function exist:

- the failure mode “unintended closed” contact is always dangerous (typical dangerous failure of the position switch);
- the failure mode “unintended opened“ contact is not relevant for the opening of the guard door and only has an influence on the availability of the machine. It is a no effect failure (IEC 61508-4:2010, 3.6.14) for the defined function. Therefore, it is not a safe failure and $\lambda_S = 0$.

https://pixabay.com/de/photos/fragezeichen-frage-wissenschaft-3483960/

SAFE ≠ SAFE ?

B.4.2.2 of IEC 62061

Identification of failure modes:

A fault of an electromechanical component generally represents a situation (state) that can lead to a failure. Assuming that the safe state is an open circuit:

- the contact remains open: safe state;
- the contact remains closed: dangerous state.

The theoretical failure effects of the position switch are:

- the contact will not (anymore) open: dangerous failure (unintended closed);
- the contact will open "by itself": safe failure
- the contact will not (anymore) close: safe failure
- the contact will close "by itself": dangerous failure (uni… …ed).

NOTE See also failure modes in IEC 60947-4-1.

Prac… …iderations:

The opening of the … defines the failure modes of the position switch to be considered. That means that practica… … failures of the position switch related to this safety function exist:

- the failure mode "unintended closed … …ways dangerous (typical dangerous failure of the position switch);
- the failure mode "unintended opened" contact is no… …f… the opening of the guard door and only has an influence on the availability of the … …e. It is a no effect failure (IEC 61508-4:2010, 3.6.14) for the defined function. Therefo…, it is not a safe failure and $\lambda_S = 0$.

WHY ?

The table below lists the normal failure rates and the percentage of dangerous failures for SIRIUS product groups (operating in low demand mode).

Siemens SIRIUS product group (electromechanical components)	Normal failure rate (in FIT) 1)	Ratio of dangerous failures 2)
EMERGENCY STOP control devices (with positive opening contacts)	100 3)	20%
Cable-operated switches for EMERGENCY STOP function (with positive opening contacts)	100 3)	20%
Standard position switches (with positive opening contacts)	100	20%
Position switches with separate actuator (with positive opening contacts)	100	20%
Position switches with solenoid interlocking (with positive opening contacts)	100	20%
Hinge switches (with positive opening contacts)	100	20%
Pushbuttons (non-latching) (with positive opening contacts)	100	20%
Contactors / motor starters (with positively driven contacts or mirror contacts)	100	<40% 4)
Circuit breakers 3RV	50	<40%
Compact branch (3RA6)	100 5)	<40% 5)

1) The failure rate data in the table is limited to 100 FIT (except circuit breakers, which are limited to 50 FIT)
2) Valid under the above-mentioned conditions
3) Also limited to 100 FIT due to protection against tampering together with latching
4) The SIL level can be improved by means of fault detection using positively driven auxiliary switches
5) Temporary value

Table D.1 – Examples of the failure mode ratios for electrical/electronic components

Component	Failure mode	Typical failure mode ratios %
Switch with positive opening on demand, for example push button, emergency stop device, position switches, cam operated, selector switches	Contacts will not open	20
	Contacts will not close	80

B.4.2.2 Evaluation of SFF

The safe failure fraction (SFF) can be calculated using the following equation:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

where

λ_S is the rate of safe failure,

$\sum \lambda_S + \sum \lambda_D$ is the overall failure rate,

λ_{DD} is the rate of dangerous failure which is detected by the diagnostic functions,

λ_D is the rate of dangerous failure.

Depending from the safety function, a failure can be safe (λ_S) or dangerous (λ_D).

SAFE ≠ SAFE ?

Picture: dooder

https://pixabay.com/de/illustrations/fragezeichen-frage-antwort-1019993/

Conclusion

- Stay consistent between standards
- Don’t classify “safe” failures as “no effect” failures in order to lower the SFF
- If you are not happy with an HFT=0 system, then require HFT=1

excellence in dependable automation

Many Thanks for your Attention

stephan.aschenbrenner@exida.com

+49/8362-507274