

Functional Safety – One Position switch

SIRIUS 3SE5

FAQ • November 2010



Safe Machine Concepts without Detours –



benefit from the Safety Evaluation Tool.

Service & Support

Answers for industry.

SIEMENS

This document is from the Service&Support portal of Siemens AG, Industry Automation and Drive Technologies. The terms of use listed on this web site apply (www.siemens.com/terms_of_use).

The link below takes you directly to the download page of this document.

<http://support.automation.siemens.com/WW/view/en/45787668>

Question

Which safety integrity according to IEC 62061 and ISO 13849-1 in a safety function can be claimed by the use of one single position switch with separate actuator in combination with a non safety-related part, e.g. a proximity switch?

Answer

With a two-channel architecture in combination of a non safety-related part, max. SIL 3 according to IEC 62061 or PL e in accordance with ISO 13849-1 can be achieved in conjunction with a safety-related evaluation, for instance a fail-safe controller.



The information in this document was tested by SP, Technical Research Institute of Sweden.

Table of Contents

1	Introduction	4
1.1	Requirements	4
1.2	Required hardware and software	5
1.3	Exemplary Software solution with a modular safety system 3RK3	7
2	Safety Function	8
3	Interconnection Examples	9
3.1	Two-channel architecture	9
4	Safety-related Evaluation	10
4.1	Two-channel architecture	10
4.1.1	DETECTING (sensor circuit)	10
4.1.2	EVALUATING (safety-related evaluation)	12
4.1.3	REACTING (actuator circuit)	12
4.1.4	Result	14
5	Validation / Check List	15
6	References	16
6.1	References	16
6.2	Internet links	16

1 Introduction

Based on the Functional Safety standards, IEC 62061 and ISO 13849-1, it is possible to assess safety functions with regard to quality and quantity evaluation of use of safety-related and non safety-related parts.

Position switches with separate actuator frequently are used in guard and guard interlocking applications.

Sample application:

When a guard will be opened the hazardous movement(s) must be terminated.

1.1 Requirements

The use and the assessment of the position switch with separate actuator in a safety function is possible only in conjunction with a safety-related evaluation, for example, using a fail-safe SIMATIC S7 F controller or a 3RK3 modular safety system.

The background is the control of failures by means of suitable diagnostic measures and thus required fault reactions.

Note

Other safety-related evaluations can be used alternatively if a cross comparison (of the input signals) in the sense of “discrepancy monitoring” is ensured for a two-channel design.

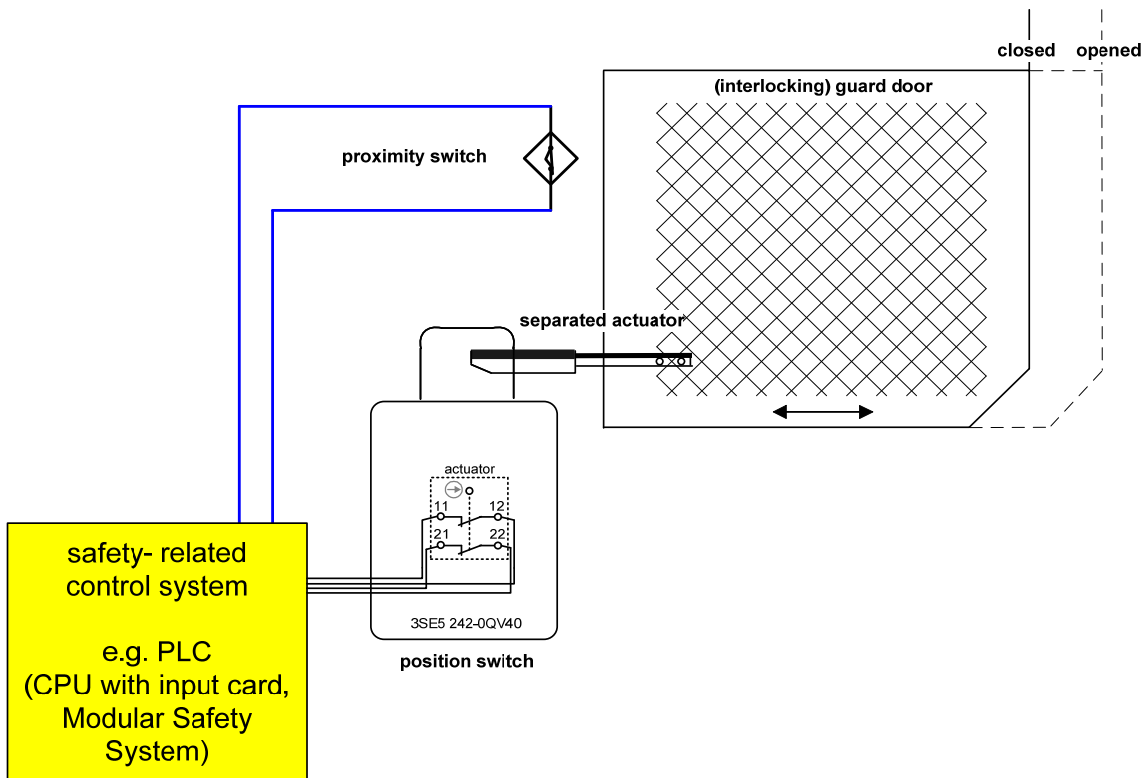
1.2 Required hardware and software

The representations and descriptions of this FAQ are based on the following hardware and software components:

Hardware components

A 3SE5242 position Switch with Tumbler is considered as an example.

Figure 1-1



Safety-related control function with a control system:

Monitoring of the separated actuator by dynamical plausibility control based on the proximity switch is realized by a safety-related control system, CPU and input card or Modular Safety System.



DANGER

Constructive measures and the fault reaction time must be taken into account: This concerns especially the use of the non “well-tried” component (e.g. the proximity switch) according to ISO 13849-2.

The safety-related evaluation is performed using a 3RK3 modular safety system.

NOTICE

Design and selection of the interlocking switch shall fulfill the requirements of EN 1088 (or ISO 14119 under revision).

Standard software components

At this point, the requirements according to IEC 62061 or ISO 13849-1 with regard to the used software are not considered in detail since the component manufacturer provides the qualified software environment.

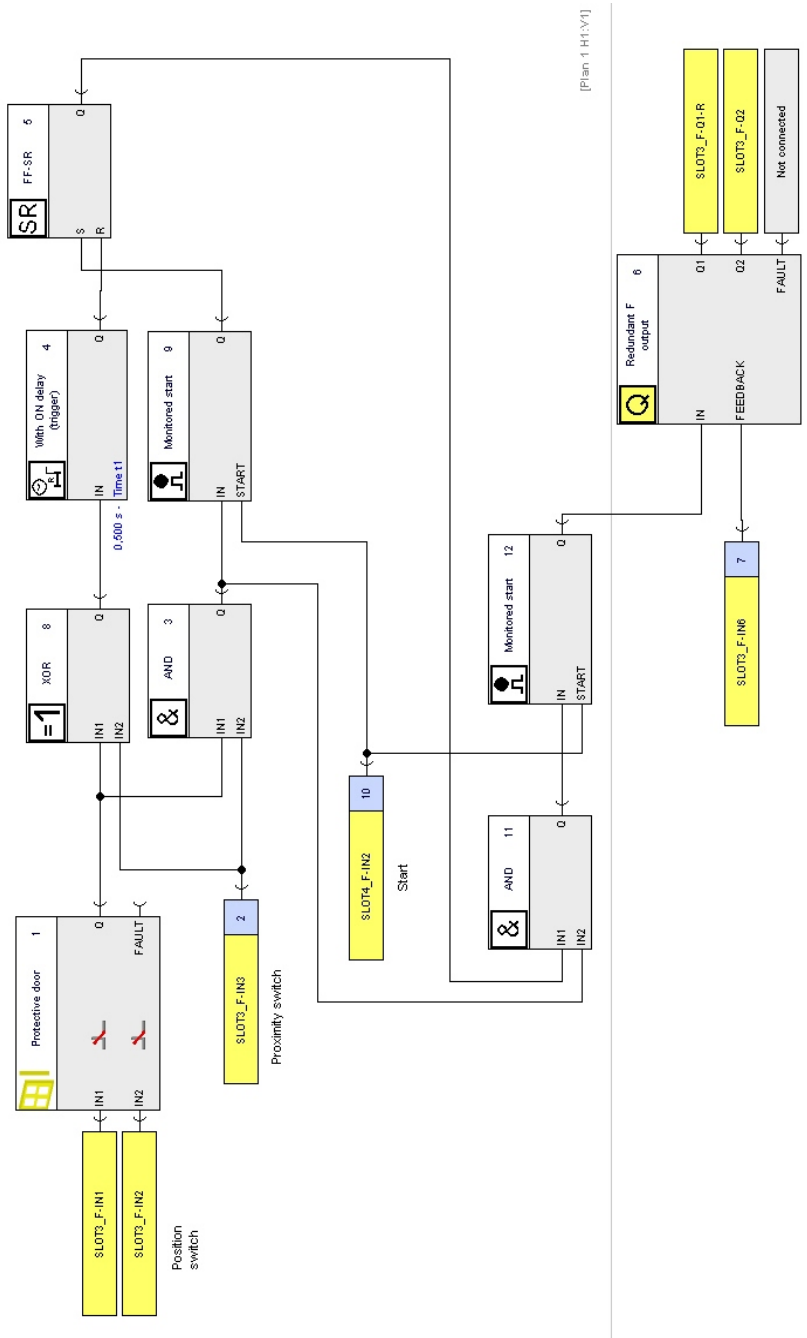
NOTICE

A two-channel architecture always requires a cross comparison of the components (thus of the input signals) in the sense of “discrepancy monitoring”.

1.3 Exemplary Software solution with a modular safety system 3RK3

Following figure shows an exemplary configuration of the modular safety system 3RK3 (the software Modular Safety System ES is pre-certified to be used up to SIL 3 acc. to IEC 61508 and PL e acc. to ISO 13849-1).

Figure 1-2



2 Safety Function

The functional description of the safety function is as follows:

“When the guard door will be opened the drive must be stopped.”

The considerations are based on two-channel architecture.

Based on the risk assessment, the stop can be non-delayed with Stop Category 0 or delayed with Stop Category 1 according to IEC 60204-1.

It is assumed that the safety function is demanded once per hour (or 8760 times per year). High demand mode merely affects the calculations of the actuator circuit – basically, it does not influence the results.

Reason In machinery (factory automation) high demand mode is typical due to the fact that the safety function will be performed more than on time per year, in difference to the process industry where the low demand mode is used.

As an example, the entire safety function with all used components is assessed.

NOTICE

The following explanations only show the basic interconnections and their assessment.

All other requirements of the listed standards such as common cause failure (CCF) and systematic integrity must always be additionally considered:

The person who validates the safety function is responsible for the fulfillment of the SIL acc. to IEC 62061 or PL acc. to ISO 13849 and of all requirements not mentioned in this document.

NOTICE

One single position switch with or without interlocking is characterized by an individual and not unique coded actuator.

Measures against manipulation or misuse shall be taken into account (see Machinery Directive, Annex I, 1.1.2 and EN 1088 under revision).

The following described example represents one solution due to a diagnostic or monitoring function based on the evaluation of a supplement initiator, e.g. proximity switch as a non well-tried component according to ISO 13849-2.

3 Interconnection Examples

Base is two-channel architecture of following explications.

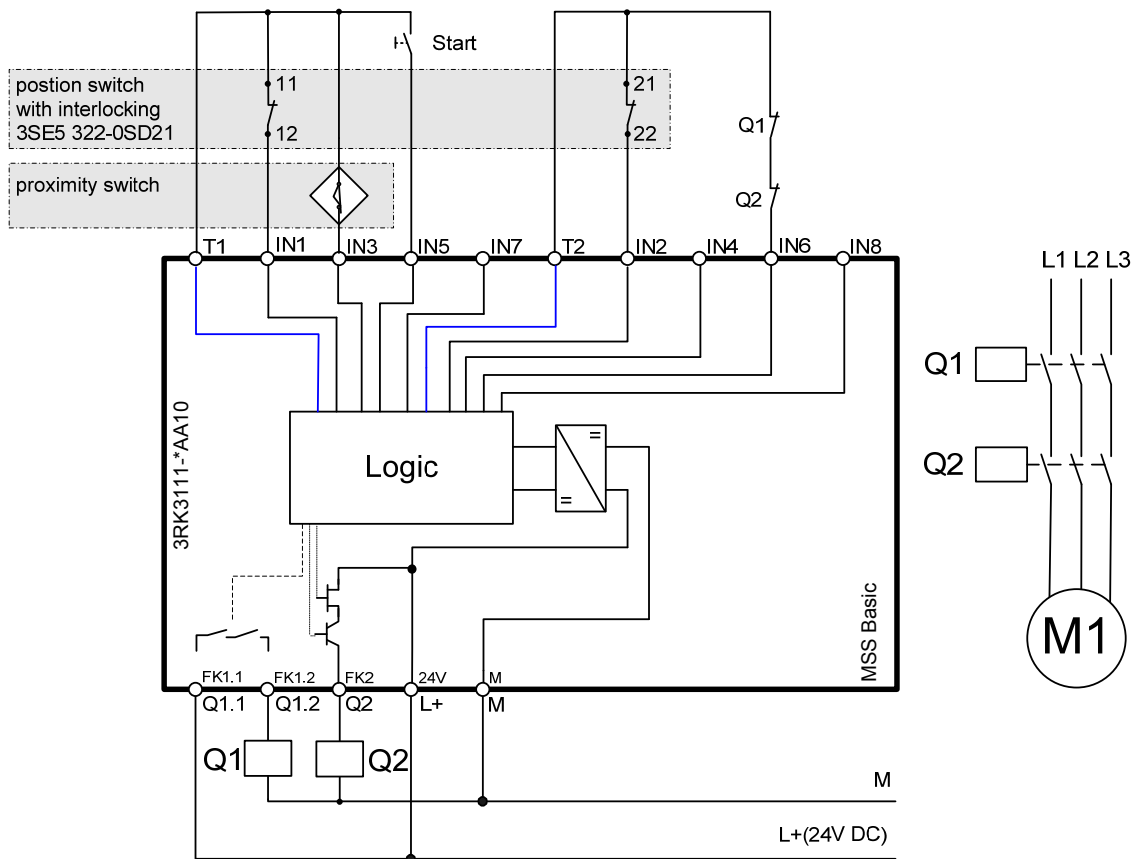
3.1 Two-channel architecture

A fault does not lead to the loss of the safety function.

Reason Two-channel (electrical) control of the position switch and dynamical plausibility control in conjunction of the proximity switch evaluation.

For detailed assessment see 4.1.1.

Figure 3-1



4 Safety-related Evaluation

Assessment is based on two-channel architecture of the safety function.

4.1 Two-channel architecture

4.1.1 DETECTING (sensor circuit)

A hardware fault tolerance (HFT) of 1 according to IEC 62061 or Category 4 in accordance with ISO 13849-1 can be selected.

Reason The position switch may fail when the separate actuator will break. A fault exclusion would limit the achievable SIL CL up to SIL 2 (see 6.7.7, exception in IEC 62061) or PL up to PL d based on Category 3.

The supplement (control) use of a proximity switch allows “bypassing” this fault exclusion: the loss of the safety function due to a failure of the separate actuator can be detected by a dynamical (time, plausibility) control in dependence of the proximity switch and the electrical contact elements of the position switch.

A strong relationship in sense of plausibility of the signal states of both parts (proximity and position switch) must be implemented.

The diagnostic coverage (DC) can be assumed to be 99 %.

Reason The positively driven contacts (physically) will not defeat at the same time due to wearing of the mechanical part of the position switch.

Additionally, the proximity switch control (third channel) improves the diagnostic coverage (see table E.1, “cross monitoring ...” of ISO 13849-1).



DANGER

Calculation of average probability of random hardware failures basically is calculated on the failure rates of the position switch.

The use of the proximity additionally will improve the diagnostic function to detect one critical failure of the guard door monitoring that could lead to the loss of the safety function – the separate actuator breaks at the moment when the guard door will be closed. This failure must be controlled by performing a fault reaction: in this special failure the proximity switch will be able by next opening of the guard door to perform the safety function.

Due to permanently monitoring and controlling of the correct functioning of the proximity switch (time based control in relation with the electrical signals of the position switch) an accumulation of failures may be excluded. In this case a loss of the safety function also can be excluded due to the fault reaction initiated by the proximity switch.

Further the use of different technologies represents an effective measure against common cause failure.

The maximum safety integrity that can be achieved is listed below:

ISO 13849-1

The $MTTF_d$ of each channel is calculated as follows:

$$n_{op} = 8760 \text{ [operations/year] (one time per hour)}$$

$$MTTF_d = \frac{B10_d}{0.1 \cdot n_{op}} = 5.71 \text{ E}+03 \text{ [years]}$$

$$B10_d = \frac{B10}{\text{Ratio of dangerous failures}} = 5,000,000 \text{ [switching cycles]}$$

$B10 = 1,000,000$ (manufacturer information, SN31920)

Ratio of dangerous failures = 20 % (manufacturer information, SN31920)

- PL e according to table 7
 - Category 4 (no fault exclusion of break of separate actuator)
 - DC_{avg} high (99 %)
 - $MTTF_d$ of each channel high (> 30 years)
- Average probability of dangerous failures
 - Annex K
 - $PFH_D = 2.47 \text{ E}-08$

The assumed useful lifetime (manufacturer information) is 20 years.

IEC 62061

The failure rate λ_D of one contact element of the position switch is calculated as follows:

$$C = 1 \text{ [operations per hour]}$$

$$\lambda_D = (\text{Ratio of dangerous failures}) \cdot \frac{0.1 \cdot C}{B10} = 2.00 \text{ E}-08$$

$B10 = 1,000,000$ (manufacturer information, SN31920)

Ratio of dangerous failures = 20 % (manufacturer information, SN31920)

- Architectural constraint SIL CL = 3 according to table 5
 - $DC = 99 \%$
 - $SFF = 99 \%$ (due to DC)
 - $HFT = 1$
- Average probability of dangerous failures
 - Subsystem architecture D (two-channel with diagnostics)
 - $\beta = 0.1$ (worst case CCF factor)
 - $T_1 = 175,200$ [hours] (20 years, 8760 hours/year)
 - $T_2 = 1$ [hours]
 - $DC_{\text{Subsystem element 1}} = DC_{\text{Subsystem element 2}} = 99 \%$
 - $PFH_D = 2.00 \text{ E}-09$

The assumed useful lifetime (manufacturer information) is 20 years.

4.1.2 EVALUATING (safety-related evaluation)

According to the manufacturer documentation, the 3RK3 modular safety system can be used up to max.

SIL 3 according to IEC 62061
or
 PL e according to ISO 13849-1.

The average probability of dangerous failures specified by the manufacturer is $PFH_D = 5.14 \text{ E-}09$.

4.1.3 REACTING (actuator circuit)

A hardware fault tolerance (HFT) of 1 according to IEC 62061 or Category 4 in accordance with ISO 13849-1 can be selected.

Reason A fault (welding of the main circuit contacts) of a contactor is detected by means of the mirror contacts.

The diagnostic coverage (DC) can be assumed to be 99 %.

Reason The mirror contacts of the power contactor allow this high diagnostic coverage: If a power contactor has a fault (failure of the main circuit contacts), reactivation is prevented (see table E.1, "cross monitoring ..." of ISO 13849-1).

The maximum safety integrity that can be achieved is listed below:

ISO 13849-1

The $MTTF_d$ of each channel is calculated as follows:

$$n_{op} = 8760 \text{ [operations/year]}$$

$$MTTF_d = \frac{B10_d}{0.1 \cdot n_{op}} = 2.56 \text{ E+}05 \text{ [years]}$$

$$B10_d = \frac{B10}{\text{Ratio of dangerous failures}} = 1,333,333 \text{ [switching cycles]}$$

$$B10 = 1,000,000 \text{ (manufacturer information, SN31920)}$$

$$\text{Ratio of dangerous failures} = 75 \% \text{ (manufacturer information, SN31920)}$$

- PL e according to table 7
 - Category 4
 - DC_{avg} high (DC = 99 %)
 - $MTTF_d$ of each channel high (> 30 years)
- Average probability of dangerous failures
 - Annex K with $MTTF_d$ of each channel max. 100 years
 - $PFH_D = 2.47 \text{ E-}08$

The assumed useful lifetime (manufacturer information) is 20 years.

IEC 62061

The failure rate λ_D of a power contactor is calculated as follows:

$$C = 1 \text{ [operations per hour]}$$

$$\lambda_D = (\text{Ratio of dangerous failures}) \cdot \frac{0.1 \cdot C}{B10} = 7.50 \text{ E-08}$$

B10 = 1,000,000 (manufacturer information, SN31920)

Ratio of dangerous failures = 75 % (manufacturer information, SN31920)

- Architectural constraint SIL CL = 3 according to table 5
 - DC = 99 %
 - SFF = 99 % (due to DC)
 - HFT = 1
- Average probability of dangerous failures
 - Subsystem architecture D (two-channel with diagnostics)
 - $\beta = 0.1$ (worst case CCF factor)
 - $T_1 = 175,200$ [hours] (20 years, 8760 hours/year)
 - $T_2 = 1$ [hours]
 - $DC_{\text{Subsystem element 1}} = DC_{\text{Subsystem element 2}} = 99 \%$
 - $PFH_D = 7.50 \text{ E-09}$

The assumed useful lifetime (manufacturer information) is 20 years.

4.1.4 Result

The entire safety function complies with the following safety integrity:

Table 4-1

SRP/CS or subsystem	ISO 13849-1		IEC 62061	
	PL	PFH _D	SIL CL	PFH _D
DETECTING	PL e	2.47 E-08	SIL 3	2.00 E-09
EVALUATING	PL e	5.14 E-09	SIL 3	5.14 E-09
REACTING	PL e	2.47 E-08	SIL 3	7.50 E-09
Result	PL e	5.45 E-08	SIL 3	1.46 E-08

Notes

- The limit for SIL 3 or PL e is 1.00 E-07.
- The determined PFH_D values are determined by the 3SE5 and the power contactors and reach max. 49.4 % of the limit when using ISO 13849-1:
The PFH_D value of the power contactors is limited by a max. possible MTTF_d of each channel in Annex K of 100 years.
- A calculation according to IEC 62061 is not limited and therefore yields a better result (14.6 % of the limit).
However, the result does not change fundamentally and both methods can be considered as equivalent.

5 Validation / Check List

Table 5-1

Protocol No.:		Page 1 of 1
Client:		
Testing location:		
Test specification.:		
Machine/line:		
Circuit diagram no:		
Safety zone / function:		
Used components		
Sensor(s) manufacturer/type/item number	Logic manufacturer/type/item number	Actuator(s) manufacturer/type/item number
Adjusted parameter	Hardware / Software	
Fault injection (contact elements of position switch)	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Fault injection (proximity switch)	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Consideration of time delay of the proximity switch (software and mounting)	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Issued by:		Reviewed by:
Date	Name/Position	Signature
Other Aspects:		
Reference to SET report		
Abbreviations:		
<i>SET</i>	<i>Safety Evaluation Tool</i>	

6 References

6.1 References

This list is not complete and only presents a selection of related references.

Table 6-1

Reference	Title
\1\ IEC 62061:2005	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
\2\ ISO 13849-1:2008	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
\3\ ISO/DIS 13849-2:2010	Safety of machinery – Safety-related parts of control systems – Part 2: Validation
\4\ EN 1088:1995 (ISO/CD 14119:2010)	Safety of machinery – Interlocking devices associated with guards – Principles for design and selection
\5\ Brochure	Functional Safety of Machines and Systems – Easy Implementation (Order no.: E20001-A230-M103-V3-7600)
\6\ Technical book:	Patrick Gehlen Funktionale Sicherheit von Maschinen und Anlagen Umsetzung der Europäischen Maschinenrichtlinie in der Praxis (Publicis Corporate Publishing, ISBN: 9783895783661)

6.2 Internet links

This list is by no means complete and only provides a selection of useful information.

Table 6-2

	Topic	Title
\1\	Reference to the document	http://support.automation.siemens.com/WW/view/en/45787668
\2\	Siemens I IA/DT Customer Support	http://support.automation.siemens.com
\3\	Safety Evaluation Tool	http://www.siemens.de/safety-evaluation-tool
\4\	Position switch 3SE5242-0QV40	Mall / Catalog: https://mall.automation.siemens.com/DE/guest/index.asp?aktPrim=0&nodeID=10036277&mlfb=3SE5242%2D0QV40&aktTab=4&lang=en Support: http://support.automation.siemens.com/WW/view/de/25206372 http://support.automation.siemens.com/WW/view/en/25206372
\6\	Safety Integrated	http://www.siemens.com/safety-integrated http://support.automation.siemens.com/WW/view/en/10807258/133300