


Auslegung und Bewertung von steuerungstechnischen Sicherheitsfunktionen




Praktische Auslegung gemäß den aktuellen harmonisierten Normen

Thomas Kramer-Wolf
Fachreferent Normen


the spirit of safety

► **CE Kennzeichnung
Gesetze**



Richtlinien (Gesetze) mit CE Kennzeichnung (Auszug)

Richtlinie	Kurztitel (nicht offiziell)	Gültigkeit
98/37/EG	(Alte) Maschinenrichtlinie	→12/2009
2006/42/EG	(Neue) Maschinenrichtlinie	12/2009 →
2001/95/EG	Produktsicherheitsrichtlinie	
2004/108/EG	EMV Richtlinie	
1999/5/EG	Funkanlagenrichtlinie	
2003/10/EG	Lärmrichtlinie	
2006/95/EG	Niederspannungsrichtlinie	
89/686/EWG	Richtlinie Persönliche Schutzausrüstungen	




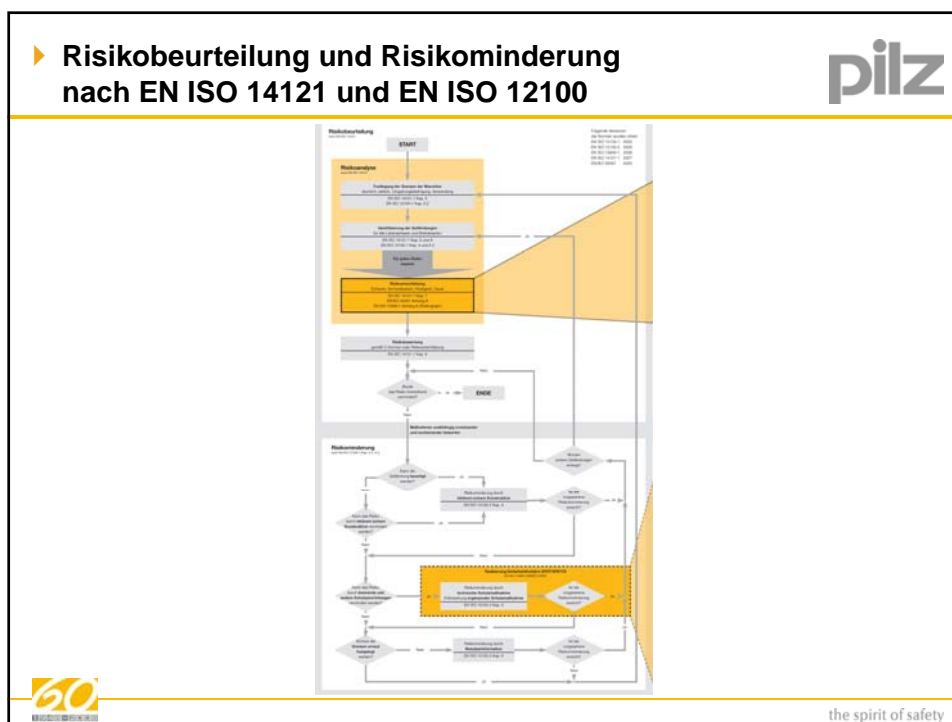
the spirit of safety

► **CE Kennzeichnung**
Normen zum Thema Laser und Sicherheit

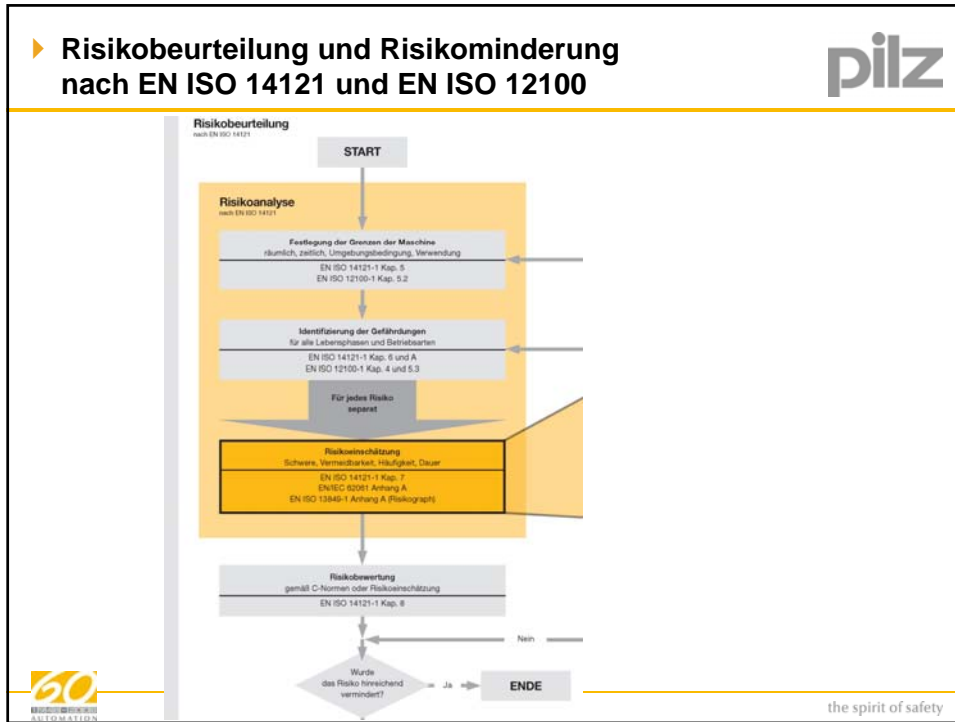
pilz

Nummer	Titel	Status	Datum
EN ISO 11553-1	SICHERHEIT VON MASCHINEN - LASERBEARBEITUNGSMASCHINEN - TEIL 1: ALLGEMEINE SICHERHEITANFORDERUNGEN	Harmounisiert	2008
EN 60825-1 & prEN 60825-4	SICHERHEIT VON LASER EINRICHTUNGEN - TEIL 1: KLASSIFIZIERUNG VON ANLAGEN, ANFORDERUNGEN UND BENUTZER-RICHTLINIEN & TEIL 4: LASERSCHUTZWAENDE	Harmounisiert	2008
EN 60204-1	SAFETY OF MACHINERY - ELECTRICAL EQUIPMENT OF MACHINES - PART 1: GENERAL REQUIREMENTS	Harmounisiert	2009
EN ISO 12100-1&2	SAFETY OF MACHINERY - BASIC CONCEPTS, GENERAL PRINCIPLES FOR DESIGN	Harmounisiert	2009
EN ISO 14121	SAFETY OF MACHINERY - PRINCIPLES OF RISK ASSESSMENT	Harmounisiert	2007

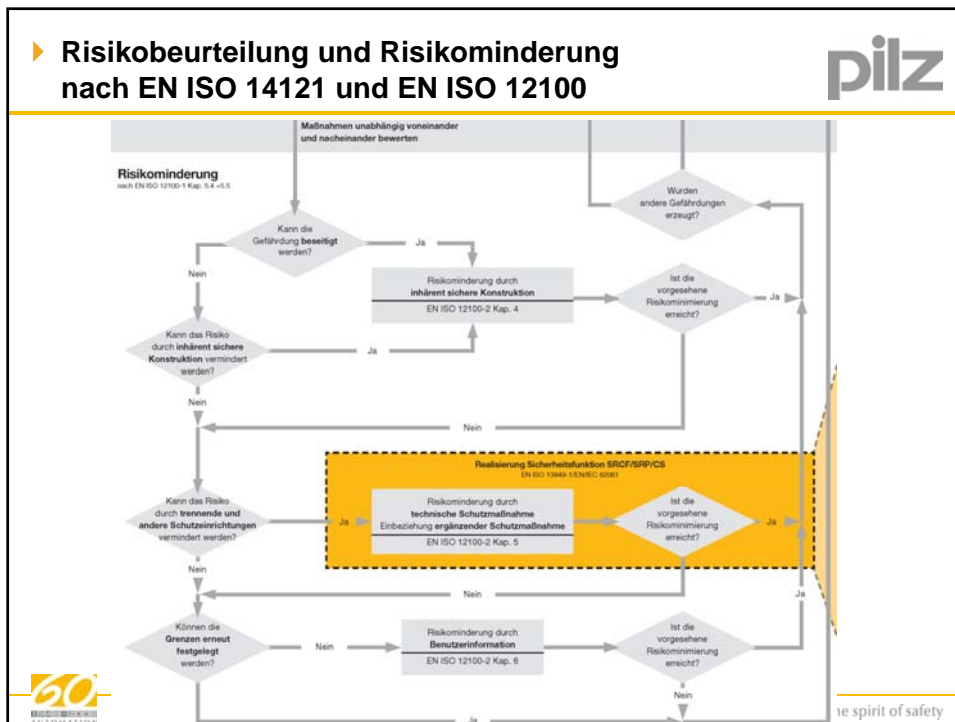

3
Vorname Name, Datum
Titel der Präsentation
the spirit of safety



► **Risikobeurteilung und Risikominderung nach EN ISO 14121 und EN ISO 12100**



► **Risikobeurteilung und Risikominderung nach EN ISO 14121 und EN ISO 12100**



Risiko Analyse
Grenzen der Maschine festlegen

pilz

- ▶ Zeitlich
- ▶ Räumlich
- ▶ Umgebungsparameter
- ▶ Einsatzzweck
- ▶ Nutzer/Anwender
- ▶ ...

60
ANIMATION

the spirit of safety

Risiko Analyse

pilz

Identifizieren der Gefährdungen

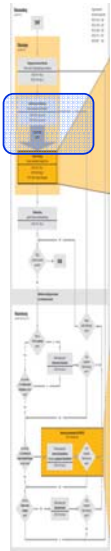
- ▶ Ort
- ▶ Zeitpunkt
- ▶ Art des Gefährdungen
 - Einfangen
 - Quetschen
 - Stoß
 - ...

60
ANIMATION

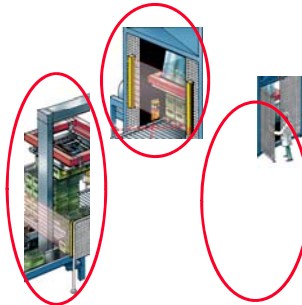
the spirit of safety

► **Risiko Analyse**
Gefährdungen nach EN ISO 12100-1

pilz



- ▶ Elektrische Gefährdung
- ▶ **Thermische** Gefährdung
- ▶ Gefährdung durch **Lärm**
- ▶ Gefährdungen durch **Schwingungen**
- ▶ Gefährdungen durch **Strahlung**
- ▶ Gefährdungen durch **Materialien und Substanzen**
- ▶ Gefährdungen durch Vernachlässigung **ergonomischer Grundsätze** bei der Konstruktion von Maschinen
- ▶ Gefährdungen durch **Ausrutschen, Stolpern und Stürzen**
- ▶ **Mechanische** Gefährdung
- ▶ Gefährdungskombinationen
- ▶ Gefährdungen in Zusammenhang mit der **Einsatzumgebung** der Maschine

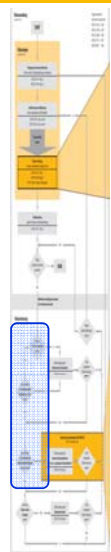


60
ANIMATION

the spirit of safety

► **Entscheidung der risikoreduzierenden Maßnahmen**


pilz



Verbale „Wenn - Dann“ Beschreibung der SRCF*

Beispiel:
Schutztüre zur Verhinderung des Zugangs

- ▶ **SRCF 1:** Wenn **Schutztüre geöffnet** wird, dann muss die Bewegung stillgesetzt werden
- ▶ **SRCF 2:** Wenn **Bewegung aktiv**, dann muss die Türe zugehalten sein
- ▶ **SRCF 3:** Wenn **Lichtgitter 1 unterbrochen**, dann muss die Bewegung stillgesetzt werden




* SRCF = Safety related control function = Sicherheitsfunktion

60
ANIMATION

the spirit of safety

► Bewerten aller Risiken und Sicherheitsfunktionen

pilz



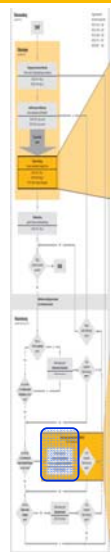
► Die Sicherheitsfunktionen der einzelnen Risiken



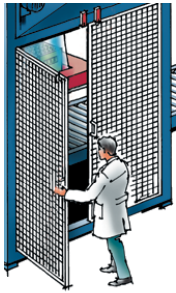
the spirit of safety

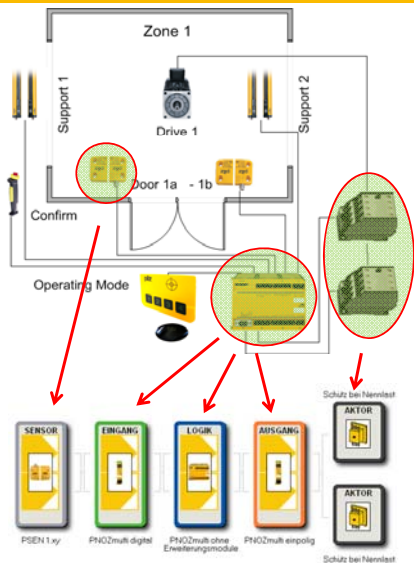
► SRCF 1a

pilz



Wenn **Schutztüre 1a** geöffnet wird, dann muss die Bewegung stillgesetzt werden





the spirit of safety

► SRCF 1b

pilz

Wenn **Schutztüre 1b** geöffnet wird, dann muss die Bewegung stillgesetzt werden

Zone 1

Support 1

Drive 1

Support 2

Door 1a - 1b

Confirm

Operating Mode

Schütz bei Nennlast

Schütz bei Nennlast

SENSOR PSEN 1-xy

EINGANG PHOZmult digital

LOGIK PHOZmult ohne Erweiterungsmodul

ABSGANG PHOZmult einpolig

AKTOR

AKTOR

60 INFORMATION

the spirit of safety

► SRCF 3

pilz

Wenn **Lichtgitter 1** unterbrochen wird, dann muss die Bewegung stillgesetzt werden

Zone 1

Support 1

Drive 1

Support 2

Door 1a - 1b

Confirm

Operating Mode

Schütz bei Nennlast

Schütz bei Nennlast

SENSOR PSEN ep-4E

EINGANG PHOZmult digital

LOGIK PHOZmult ohne Erweiterungsmodul

ABSGANG PHOZmult einpolig

AKTOR

AKTOR

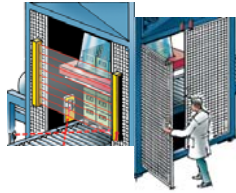
60 INFORMATION

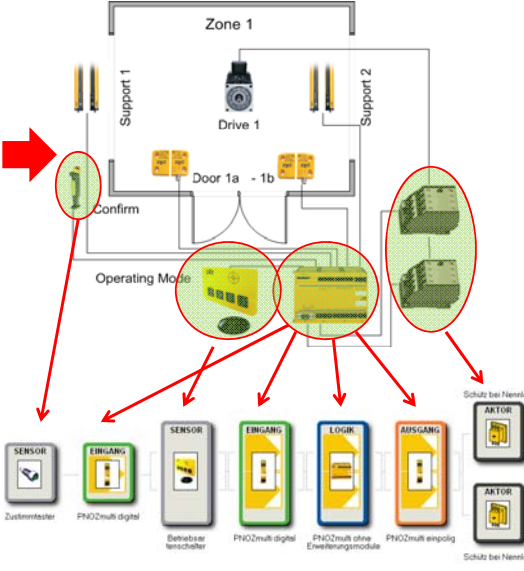
the spirit of safety

► SRCF 4

pilz

Wenn in **Betriebsart Freifahren** der **Confirm-Taster** betätigt ist, dann darf unabhängig vom Öffnungszustand der Türen und Lichtgitter die Bewegung im Tippbetrieb erfolgen





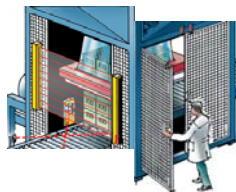
ZONE 1
 Support 1 Drive 1 Support 2
 Door 1a - 1b
 Confirm
 Operating Mode
 ZUSTIMMTASTER PNOZmulti digital BEWEISERLENSCHALTER PNOZmulti digital PNOZmulti ohne Erweiterungsmodul PNOZmulti empölig Schutz bei Herunterfahren AKTOR

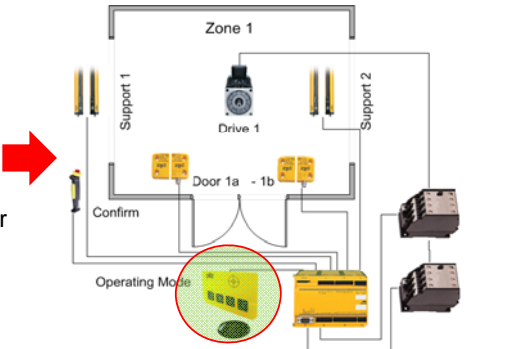
the spirit of safety

► Betriebsart - Anmerkung

pilz

Falls die gewählte Betriebsart für eine Sicherheitsfunktion unerheblich ist, z.B. weil sie unabhängig von der Betriebsart gilt, so kann auf die Einbindung des Betriebsartenwahlschalter in die entsprechende SRCF verzichtet werden.






the spirit of safety

Sicherheitsanforderungen SRCF 1 EN ISO 13849


pilz

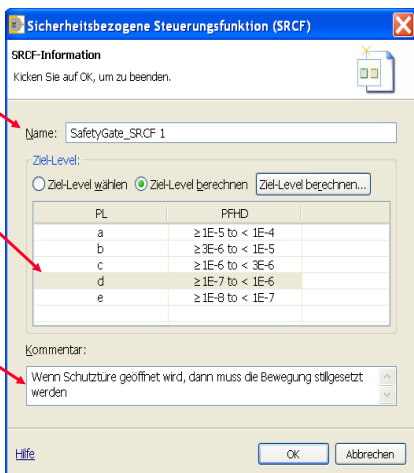


Benennen der Sicherheitsfunktion

Bestimmen des erforderlichen Sicherheitslevels der Sicherheitsfunktion

Beschreiben der Sicherheitsfunktion






the spirit of safety

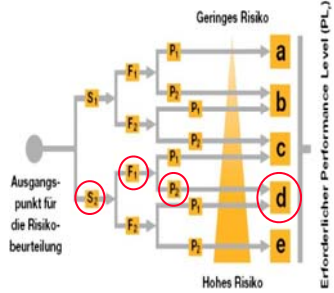

Sicherheitsanforderungen EN ISO 13849-1

pilz



Bestimmen des erforderlichen Performance Levels **PL**, anhand der Risiko Parameter:

- ▶ **S**_Schwere der Verletzung:
 - 1 = Leichte (üblicherweise reversibel)
 - 2 = Ernst (üblicherweise nicht reversibel, einschließlich Tod)
- ▶ **F**_Häufigkeit und/oder Dauer der Gefährdungsexposition
 - 1 = Selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz
 - 2 = Häufig bis dauernd und/oder die Zeit der Gefährdungsexposition ist lang
- ▶ **P**_Möglichkeit der Vermeidung der Gefährdung oder Begrenzung des Schadens
 - 1 = Möglich unter bestimmten Bedingungen
 - 2 = Kaum möglich

the spirit of safety

Design Sicherheitsfunktion **pilz**

- ▶ Design der Sicherheitsfunktion
- ▶ Auswahl der Sicherheitskomponenten
- ▶ Bestimmen
 - Nutzungsverhalten von verschleißbehafteten Komponenten
 - Sicherheitsparameter der Geräte
 - Diagnose Deckungsgrad der Komponenten



PSEN 1.xy



PNOZ s4




Contactor nominal load
ACTUATOR
ACTUATOR
Contactor nominal load




the spirit of safety

Design Sicherheitsfunktion **pilz**




System-Modul	Erforderlicher PL	Ergebnis	COF-Faktor	PFHD	Erreichte PL
SafetyGate_Pld	4	Ziel erreicht	1,29E-07	0	
SafetyGate_Fle	4	Ziel erreicht	5,17E-08	0	



the spirit of safety

Design Sicherheitsfunktion
Bestimmen des Nutzverhaltens

pilz

Bestimmen von

- ▶ Struktur/Verdrahtung
- ▶ Schalthäufigkeit
- ▶ Diagnosedeckungsgrad

Komponente konfigurieren (PSEN Lay)
 Klicken Sie auf OK, um zu beenden.

Interne Architektur
 Einkanalig (1001) Zweikanalig (1002)

Anzahl der Betriebszyklen
 Betriebstage pro Jahr: 365
 Betriebsstunden pro Tag: 24
 Zeit zwischen zwei Betätigungen Betätigungen pro Zeiteinheit
 0,50 Stunde(n) 2,00 pro Stunde

Konfiguration der Verdrahtung
 Keine Fehlerausschluss Querschlusserkennung

Diagnosedeckungsgrad
 Plausibilitätsprüfung : [0,00% - 99,00%]: 99,00
 Anforderungsrate $\leq 1/100$ Testrate (Kategorie 2) MTTF d,TE $> 0,5 * MTTF d,L$

Hilfe OK Abbrechen

the spirit of safety

Design Sicherheitsfunktion
Bestimmen des Nutzverhaltens

pilz

Komponente konfigurieren (PSEN me2)
 Klicken Sie auf OK, um zu beenden.

Interne Architektur
 Einkanalig (1001) Zweikanalig (1002)

Anzahl der Betriebszyklen
 Betriebstage pro Jahr: 365
 Betriebsstunden pro Tag: 24
 Zeit zwischen zwei Betätigungen Betätigungen pro Zeiteinheit
 0,50 Stunde(n) 2,00 pro Stunde

Konfiguration der Verdrahtung
 Keine Fehlerausschluss Querschlusserkennung

Diagnosedeckungsgrad
 Plausibilitätsprüfung : [0,00% - 99,00%]: 99,00
 Anforderungsrate $\leq 1/100$ Testrate (Kategorie 2) MTTF d,TE $> 0,5 * MTTF d,L$

Hilfe OK Abbrechen

the spirit of safety

Bestimmen des CCF

Bestimmen und Dokumentieren der CCF Parameter

The screenshot shows the CCF Editor interface. On the left, a tree view shows the project structure. The main window displays the results for EN/IEC 62061 and EN ISO 13849-1. The EN/IEC 62061 results show a CCF-Faktor of 0,19 and a score of 0/100. The EN ISO 13849-1 results show a score of 100/100. The interface includes a list of requirements with checkboxes and scores.

CCF Editor EN/IEC 62061

Ergebnisse

CCF-Faktor: 0,19

EN ISO 13849-1

Results: 100/100

CCF Score: 05 or better - Meets the requirements

EN/IEC 62061 0/100

0/20

1a Sind SRECS-Signalkabel für die einzelnen Kanäle getrennt von anderen Kanälen geführt oder ausreichend geschützt?

1b Ist die Erkennung von Signalübertragungsfehlern bei Verwendung von Informationscodierung/decodierung ausreichend?

2 Sind SRECS-Signalkabel und elektrische Energieversorgungsleiter an allen Stellen getrennt oder ausreichend geschützt?

3 Werden Teilsystem-Elemente als physikalisch getrennte Einheiten in eigenen lokalen Gehäusen vorgesehen, wenn sie zu einem CCF beitragen können?

0/38

4 Werden in dem Teilsystem verschiedene elektronische Technologien verwendet, zum Beispiel einmalige Elektronik oder programmierbare Elektronik und andersseits ein elektronisches Relais?

5 Werden in dem Teilsystem Elemente verwendet, die verschiedene physikalische Prinzipien nutzen (z. B. Erfassungselemente an einer Schutzvorrichtung, die mechanische oder magnetische Erfassungsverfahren verwenden)?

6 Werden in dem Teilsystem Elemente mit unterschiedlichem Zeitverhalten in Bezug auf funktionalen Betrieb und/oder Ausfallarten verwendet?

7 Haben die Teilsystem-Elemente ein Diagnose-Testintervall von ≤ 1 min?

the spirit of safety

Validierung

Übersicht der Teilergebnisse

Prüfen des Ergebnisses

The screenshot shows the SRPF Editor interface. A table displays the validation results for SafetyGate_SRCF1. The table has columns for PL, PFD, Cat., DCavg, MTTFd: begrenzt, MTTFd: sym., MTTFd/Ch1, MTTFd/Ch2, and DC. The results show a CCF-Faktor of 0,19 and a PFD of 5,17E-08. A red circle highlights the PFD value, and a red arrow points to it with the text 'Prüfen des Ergebnisses'. The interface also includes a tree view on the left and a status bar at the bottom.

SafetyGate_Pld - 13849_SafetyGatePNOZ_X

SafetyGate_Plc - 13849_SafetyGatePNOZmulti

SafetyGate_SRCF1 - Verpackungsmaschine

Teilsystem/Kanal	Anteil am PL	PL	PFD	Cat.	DCavg	MTTFd: begrenzt	MTTFd: sym.	MTTFd/Ch1	MTTFd/Ch2	DC
SafetyGate_SRCF1		5,17E-08	2,47E-08	+	99,00%	100,00Jahre	205,39Jahre	205,39Jahre	205,39Jahre	99,00%
Teilsystem										
PSN 1.xy										99,00%
PSN 1.xy										99,00%
PNOZ XS			2,31E-09							
Teilsystem										99,00%
Schutz bei Nennlast			2,47E-08	+	99,00%	100,00Jahre	1141,55Jahre	1141,55Jahre	1141,55Jahre	99,00%
Schutz bei Nennlast										99,00%

SRPF-Ergebnis: Wartezeit-Ergebnisse

System/Modul	Erforderlicher PL	Ergebnis	CCF-Faktor	PFD	Erreichter PL
SafetyGate_SRCF1	0	Ziel erreicht	Ziel erreicht	5,17E-08	0

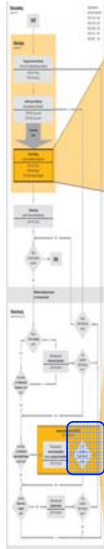
EN ISO 13849-1

the spirit of safety

► Validierung



Erzeugen des Reports (PDF)



Projekt-Details

Projektnummer: 110941_SafetyControl_V2_1
Sicherheitsnormen: EN ISO 13045 (PL)
Autor: PLC
Version: 1.0
Erstellungsdatum: 26. März 2007 15:16:35
Letzte Änderung: 15. Januar 2008 09:31:33

SRCF-Übersicht

Systemteil	Minimale PL	Ergebn	SRCF-Punkt	Weg	Minimale PL
Systemteil_1	2	OK	1	1/10	2
Systemteil_2	2	OK	2	2/10	2

ES ERWÄHNTE SICH BERECHNUNG DIE NUR DANN GILT, WENN AUCH DIE FOLGENDEN ANFORDERUNGEN ERFÜLLT WERDEN:

Nr.	Frage	Antwort
1	Benutzerspezifische Vorgehensweise wurde verwendet	
2	Benutzerspezifische Vorgehensweise wurde verwendet	
3	Benutzerspezifische Vorgehensweise wurde verwendet	
4	Benutzerspezifische Vorgehensweise wurde verwendet	
5	Benutzerspezifische Vorgehensweise wurde verwendet	
6	Benutzerspezifische Vorgehensweise wurde verwendet	
7	Benutzerspezifische Vorgehensweise wurde verwendet	
8	Benutzerspezifische Vorgehensweise wurde verwendet	
9	Benutzerspezifische Vorgehensweise wurde verwendet	
10	Benutzerspezifische Vorgehensweise wurde verwendet	



the spirit of safety