Neuerungen bei Normen

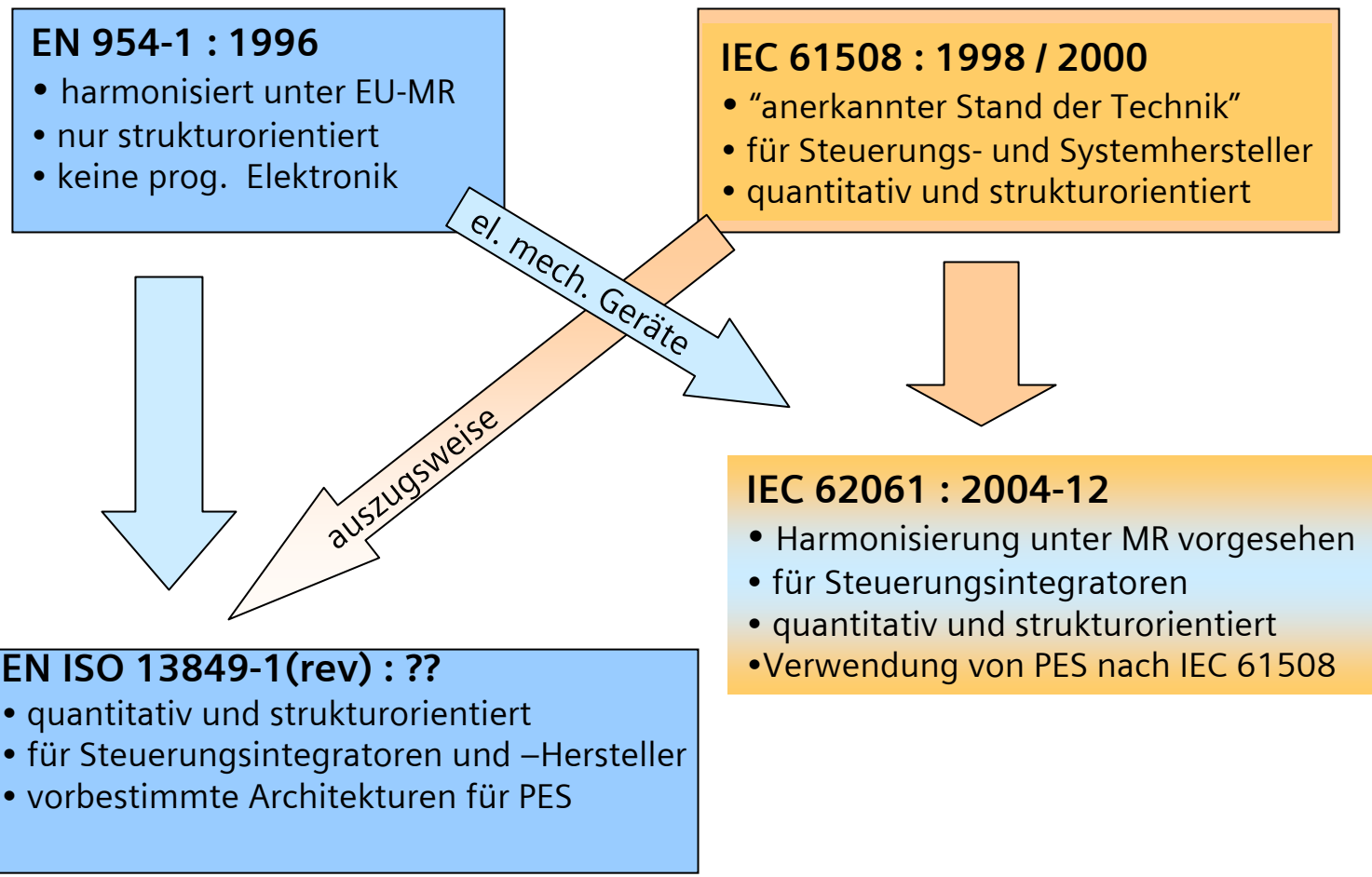
EN 954 / ISO 13849 und IEC 62061

SIEMENS

Inhalt

- Basisnormen für sicherheitsrelevante Maschinensteuerungen heutiger Stand
- Gründe für Neuerungen
- Lösungsansatz
- Neue Systematik
- Konzept IEC 62061
- Konzept ISO 13849-1(rev)
- Resümee

Weiterentwicklung der Basisnormen



Basisnormen, bisheriger Stand

- EN 954-1 : 1996 (int. ISO 13849-1)
  - ist harmonisiert unter der MR → Vermutungswirkung für CE
  - Konzept für Elektromechanik, Hydraulik etc
  - Ist für komplexe Elektronik nicht ausreichend
  - Erst Teil 2 (ISO 13849-2) von 2003 verweist auf IEC 61508
- Technische Entwicklung ist weiter gegangen
  - Methoden zur Ertüchtigung von Elektronik für Sicherheitsaufgaben wurden entwickelt.
- IEC 61508 (EN 61508)
  - Definiert Anforderungen zur Ertüchtigung von Elektronik für Sicherheitsaufgaben
  - Ist nicht unter der Maschinenrichtlinie harmonisiert
  - Beschreibt den "Stand der Technik"

derzeit geforderte Produkteigenschaften

... für funktionale Sicherheit

- **EN 60204-1:1997**
  - Verlangt (im Prinzip) Erfüllung von EN 954
  - Erlaubt programmierbare Elektronik und Busverbindungen nur wenn IEC 61508 erfüllt ist (über Vorwort)
- **EN 954**
  - Verlangt (durch Verweis in 13849-2)Anwendung von IEC 61508 für programmierbare Elektronik und Busverbindungen
- **NFPA 79 : 2002**
  - Verlangt Listung gemäß IEC 61508 für programmierbare Elektronik und Busverbindungen

Sicherheitstechnik entwickelt sich weiter

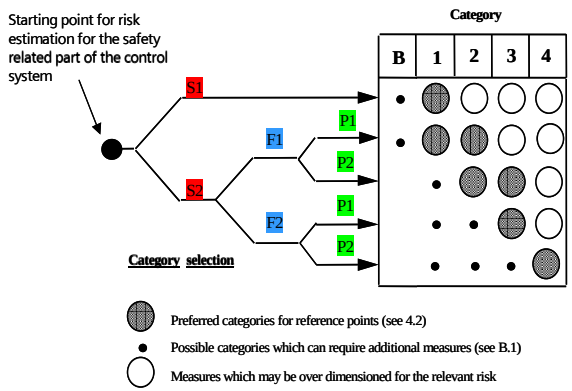
- Elektronik zieht auch bei der Sicherheitstechnik ein
  - S7-400F / 300F
  - Sinumerik Safety integrated
  - PROFIsafe
  - ASIsafe
  - 3TK28-Elektronik
- Neue Systematik
  - ermöglicht neue Sicherheitskonzepte
  - deckt Schwachstellen der bisherigen Regelungen auf

➔Neue Normen werden entwickelt

➔Bestehende Normen werden weiterentwickelt

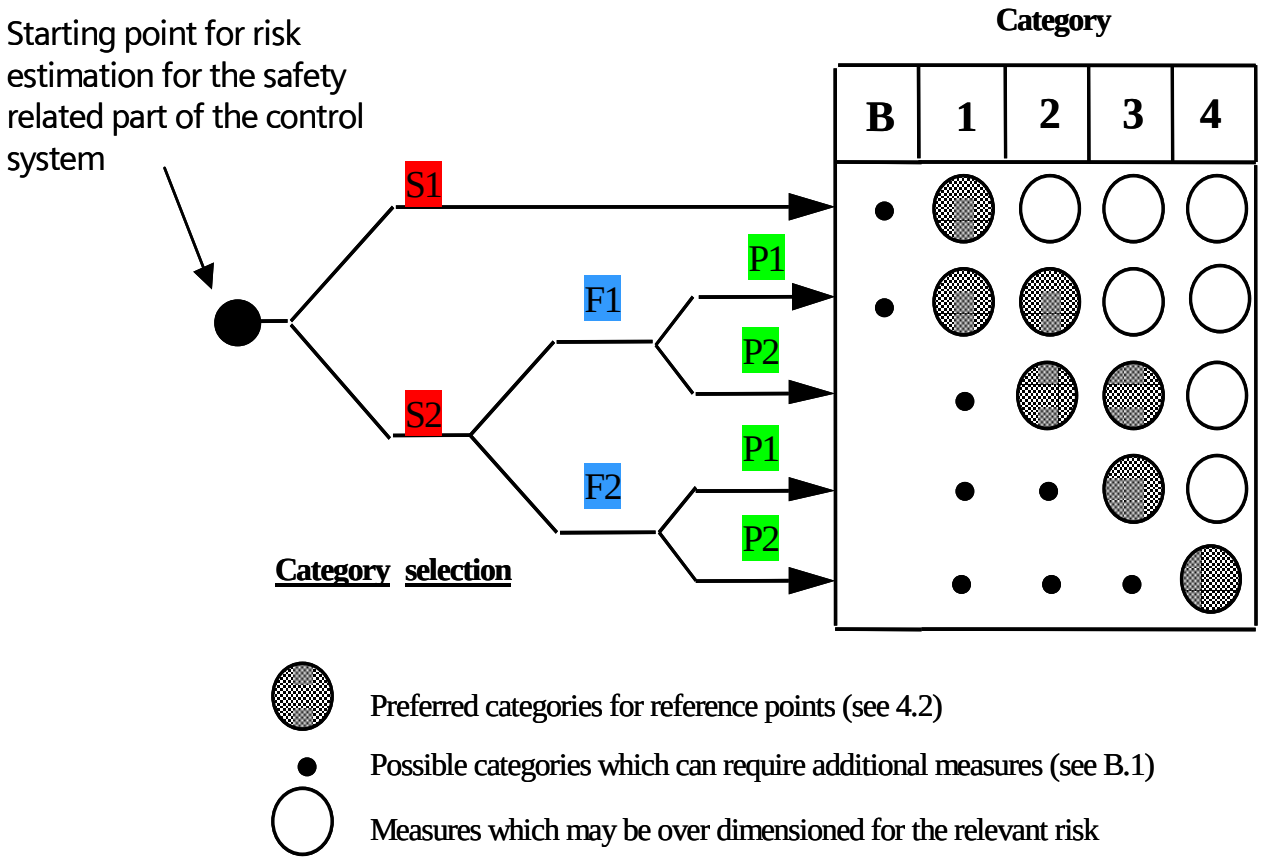
Probleme der bisherigen Situation

- Verwendung elektronischer Systeme für Sicherheitsfunktionen ist durch EN 954 nicht abgedeckt.
  - ➔Stand der Technik ist nicht ausreichend repräsentiert
- Die Kategorien nach EN 954 „sind nicht hierarchisch“
  - Kategorien beschreiben Lösungsstrukturen
  - Die praktizierte Abstufung der zugeordneten Safety Performance ist durch die Norm nicht definiert
- Die Kriterien zur Festlegung einer geforderter Kategorien sind nicht eindeutig
  - → Risikograph



Neuerungen bei Normen

Probleme der bisherigen Situation: Risikograph nach EN 954-1



Probleme der bisherigen Situation

- Verwendung elektronischer Systeme für Sicherheitsfunktionen ist durch EN 954 nicht abgedeckt.
  - ➔Stand der Technik ist nicht ausreichend repräsentiert
- Die Kategorien nach EN 954 „sind nicht hierarchisch“
  - Kategorien beschreiben Lösungsstrukturen
  - Die praktizierte Abstufung der zugeordneten Safety Performance ist durch die Norm nicht definiert
- Die Kriterien zur Festlegung einer geforderter Kategorien sind nicht eindeutig

➔Die Festlegung einer bestimmten Lösung ist (oft) abhängig von der Interpretation durch eine Prüfstelle.

➔Für die gleiche Anwendung können unterschiedliche Lösungen gefordert werden, wenn verschiedene Prüfstellen zuständig sind

technische Schwachpunkte

- EN 954 hat keinen definierten Bezug zu Sicherheitsfunktionen
  - Kategorien stellen Anforderungen an „sicherheitsrelevante Teile von Steuerungen“
  - Der Zusammenhang zur notwendigen „Safety Performance“ für eine Sicherheitsfunktion ist nicht definiert.
  - Die Komplexität von Sicherheitsfunktionen bleibt unberücksichtigt
- Abstufung der Kategorien von EN 954 bezieht sich auf Hardwarestrukturen
- Ausfallraten und Lebensdauer der verwendeten Komponenten werden nicht explizit betrachtet

➔Quantitative Aussagen zur Zuverlässigkeit bestimmter Sicherheitsfunktionen sind nicht möglich.

➔Systematische Abstufung der Safety Performance ist nicht möglich

“Kategorien sind nicht hierarchisch”

... das ist die offizielle Aussage von EN 954-1

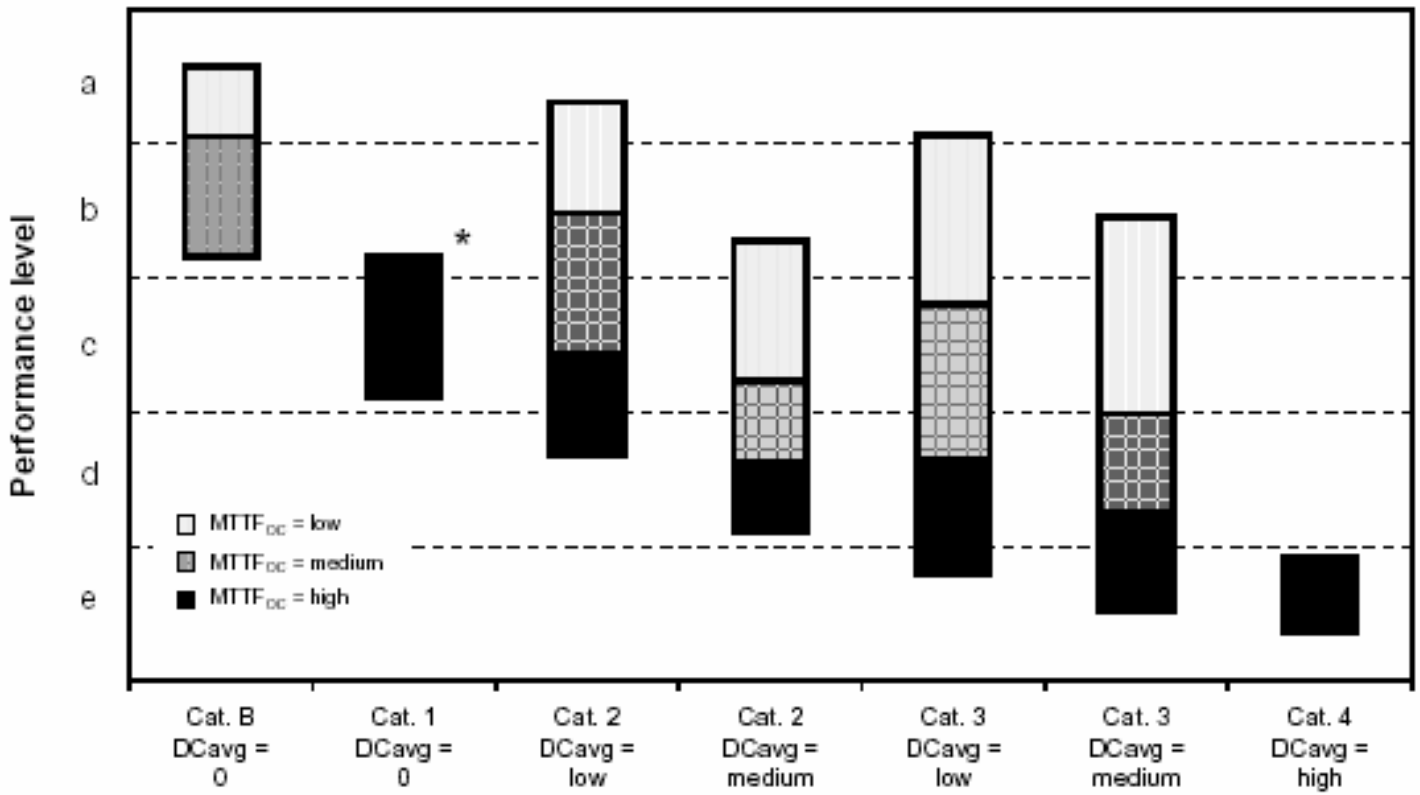


Bild aus draft ISO 13849-1(rev)

Lösung: IEC 62061 und Revision der EN 954-1

- Es wird ein quantitatives Maß für die Safety Performance eingeführt
  - IEC 62061: Safety Integrity Level (SIL)
  - ISO 13849-1(rev): Performance Level (PL)
- IEC 62061 und ISO 13849-1(revision) betrachten Sicherheitsfunktionen
  - einer bestimmten Gefährdungen (durch die Maschine) kann eine definierte Sicherheitsfunktion zugeordnet werden
  - Für eine definierte Sicherheitsfunktion kann die erforderliche Safety Performance bestimmt werden
- Mit dem SIL (IEC 62061) und dem PL (ISO 13849-1(rev)) wird eine eindeutige, hierarchisch abgestufte Bemessungsgröße für die Safety Performance (sicherheitsbezogene Leistungsfähigkeit) definiert.

Maß der Safety Performance

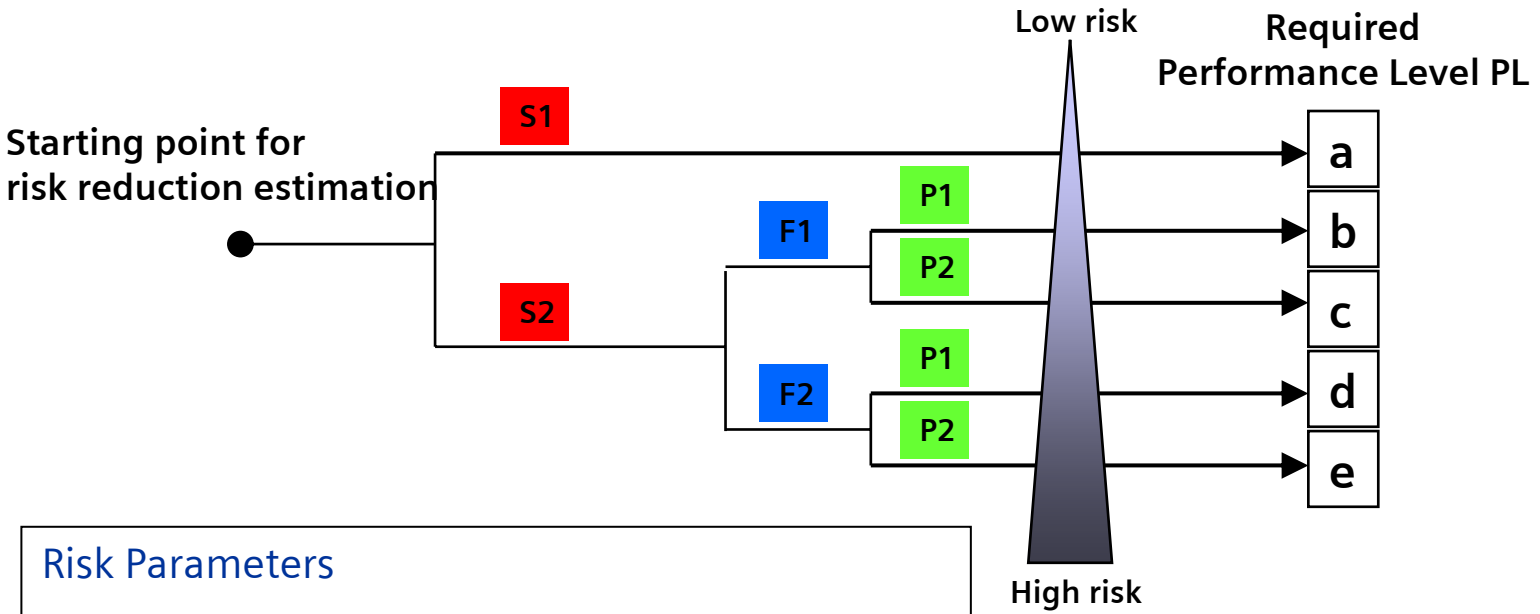
.. geforderte Safety Performance ist risikoabhängig

- **bisher: Kategorie**
  - **Lösungsabhängig**
  - **Kein eindeutiger Bezug zur Höhe des Risikos**
- **zukünftig: SIL** (Safety Integrity level) **/ PL** (Performance Level)
  - **Lösungsunabhängig**
  - **Eindeutige Abstufung nach Höhe des Risikos**

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]	SIL [EN 61508-1 (IEC 61508-1)] for information
a	$\geq 10^{-5}$ to $< 10^{-4}$	no special safety requirements
b	$\geq 3 \bullet 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \bullet 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

➔ **SIL und PL_r sind aufeinander abbildbar**

Risk evaluation (II)
Risk graph draft ISO 13849-1 (revision)



Risk Parameters

S = **Severity of injury**

F = **Frequency and/or exposure time to the hazard**

P= **Possibility of avoiding the hazard or limiting the harm**

a,b,c,d,e = **Estimates of safety-related Performance Level**

Risk evaluation (III)
SIL assignment in draft IEC 62061, annex A

Risk related to the identified hazard = Severity of the possible harm SE and Frequency and duration of exposure FD; Human and machine behavior HM; Possibility to avoid harm AV — Probability of occurrence

FIGURE A.2: Risk estimation and SIL assignment

First iteration
Further iteration(s)

Shaded area = action required

Consequences	Severity SE	CL 3-4	CL 5 - 7	CL 8 - 10	CL 11 - 13	CL 14-15
Death, loosing an eye or arm	4	SIL 1	SIL 1	SIL 2	SIL 3	SIL 3
Permanent, loosing fingers	3		(B) OM	SIL 1	SIL 2	SIL 2
Reversible, medical attention	2			(B) OM	SIL 1	SIL 2
Reversible, first aid	1				(B) OM	SIL 1

Frequency and Duration, FD	D≤ 10 min	D> 10 min
≤10min	5	-
>10m-≤hour	4	5
>hour-≤day	3	4
>day-≤2wks	2	3
>2wks	1	2

Probability Ma and Hu, HM	Human behaviour	Machine behaviour NP	Machine behaviour FP	Machine behaviour VP
S+LA		6	4	3
S+A		5	3	2
NS+LA		5	3	2
NS+A		4	2	1

Avoidance AV	
Impossible	4
Rarely	2
Possible	1

Ser. No.	Hazard	SE	FD	HM	AV	CL	Risk reduction
1	Example	3	2	3	4	9	Would give a SIL 1 requirement (Safety measures)
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							

Neuerungen bei Normen

Risk evaluation (III)
SIL assignment in draft IEC 62061, annex A

Risk related to the identified hazard = Severity of the possible harm SE and Frequency and duration of exposure FD; Human and machine behavior HM; Possibility to avoid harm AV } Probability of occurrence

Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd. event, Pr		Avoidance Av	
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Abgrenzung der Anwendung von 62061 - 13849

IEC 62061

- ist für alle elektrischen und elektronischen System beliebiger Architekturen anwendbar.
  - SIL 1 bis 3
- programmierbare Steuerungen (SPS etc) müssen IEC 61508 erfüllen

ISO 13849-1(revision)

- ist für hydraulische, pneumatische und elektromechanische Systeme ohne Einschränkungen anwendbar.
- ist bei programmierbaren elektronischen Systemen nur unter Einschränkungen anwendbar
  - bestimmte Architektur
  - bis PL d bzw SIL 2
- das Berechnungskonzept von ISO 13849-1(rev) basiert auf vorgegebenen Architekturen der Verarbeitungseinheit
- die Anforderungen von DIS ISO 13849-1(rev) für elektronische (Sub-) Systeme sind bisher nicht ausreichend.

Abgrenzung der Anwendung von 62061 – 13849

	Technology implementing the safety-related control function(s)	ISO 13849-1: 1999	ISO 13849-1(under revision)	IEC 62061
A	Non electrical, e.g. hydraulics	X	X	Not covered
B	Electromechanical, e.g. relays, or non complex electronics	X	Restricted to designated architectures (see Note 1) and up to PL=e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	X	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
D	A combined with B	X	Restricted to designated architectures (see Note 1) and up to PL=e	X see Note 3
E	C combined with B	X	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X	X see Note 2	X see Note 3

"X" indicates that this item is dealt with by this standard.

NOTE 1 Designated architectures are defined in Annex B of EN ISO 13849-1(rev.) to give a simplified approach for quantification of performance level.

NOTE 2 For complex electronics: Use of designated architectures according to EN ISO 13849-1(rev.) up to PL=d or any architecture according to IEC 62061.

NOTE 3 For non-electrical technology use parts according to EN ISO 13849-1(rev.) as subsystems.

Neuerungen bei Normen

Neue Systematik für Steuerungsentwurf

Unterschiedliche Konzepte in IEC 62061 und draft ISO13849-1(rev)

SIEMENS

Anforderungen ergeben sich aus der Risikoanalyse

- Risikoanalyse ist Gegenstand von EN ISO 12100 (früher EN 292) und EN 1050 (→ ISO 14121)
- Risikoanalyse ergibt
  - →notwendige Sicherheitsfunktionen für die betrachtete Maschine
  - →Erforderliche Safety Performance (SIL oder PL) für jede Sicherheitsfunktion
- Methoden zur Bestimmung der erforderlichen Safety Performance sind beschrieben in
  - IEC 62061 → SIL assignment process (Excel Tabelle)
  - Draft ISO 13849-1 → Risikograph

Inhalt der (System) Safety Requirements Specification

Beschreibung der Funktion

- Logik
- Zeitverhalten (Reaktionszeit, ...)
- ...

Inputs

- Eingangsinformation
- Schalthäufigkeit
- Vorgaben für Geräte (z.B. zu verwendende Geräte Typen)

Outputs

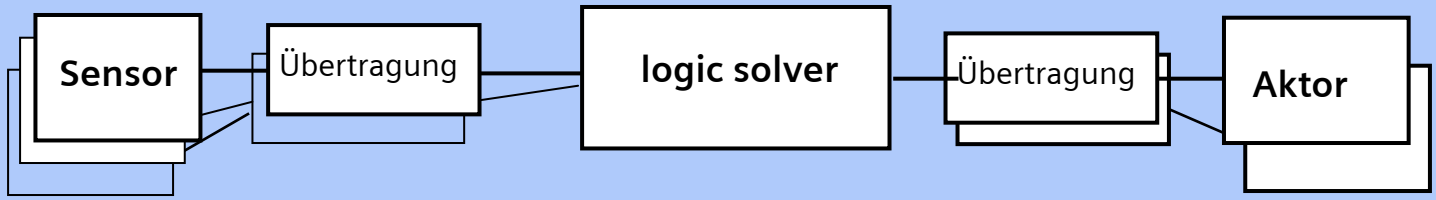
- Ausgangsinformation / Aktionen
- Schalthäufigkeit
- Vorgaben für Geräte (z.B. zu verwendende Geräte Typen)

Geforderte Safety Performance für die Funktion

- SIL oder PL (evtl. Kategorie)

Umgebungsbedingungen etc

Sicherheitsfunktion, System



Vollständige Funktion:

Informationen erfassen ⇨ Informationen auswerten ⇨ Aktionen ausführen

Safety Performanance einer Sicherheitsfunktion:

IEC 62061 (ebenso wie IEC 61508, IEC 61511):

➔ **Safety Integrity Level (SIL)**

draft ISO 13849-1(rev):

➔ **Performance Level (PL)**

SIL und PL sind ein probabilistisches Maß:

Average probability of a dangerous failure per hour

Was ist anders bei EN 954:

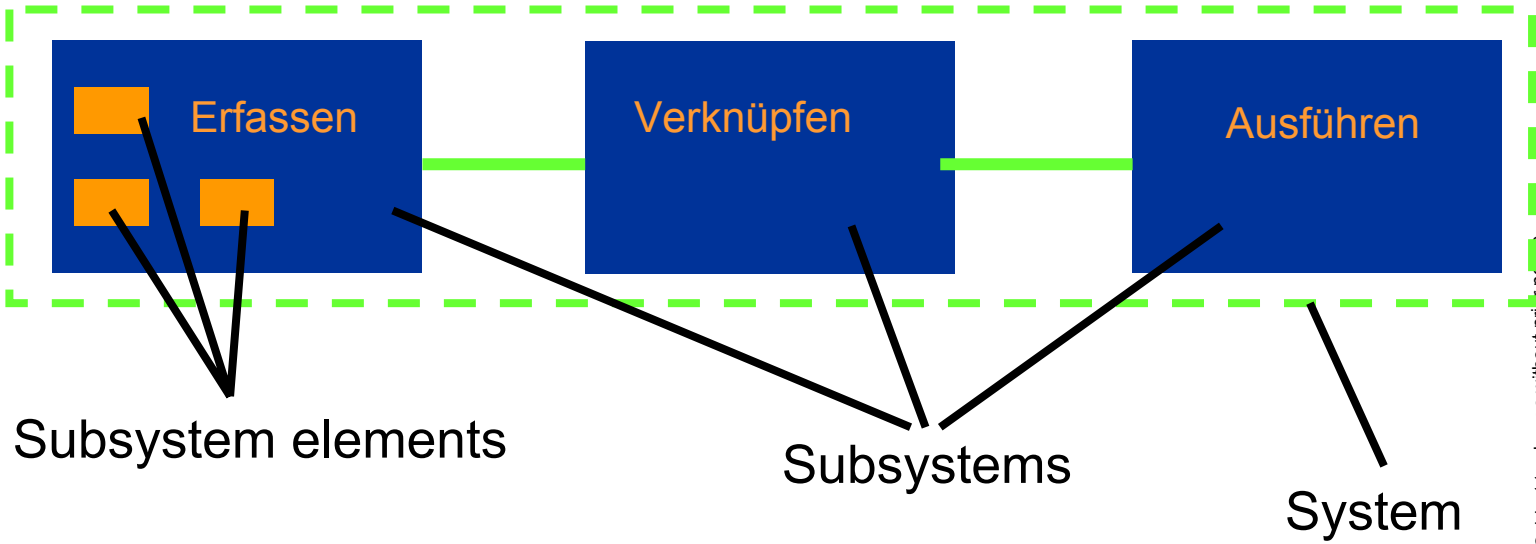
- **Ist nicht funktionsbezogen**
- **Kategorien beziehen sich auf die Teile des Systems**

Konzept IEC 62061

IEC 62061 beschreibt den
“anerkannten Stand der Technik”

Strukturierungselemente der Systemarchitektur

- Eine “Sicherheitsfunktion” wird von einem “System” ausgeführt.
- Ein “System” ist zusammengesetzt aus “Subsystemen”.
- Ein “Subsystem” besteht aus “Subsystemelementen”



Zielsetzung der IEC 62061

IEC 62061 klärt die Frage …

- **Wie kann man aus einzelnen F-Geräten ein Steuerungssystem aufbauen, das die Sicherheitsanforderungen für die vorgesehene Anwendung erfüllt ?**

  Welche Anforderungen müssen die einzelnen Geräte erfüllen?

  Wie können Geräte kombiniert werden, um die notwendige Safety Performance zu erreichen?

  ….

Anwendungsbeispiel IEC 62061 (1)

Ausgangspunkt: Es wird eine spezifische Sicherheits-funktion betrachtet

Schutzmaßnahme:
Bei offener Schutztür darf die Maschine nicht laufen.

Sicherheitsfunktion:
Schutztürverriegelung
(mit den Eigenschaften SIL bzw. Sicherheitskategorie)

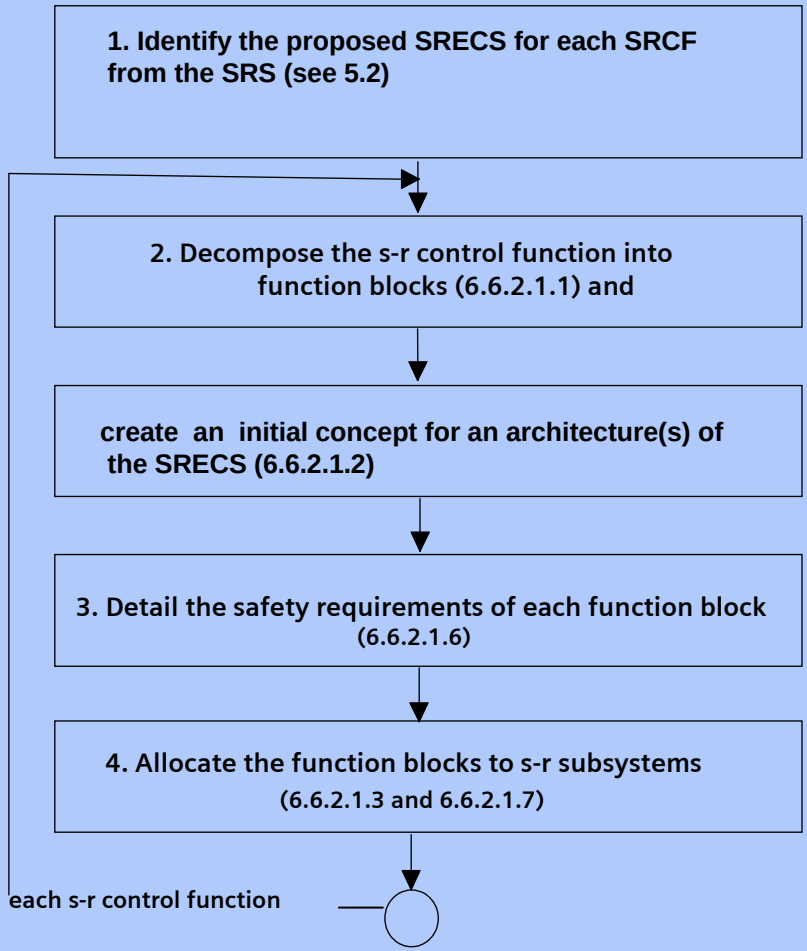
Beschreibung der Sicherheitsfunktion:
“Wenn die Schutztür geöffnet wird, Motor ausschalten. ....

SIL = Safety **I**ntegrity **L**evel

Anwendungsbeispiel IEC 62061 (2)

- **Start design from specified safety function**
- Safety function
  - "Checking position of protective doors and stop machine when door is opened"
- Decompose safety function to Function blocks
  1) Sense door position
  2) Evaluate door position with requirements of operating mode, initiate switching
  3) Execute switching
- **F = F1 + F2 + F3**

Draft IEC 62061:
SRECS design process



SRECS = safety-related electrical control system

Anwendungsbeispiel IEC 62061 (3)

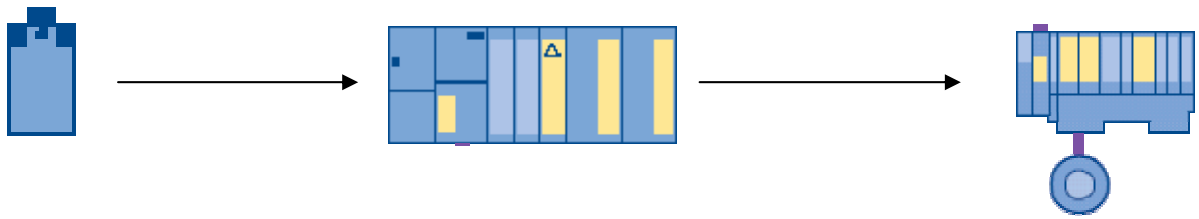
Decomposed safety function

Sense
door position + Evaluate door position ... + Execute switching

Safety requirements

Safety integrity: SIL 2
Switch off in case of failure

Create architecture



Specify safety requirements for subsystems

Sensor
- position switch
- SIL claim >= 2

PLC
- logic as specified
- SIL claim >= 2

Actuator
- motor control switch
- SIL claim >= 2

PFH_D (F1 + F2 + F3) < 10^{-6} / h

PFH_D = Wahrscheinlichkeit für einen gefährlichen Ausfall der Sicherheitsfunktion innerhalb 1 Stunde

Neuerungen bei Normen

SIEMENS

Struktur einer Sicherheitsfunktion (1)

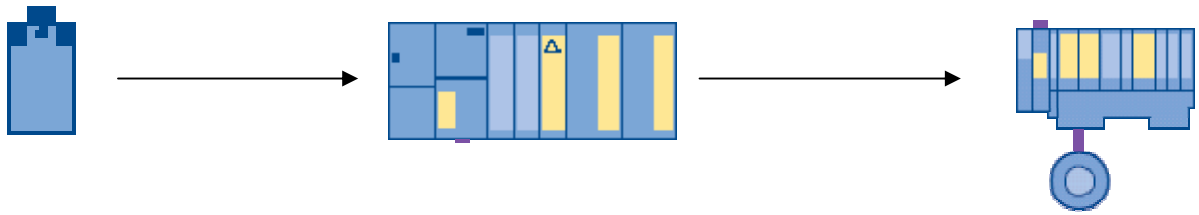
Safety requirements

Funktion: Switch off if door is open, Switch off in case of failure
Safety performance: SIL 2

Decomposed safety function

Sense door position + Evaluate door position + Execute switching

Create architecture



Specify safety requirements for subsystems

Sensor
- position switch
- SIL claim >= 2

PLC
- logic as specified
- SIL claim >= 2

Actuator
- motor control switch
- SIL claim >= 2

PFH_D (F1 + F2 + F3) < 10^{-6} / h

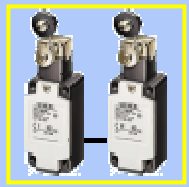
PFH_D = Wahrscheinlichkeit für einen gefährlichen Ausfall der Sicherheitsfunktion innerhalb 1 Stunde

Neuerungen bei Normen

SIEMENS

Systemstruktur (1a)

Architecture assigned to one function



→ 3TK → Schütze

Safety integrity information of subsystems

Sensor
- SIL claim limit: 2
- $PFH_{D1} = 2*10^{-7}$ / h

PLC
- SIL claim limit: 3
- $PFH_{D2} = 1*10^{-7}$ / h

Actuator
- SIL claim limit: 2
- $PFH_{D3} = 3*10^{-7}$ / h

SIL-Eignung

$SIL\ CL_{SYS} <= (SIL\ CL_{subsystem})_{lowest}$ → SIL claim limit: 2

Random integrity

$PFH_D = PFH_{D1} + ... + PFH_{Dn} + P_{TE}$ → $PFH_D = (2 + 1 + 3)*10^{-7} < 10^{-6}$

System erreicht: SIL 2

P_{TE} = Wahrscheinlichkeit eines unerkannten Fehlers in der Kommunikation

Neuerungen bei Normen

SIEMENS

Systemstruktur (1b)

Systemarchitektur für eine Funktion

Safety integrity information of subsystems

Sensor
- SIL claim limit: 2
- $PFH_{D1} = 2*10^{-7}$ / h

PLC
- SIL claim limit: 3
- $PFH_{D2} = 1*10^{-7}$ / h

Actuator
- SIL claim limit: 2
- $PFH_{D3} = 3*10^{-7}$ / h

SIL-Eignung

$SIL\ CL_{SYS} <= (SIL\ CL_{subsystem})_{lowest}$ → SIL claim limit: 2

Random integrity

$PFH_D = PFH_{D1} + ... + PFH_{Dn} + P_{TE}$ → $PFH_D = (2 + 1 + 3)*10^{-7} < 10^{-6}$

System erreicht: SIL 2

P_{TE} = Wahrscheinlichkeit eines unerkannten Fehlers in der Kommunikation

SIEMENS

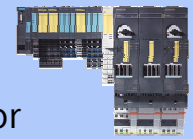
Systemstruktur, Beispiel 2

Systemarchitektur für eine andere Funktion

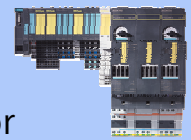
Sensor
- SIL claim limit: 2
- PFH_{D1} = $2*10^{-7}$ / h

Sensor
- SIL claim limit: 2
- PFH_{D2} = $0.5*10^{-7}$ / h

PLC
- SIL claim limit: 3
- PFH_{D3} = $1*10^{-7}$ / h



Actuator
- SIL claim limit: 2
- PFH_{D4} = $3*10^{-7}$ / h



Actuator
- SIL claim limit: 2
- PFH_{D5} = $3*10^{-7}$ / h

SIL-Eignung

$SIL\ CL_{SYS} <= (SIL\ CL_{subsystem})_{lowest}$ ➔ SIL claim limit: 2

Random integrity

$PFH_D = PFH_{D1} + ... + PFH_{Dn} + P_{TE}$ ➔ $PFH_D = (2+0.5+1+3+3)*10^{-7} < 10^{-6}$

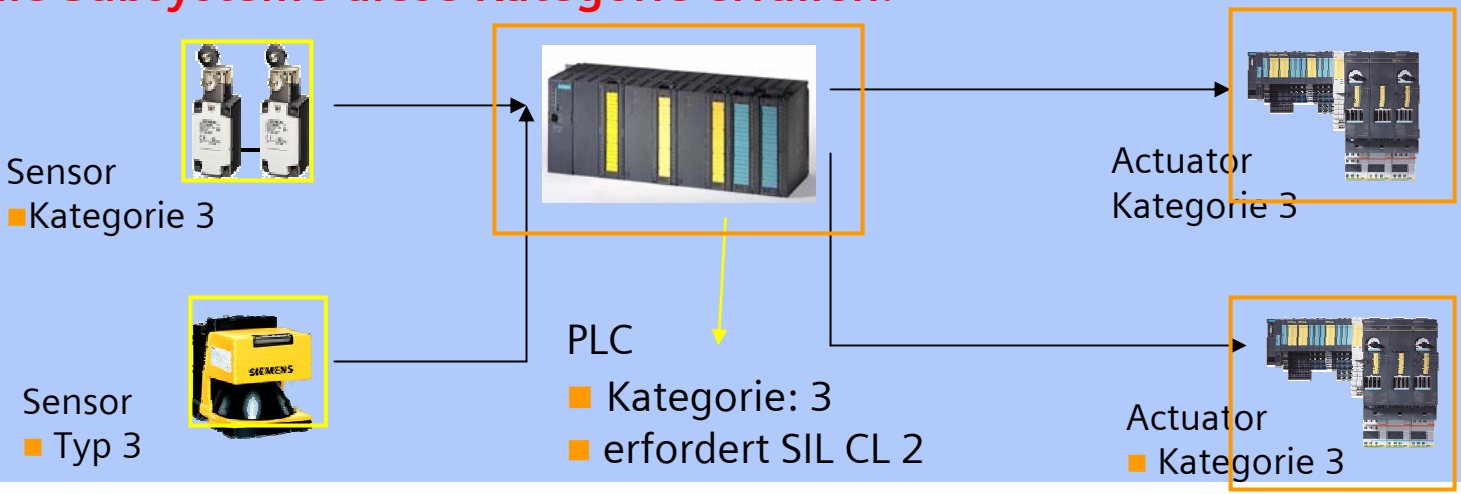
P_{TE} = Wahrscheinlichkeit eines unerkannten Fehlers in der Kommunikation

System erreicht: SIL 2

SIEMENS

Safety Performance nach EN 954 für Beispiel (2)

Das System erfüllt eine bestimmte Kategorie, wenn alle Subsysteme diese Kategorie erfüllen.



Subsystem nach 62061 kann als sicherheitsrelevantes Teil betrachtet werden auf das die Kategorien nach 954 anzuwenden sind.

- **Systematic integrity**

  Ähnlich den „bewährten Sicherheitsprinzipien“

- **Architectural constraints**

  Ähnlich den Strukturanforderungen der Kategorie.

- **Random integrity**

  PFH_D ist bei 954 nicht relevant

Safety Performance Daten von Subsystemen (1)

- **S7-300F CPU**
  - **SIL CL:** **Kategorie:**
  - **PFH_D:**
  - **P_{TE}:**
- **S7-300F Remote I/O**
  - **SIL CL:** **Kategorie:**
  - **PFH_D:**
  - **P_{TE}:**
- **Motorstarter (ET200S)**
  - **SIL CL:** **Kategorie:**
  - **PFH_D:** **B_{10} : (?)**
  - **P_{TE}:**
  - **Diagnose:** integriert

Subsystemdesign - Positionserfassung

Subsystemelement

Herstellerangaben

B_{10} :

T1:

Diagnosesupport:

Subsystem

Fehleraufdeckung durch Vergleich in der F-SPS

Zeitbezogene Ausfallrate λ

B10: Herstellerangabe

C: Schalthäufigkeit in [1 / h]

$\lambda = 0.1 \times C / B10$

Rate gefahrbringender Fehler

Gefahrbringende Fehler: “Kontakte öffnen nicht” = 50%

$\lambda_D = 0.5 \times \lambda$

Homogene Redundanz (gleiche Geräte)

$\lambda_1 = \lambda_2 = \lambda$; $DC_1 = DC_2 = DC$

Fehleraufdeckungsgrad
(bei Vergleich in F-SPS)
DC = 99%

Common cause Fehler
CCF: 5%

Safety Performance Daten von Subsystemen (2)

Zweihand-Bediengerät

SIL CL: **Kategorie:**

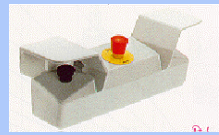
PFH_D: **B_{10} :**

P_{TE}:

Diagnose: Step7 Baustein xxxx

T2: keine feste Zeitvorgabe, Test bei jeder Betätigung

T1: Lebensdauer



Lichtvorhang

SIL CL: **Typ:**

PFH_D:

P_{TE}:

Diagnose: integriert

Zuhaltung

B_{10} :

Diagnose:

Safety Performance Daten von Subsystemelementen (1)

Positionsschalter mit Zwangsöffnung

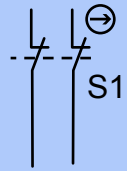
B_{10} :

Fehlermodi:

- <Fehler> **<**Anteil an aufgetretenen Ausfällen in **%>**
- Kontakte schließen nicht; 90% (Hausnummer!)
- Kontakte öffnen nicht ; 10%

T1:

Diagnosesupport: keiner



Motorschütz

B_{10} :

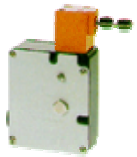
Fehlermodi:

- <Fehler> **<**Anteil an aufgetretenen Ausfällen in **%>**
- Alle Kontakte schließen nicht; 25%
- Alle Kontakte öffnen nicht; 25%
- einzelne Kontakte schließen nicht; 10%
- einzelne Kontakte öffen nicht; 10%
- Hilfskontakt schließt bei geschlossenem Lastkontakt: 1%
- ....

Diagnosesupport: zwangsgeführter Hilfskontakt (Schließer)

Subsystemdesign - Zuhaltung

Subsystemelement



Herstellerangaben

B_{10} :

T1:

Diagnosesupport: keiner

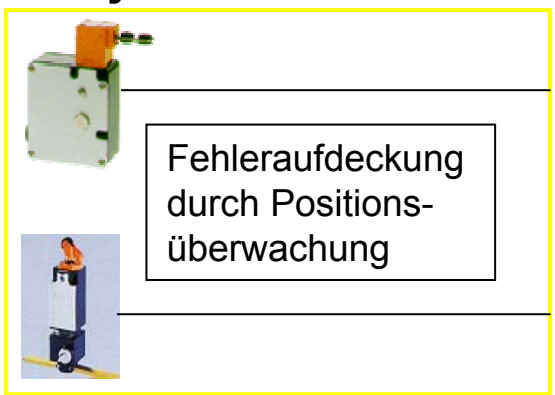
Ausfallrate λ

B10: Herstellerangabe

C: Schalthäufigkeit in [1 / h]

$\lambda = 0.1 \times C / B10$

Subsystem



Neuerungen bei Normen

Subsystemdesign - “Motorschütz”

Subsystemelement

Ausfallrate λ

B10: Herstellerangabe

C: Schalthäufigkeit in [1 / h]

$\lambda = 0.1 \times C / B10$

Subsystem

Fehleraufdeckung: Vergleich der Hilfkontakte mit Sollstellung beider Schütze in SPS

Herstellerangaben

B_{10} :

T1:

Diagnosesupport:
zwangsgeführte Hilfskontakte

Rate gefahrbringender Fehler

Gefahrbringende Fehler: “Kontakte öffnen nicht” = xx%

$\lambda_D = 0.x \times \lambda$

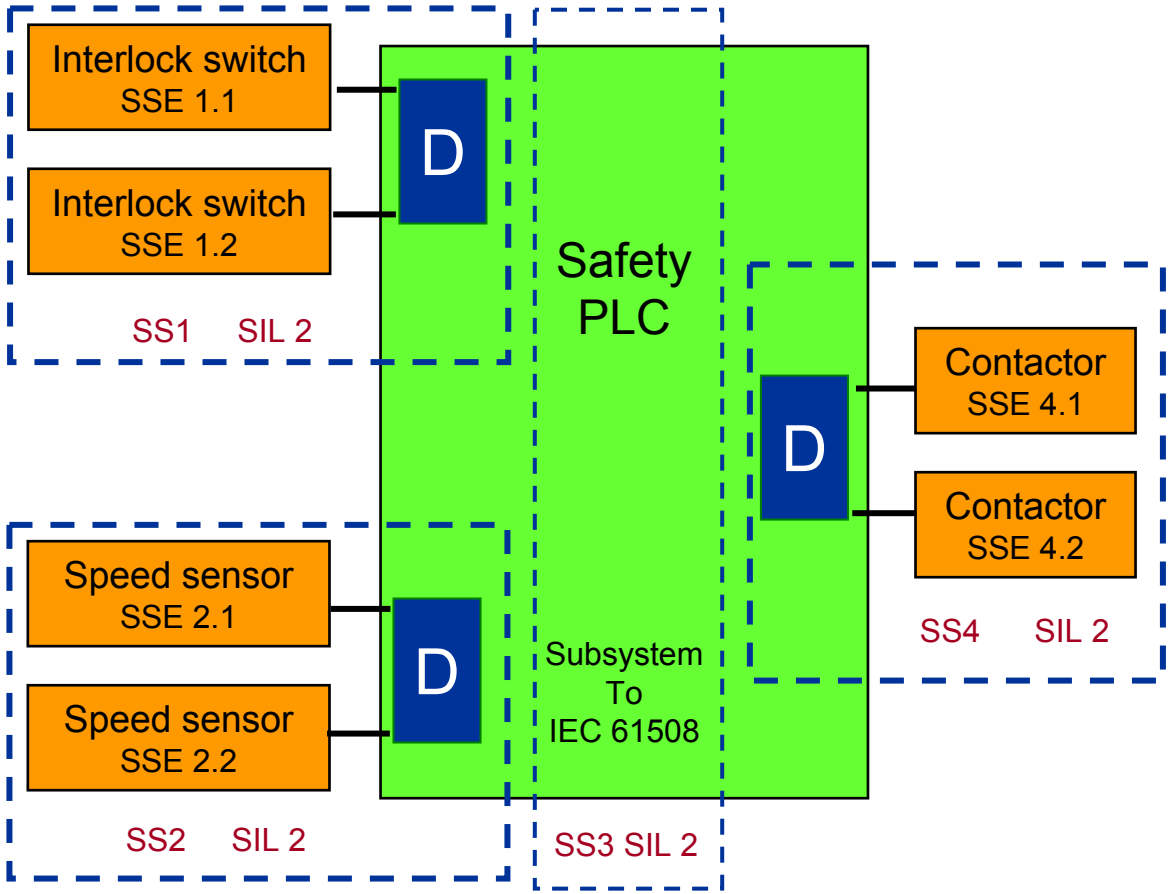
Homogene Redundanz (gleiche Geräte)
$\lambda_1 = \lambda_2 = \lambda$; $DC_1 = DC_2 = DC$

Fehleraufdeckungsgrad
(bei Vergleich in F-SPS)
DC = 99%

Common cause Fehler

Subsystemdiagnose durch SPS oder 3TK...

Statt dessen Simatic mit Software baustein und realen Geräten



Neuerungen bei Normen

Unterschiede / Gemeinsamkeiten IEC 62061 zu IEC 61508

IEC 61508 (Basisnorm)

- für Normensetzer und Steuerungshersteller und ggf. Anwender
- beschreibt detaillierte Anforderungen für das System, seine Subsysteme und dessen Komponenten
- beschreibt die Anforderungen allgemein ohne auf Anwendungsspezifika einzugehen

IEC 62061 (Anwendernorm)

- beschreibt wie ein System aus vorhandenen Subsystemen aufgebaut wird und wie dessen Sicherheitsanforderungen (SIL) bestimmt werden kann.
- beschreibt Anforderungen zum Design von Subsystemen nur für "low complexity Subsysteme" (nicht für programmierbare Elektronik)
- Für komplexe Subsysteme (z.B. SPS) wird vorausgesetzt, dass sie 61508 erfüllen.

➔Ein System, das nach 62061 designed ist, erfüllt die relevanten Anforderungen von 61508.

Konzept DIS ISO13849-1(rev)

Ist noch Entwurf.

ISO 13849-1(revision)

- ist derzeit noch im Entwurfsstadium (prEN ....) (09.2004)
  - Bei der Kommentierung sind viele, umfangreiche Einsprüche eingegangen
  - Es sind noch technische Änderungen zu erwarten
  - Verabschiedung frühestens 2005 (genauerer Termin ist derzeit nicht bekannt)
- Bis zur Verabschiedung gilt weiterhin EN 954

➔ Erläuterung zur Anwendung von ISO 13849-1 (revision) nur mit Vorbehalt.

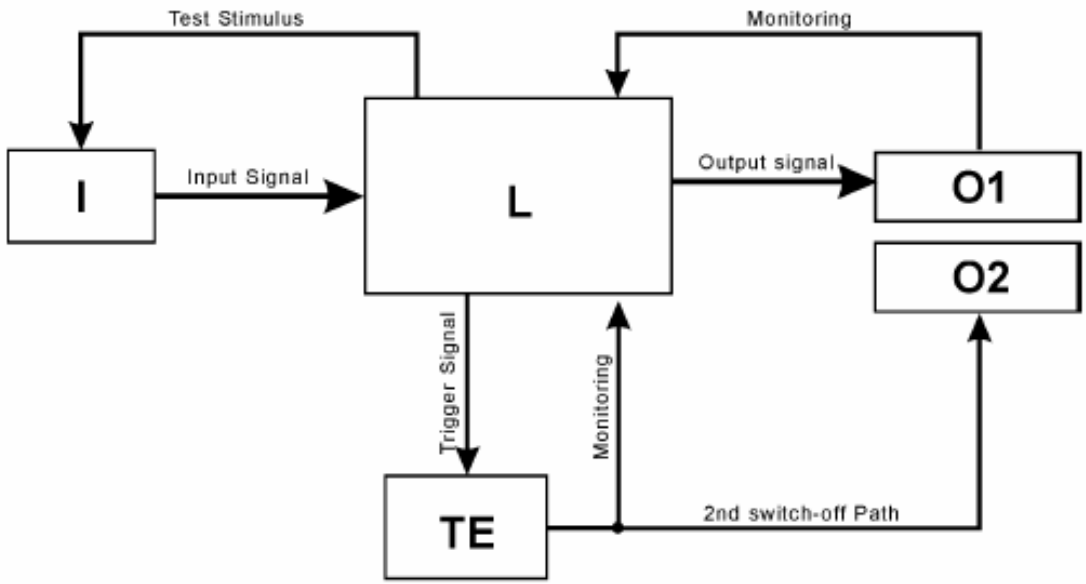
Draft ISO 13849-1(rev)

- Kategorien aus EN 954-1 sind nicht mehr das Maß für die Safety Performance
- Kategorien dienen der “internen” Strukturierung

- ISO13849-1(rev) verwendet andere Begriffe als IEC
  - System: PL (Performance Level) anstatt SIL (Safety Integrity Level)
    - PL (Performance Level) und SIL (Safety Integrity Level) korrespondieren
  - Geräte: MTTF anstatt PFH
    - Keine direkte Umrechnung zwischen MTTF und PFH

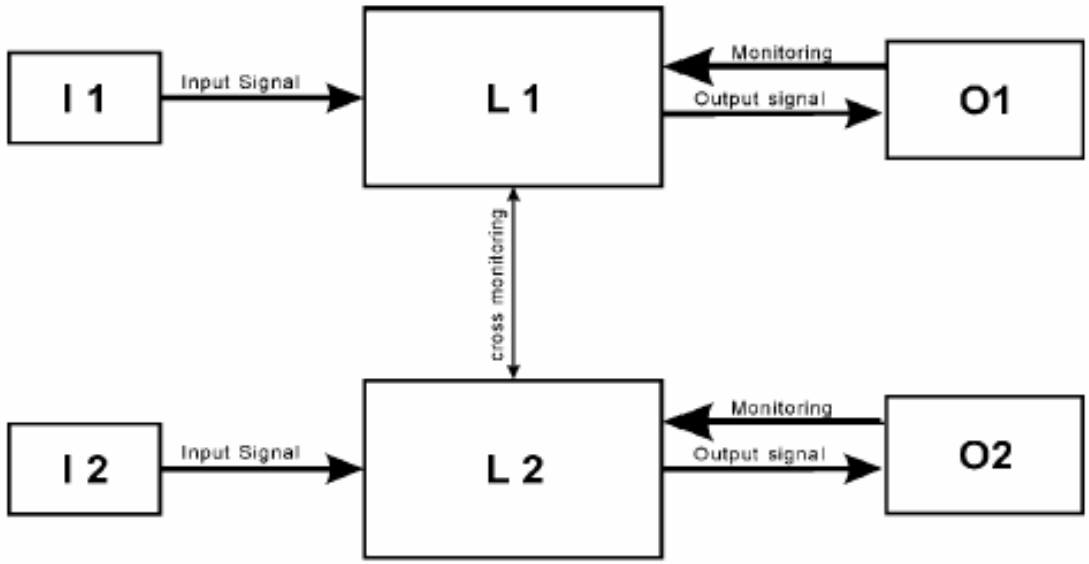
- Methoden zur Quantifizierung basieren auf “designated architectures”
  - Für diese Architekturen können vorberechnete PL-Werte über Tabellen ermittelt werden.

Architektur nach Kategorie 2



I: Input e.g. Sensor
L: Logic
O1/O2: Output e.g. Actuator
TE: Test equipment

Architektur nach Kategorie 4



I 1, I 2: Inputs e.g. Sensors
L1, L2: Logic
O: Outputs e.g. Actuator

Status ISO 13849-1(rev)

04. 2004: DIS zur 1. Kommentierung verteilt

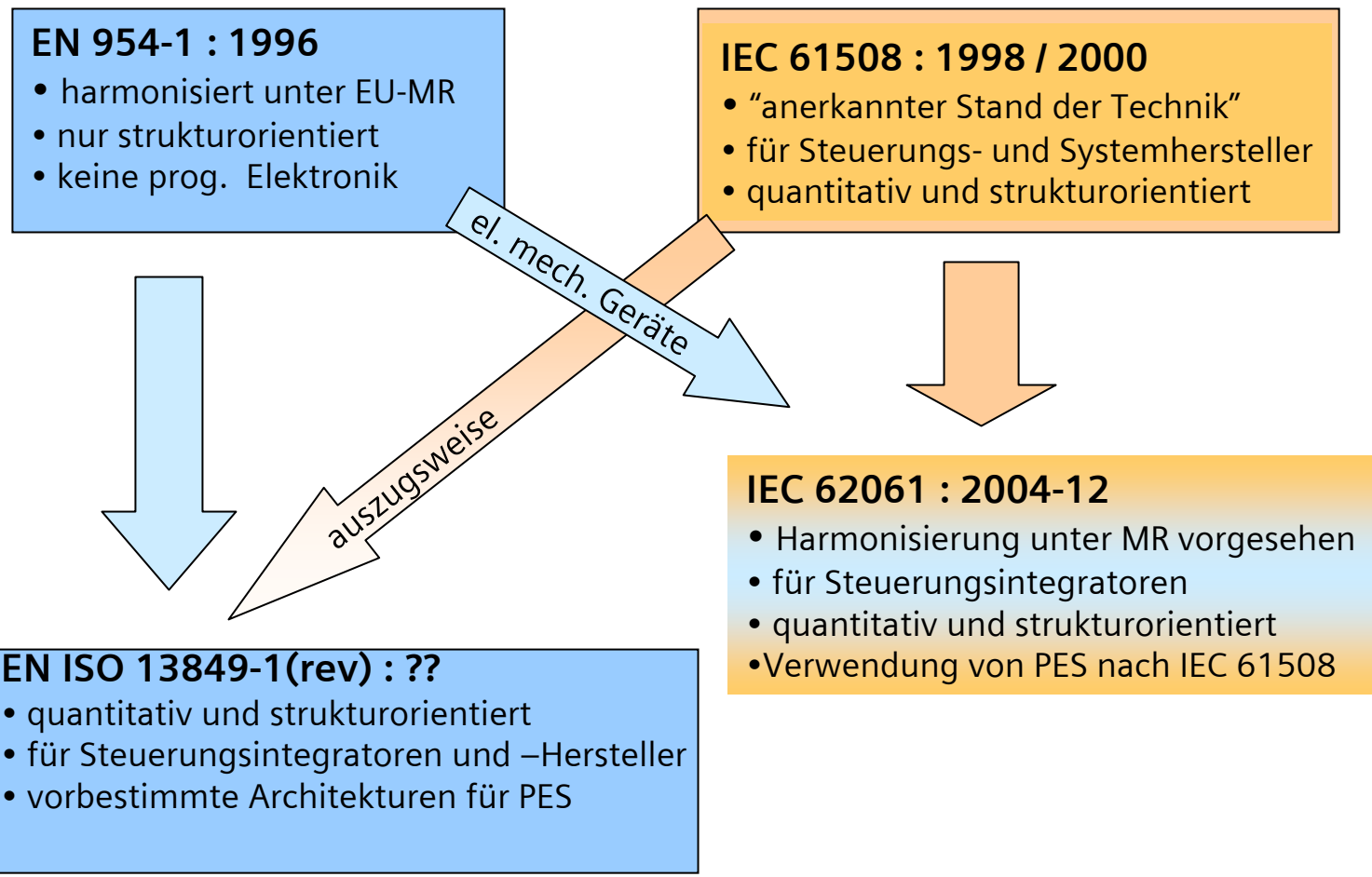
10. 2004: Einsprüche / Kommentare > 130 Seiten

- die vorhandenen Anforderungen reichen nicht für sichere programmierbare Elektronik
- Software ist nicht behandelt
- Quantifizierung für elektromechanische Geräte ist nicht korrekt behandelt

➔ es sind noch umfangreiche technische Arbeiten notwendig

➔Termin für FDIS ist unklar

Weiterentwicklung der Basisnormen



Resümee

- Durch Anwendung von EN 954 (alt) können die Anforderungen der EU-Maschinenrichtlinie erfüllt werden (formal).
- Durch (zusätzliche) Anwendung von IEC 62061 wird nicht nur die MR formal erfüllt, sondern darüber hinaus der aktuelle Stand der Technik.
- Die Weiterentwicklung der Sicherheitstechnik ermöglicht
  - ... differenziertere funktionsbezogene Betrachtung
  - ... Berücksichtigt auch die Qualität der verwendeten Geräte (Ausfallraten)
  - ... beachtet auch die Beanspruchung und Lebensdauer der Geräte
- Zu ISO 13849-1(rev) sind noch keine verbindlichen Aussagen möglich
  - Technik ändert sich noch
  - Termin steht noch nicht fest