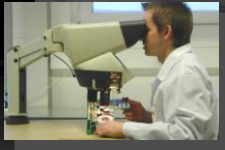
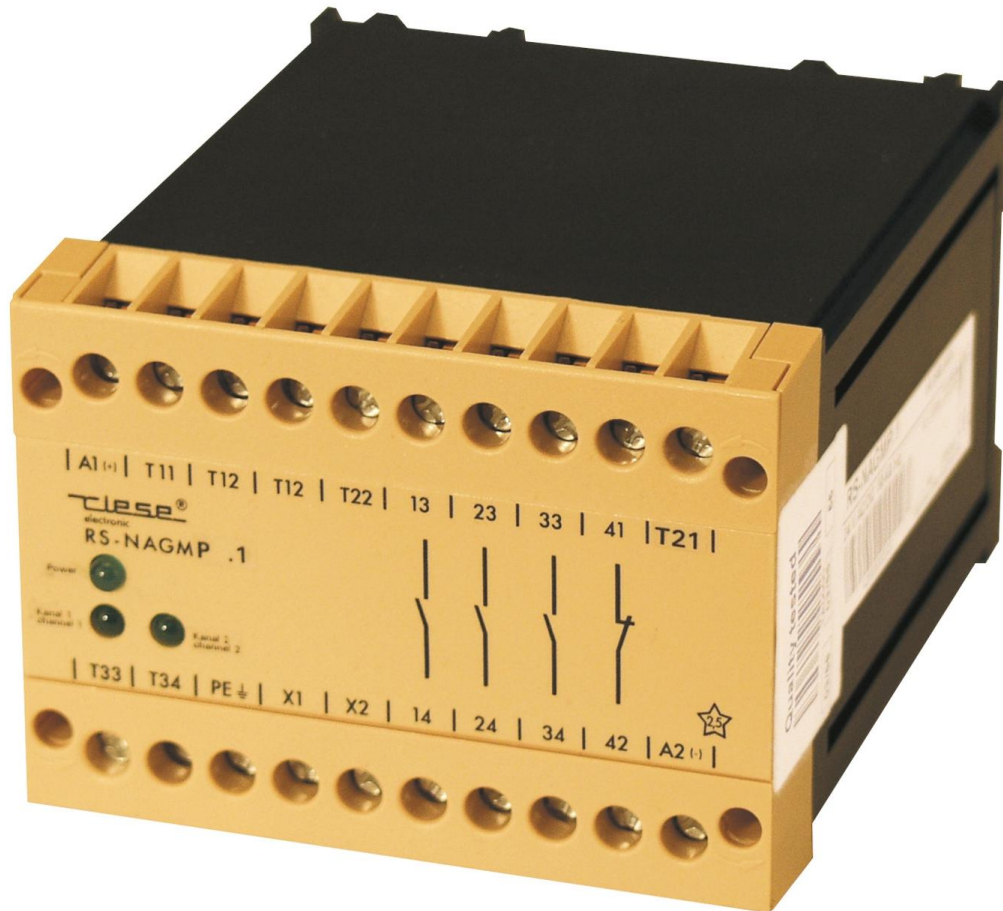


SIL - Normen

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



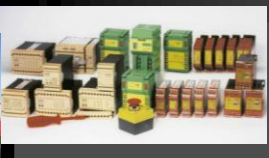
- Allgemeiner Vergleich
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss



NAGMP



SAFE C1



Allgemeiner Vergleich

DIN EN 954

„Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen“

- **Allgemeiner Vergleich**
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss

EN 954 - Aufbau

Geräte bestanden aus:

- ⌘ Mechanische Bauteile (zwangsgeführte Relais)
- ⌘ Einfache elektrische Bauteile (Transformatoren, Dioden, Optokoppler)
- ⌘ Einfache elektronische Bauteile (bipolare Transistoren, niedrigintegrierte Logikbauteile HC / HCT)
- ⌘ THT – bedrahtete Bauelemente
- ⌘ Keine FETs, hochintegrierte ICs wie Prozessoren, Controller



- Allgemeiner Vergleich

- Entwicklung

- Allgemein

- Fehlerbetrachtung

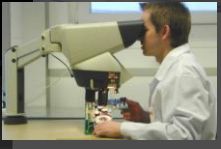
- Funktionalität

- Hilfsmittel

- Hardware

- Anwendung

- Abschluss



EN 954 - Sicherheitskategorien

Kategorie	Bedeutung	Bemerkung
B	Bewährt	Ein Fehler kann zum Verlust der Sicherheitsfunktion führen
1	Bewährt	Wie B jedoch Wahrscheinlichkeit, dass ein Fehler auftritt kleiner als in B
2	Testung	Ein Fehler kann zum Verlust der Sicherheitsfunktion führen, wird jedoch durch eine zyklische Testung erkannt
3	Ein-Fehler sicher	Ein einzelner Fehler führt nicht zum Verlust der Sicherheitsfunktion. Einige aber nicht alle Fehler werden erkannt. Eine Anhäufung von Fehlern kann zum Verlust der Sicherheitsfunktion führen
4	Mehr-Fehler sicher	Beim Auftritt eines Fehlers bleibt die Sicherheitsfunktion erhalten. Ein Fehler wird so rechtzeitig erkannt, dass eine Anhäufung nicht zum Verlust der Sicherheitsfunktion führt.

- Allgemeiner Vergleich

-Entwicklung

- Allgemein

- Fehlerbetrachtung

- Funktionalität

- Hilfsmittel

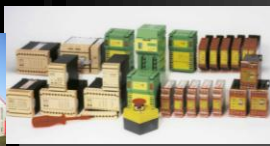
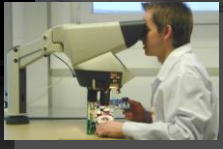
- Hardware

-Anwendung

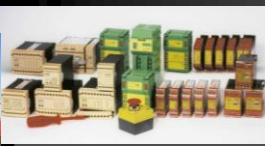
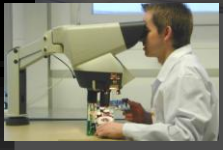
-Abschluss

EN 954 - Zertifizierung

- ⌘ Zertifizierung durch BG / TÜV
- ⌘ Nur die Entwicklung des Gerätes wurde betrachtet, das Umfeld nur in kleinem Maße
- ⌘ Mögliche Fehler wurden „abgezählt“, die Reaktion des Gerätes geprüft / abgeschätzt.
- ⌘ Gerät wurde zertifiziert, Zertifikate konnten quasi unbegrenzt verlängert werden
- ⌘ Betriebsstättenbesichtigungen dienen der Sicherstellung, dass das Gerät weiterhin so gebaut wird, wie es zugelassen wurde



- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Allgemeiner Vergleich

DIN EN 61508

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

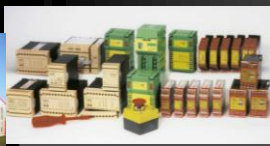
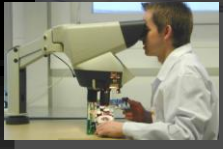
DIN EN 62061

Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Systeme

DIN EN ISO 13849

„Sicherheit von Maschinen -
Sicherheitsbezogene Teile von Steuerungen“

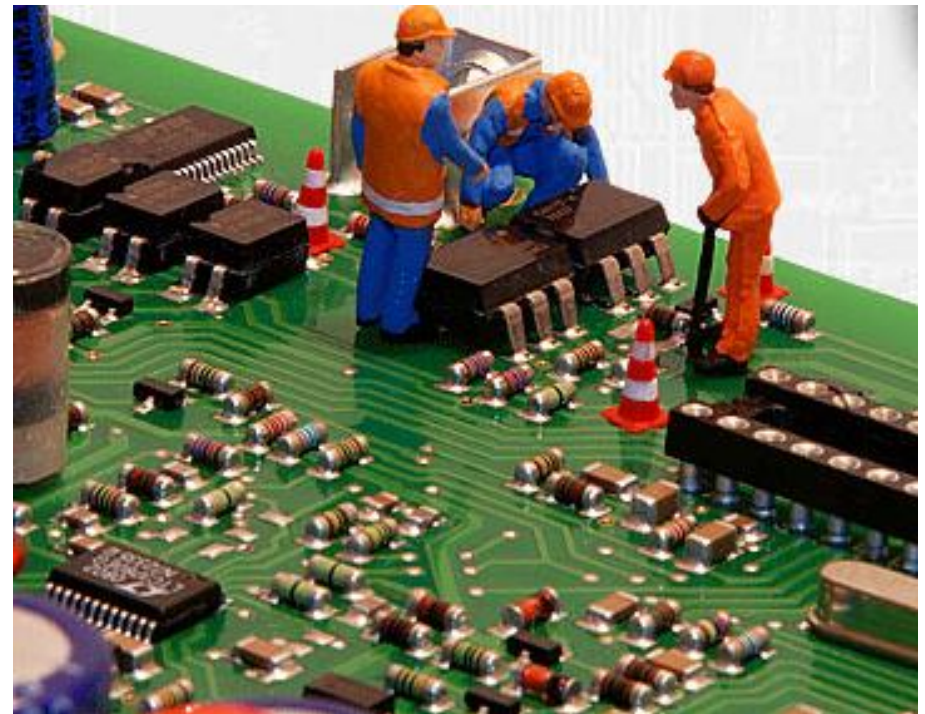
- **Allgemeiner Vergleich**
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss



SIL - Aufbau

Geräte bestehen aus:

- ⌘ Mechanische Bauteile (zwangsgeführte Relais)
oder Leistungshalbleiter
- ⌘ Einfache elektrische und elektronische Bauteile (Transformatoren, Optokoppler, Transistoren, ICs)
- ⌘ SMD und THT
- ⌘ Hochintegrierte ICs wie Prozessoren, μ Cs

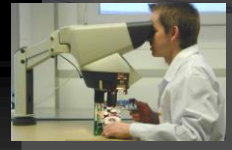


- Allgemeiner Vergleich
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss

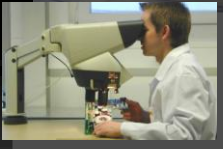
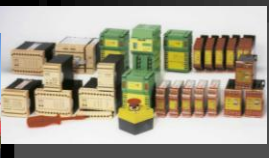
SIL – Risikobewertung - 1

SIL	Betriebsart mit hoher Anforderungsrate "High-Demand"
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Wahrscheinlichkeit eines Gefahr bringenden Ausfalls pro Stunde



- **Allgemeiner Vergleich**
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



SIL – Risikobewertung - 2

Auswirkungen	Schadensausmaß S	Klasse K = F + W + P				
		4	5-7	8-10	11-13	14-15
Tod; Verlust von Auge oder Arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, Verlust von Fingern	3			SIL1	SIL2	SIL3
Reversibel, medizinische Behandlung	2				SIL1	SIL2
Reversibel, Erste Hilfe	1					SIL1

- **Allgemeiner Vergleich**
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss

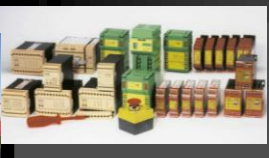
SIL – Risikobewertung - 3

Häufigkeit des Gefährdungsereignisses (Aufenthalte > 10 min)		
F		
F	≥ 1x pro Stunde	5
1x pro Stunde	> F ≥ 1x pro Tag	5
1x pro Tag	> F ≥ 1x in 2 Wochen	4
1x in 2 Wochen	> F ≥ 1x pro Jahr	3
1x pro Jahr	> F	2

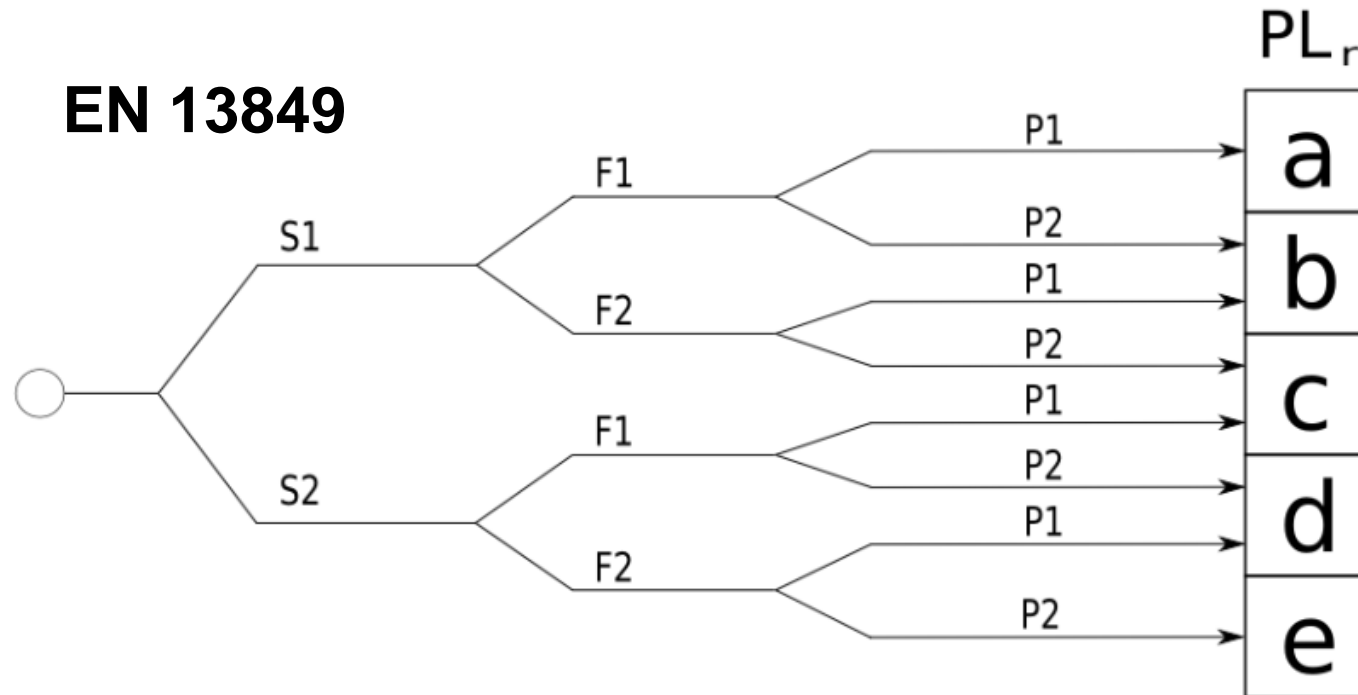
Möglichkeit zur Vermeidung des Gefährdungsereignisses	
P	
Unmöglich	5
Möglich	3
Wahrscheinlich	1

Eintrittswahrscheinlichkeit des Gefährdungsereignisses	
W	
Häufig	5
Wahrscheinlich	4
Möglich	3
Selten	2
Vernachlässigbar	1

- **Allgemeiner Vergleich**
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss



SIL – Risikobewertung - 4

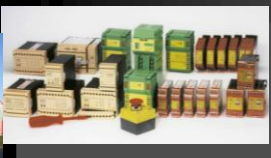
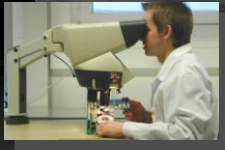


S - Schwere der Verletzung

F - Gefährdungsexposition

P - Möglichkeit der Vermeidung der Gefährdung

- **Allgemeiner Vergleich**
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- Abschluss



SIL

EG-Baumusterprüfbescheinigung

- ⌘ Zertifizierung durch akkreditierte Stelle
- ⌘ Prüfung der Entwicklung
- ⌘ Ermittlung der Kategorie
- ⌘ Ermittlung der Ausfallwahrscheinlichkeiten
- ⌘ EG-BMP können nicht verlängert werden
- ⌘ Beurteilung des QM-Systems
- ⌘ Betriebsstättenbesichtigungen dienen der Sicherstellung, dass das Gerät weiterhin so gebaut wird, wie es zugelassen wurde

- Allgemeiner Vergleich

-Entwicklung

- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware

-Anwendung

-Abschluss

Entwicklung

Realisierung der Sicherheit

Was hat sich geändert?

- Allgemeiner Vergleich

- **Entwicklung**

- Allgemein

- Fehlerbetrachtung

- Funktionalität

- Hilfsmittel

- Hardware

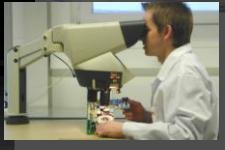
- Anwendung

- Abschluss

Entwicklung - EN 954 - **Allgemein**

- ⌘ Funktionalität: gering
- ⌘ Hilfsmittel: Multimeter, Oszilloskop
- ⌘ Entwickler hat „ \uparrow -Daumen“ überdimensioniert, z.B. 50% Reserve

- Allgemeiner Vergleich
- Entwicklung
 - **Allgemein**
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Entwicklung - SIL - **Allgemein**

- ⌘ Funktionalität: hoch
- ⌘ Hilfsmittel: Logic Analyzer, Simulations-SW
- ⌘ Die vom Entwickler einkalkulierte Reserve ist eine Rechengröße für die probabilistische Betrachtung.

- Allgemeiner Vergleich
- Entwicklung
 - **Allgemein**
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss

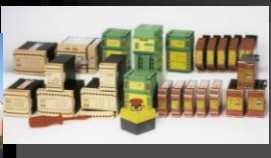
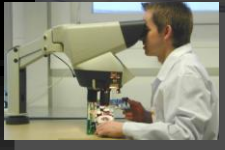
Entwicklung - EN 954 - Fehlerbetrachtung

- ⌘ Fehler wurden abgezählt, z.B. 3-Fehler-sicher
- ⌘ Betrachtung nur der kritischen Bauteile
- ⌘ Erstellen einer Tabelle zwecks Ermittlung des Fehlerfortpflanzungsverhaltens entsprechend der angestrebten Kategorie (nach z.B. 3 Fehlern hörte man auf)

Schwerpunkt:

HW wird z.B. durch redundante Aufbauten möglichst sicher gemacht, das Gerät läuft im Fehlerfall weiter.

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Entwicklung - SIL - FMEDA

Jedes einzelne Bauteil wird auf verschiedene Ausfallmöglichkeiten betrachtet,

z.B.: Widerstand:

- Kurzschluss (0Ω)
- Unterbrechung ($\infty \Omega$)
- Drift (-50% / +100%)

Schwerpunkt:

Auftretende Fehler sollen sofort erkannt werden, das Gerät schaltet sicher ab.

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss

Entwicklung - EN 954 - Funktionalität

⌘ Geringe Funktionalität

⌘ Wenige einfache Funktionen pro Gerät

z.B.

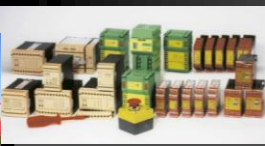
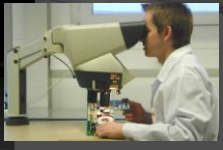
Not-Aus nur 4-kanalig

Matte nur 4-Draht-Matte auto/manuell

Lichtschanke nur Typ 4 auto/manuell

Zweihand nur Typ 3c

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - **Funktionalität**
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Entwicklung - SIL - Funktionalität

⌘ Hohe Funktionalität und bessere Flexibilität

⌘ Mehrere oder verschiedene Funktionen in einem Gerät, wie z.B.:

Not-Halt: 2- und 4-kanalig

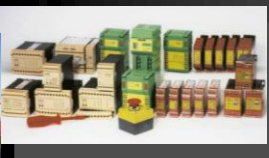
Matte: 4-Draht + 2-Draht mit Widerstand

BWS: Typ 2 + Typ 4

Zweihand: konfigurierbar

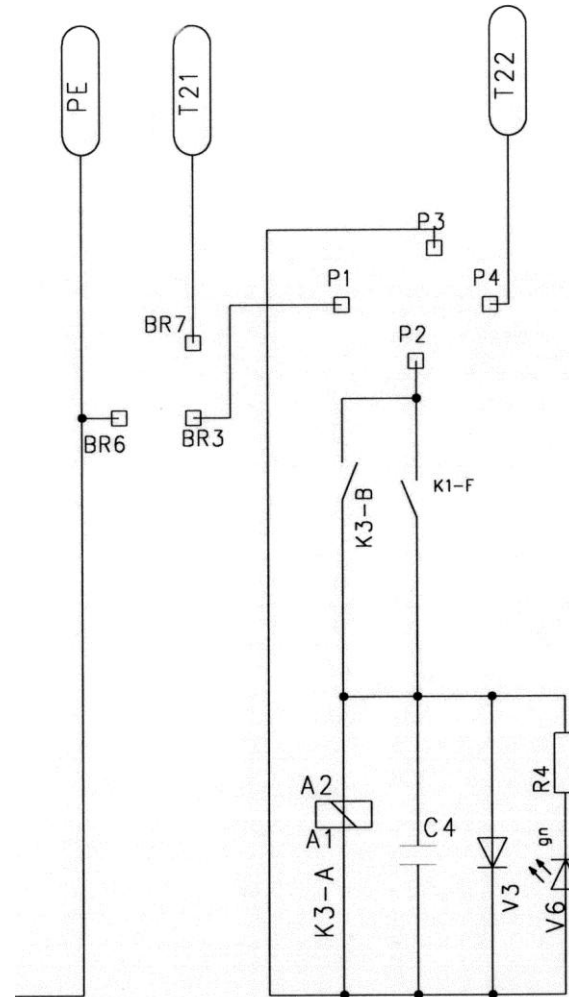
jeweils mit wahlweiser Überwachung der Eingangskreise

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - **Funktionalität**
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Entwicklung - EN 954 - Hardware

Beispiel:



- Allgemeiner Vergleich
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- **Hardware**
- Anwendung
- Abschluss

Entwicklung - EN 954 - Hardware

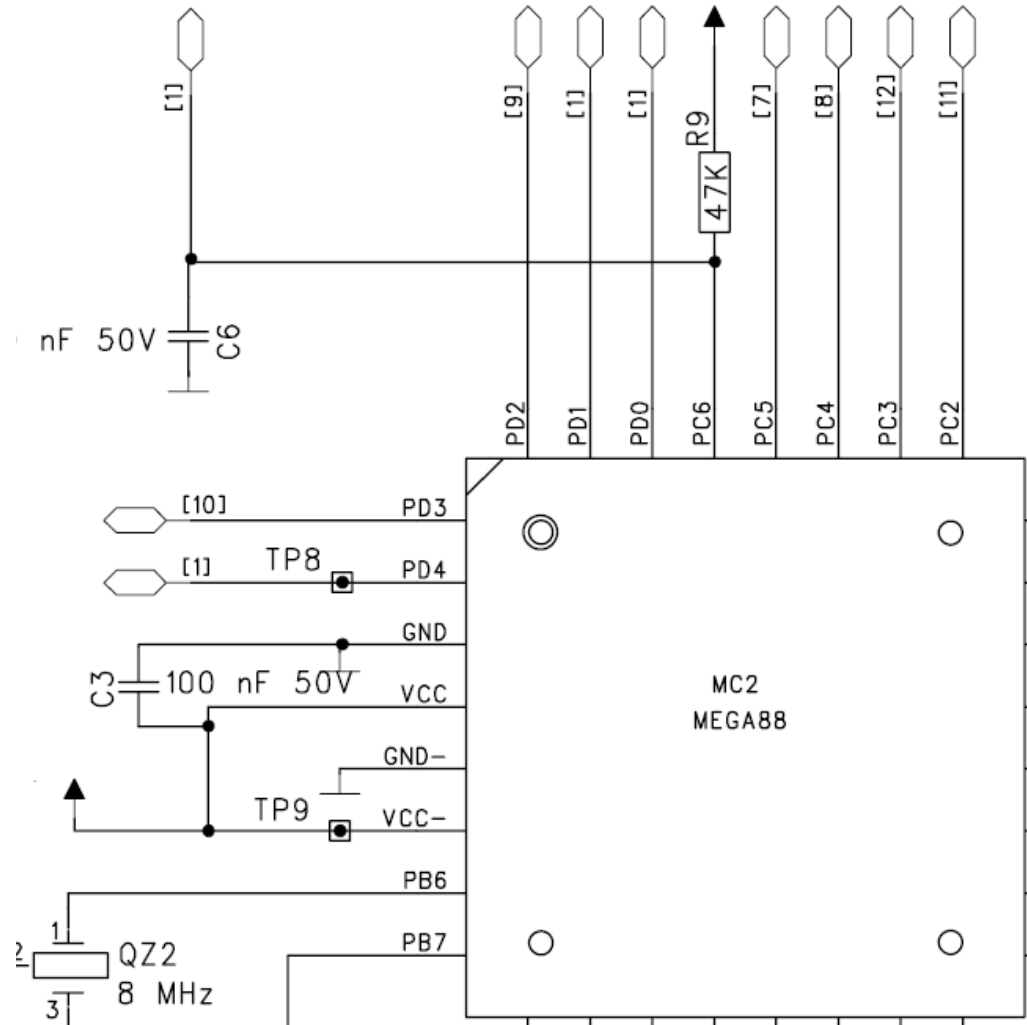
- ⌘ Redundanz in der Hardware, z.B. 2 in Reihe geschaltete Dioden
- ⌘ Kein Vergleich der beiden Kanäle
- ⌘ Keine analogen Signale wegen aufwändiger Fehlersicherheit
- ⌘ Geringe Information

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - **Hardware**
- Anwendung
- Abschluss



Entwicklung - SIL - Hardware

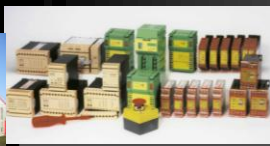
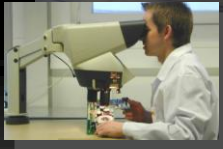
Beispiel:



- Allgemeiner Vergleich
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- **Hardware**
- Anwendung
- Abschluss

Entwicklung - SIL - Hardware

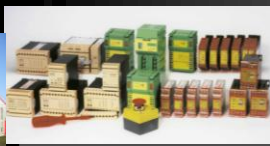
- ⌘ Redundanz in der Hardware durch 2-kanaligen Aufbau
- ⌘ Prüfung der Hardware durch die Software z.B. durch Loopbacks
- ⌘ Direkter Vergleich beider Kanäle zeitlich und logisch
- ⌘ Verarbeitung analoger Signale möglich
- ⌘ Fehler- und Info-LED mit deutlich erweiterter Information für den Bediener, z.B. warum schaltet das Relais jetzt nicht durch; welcher Fehler wurde erkannt.



- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - **Hardware**
- Anwendung
- Abschluss

Anwendung - EN 954

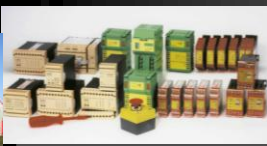
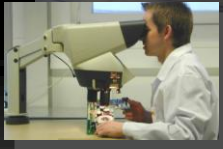
- ⌘ Ermitteln der benötigten Kategorie
- ⌘ Einsetzen von Geräten, die dieser Kategorie entsprechen unter Beachtung der Angaben des Herstellers
- ⌘ Prüfung der Sicherheitsschaltung nicht explizit gefordert, jedoch der Gesamtmaschine
- ⌘ Fachkraft benötigt



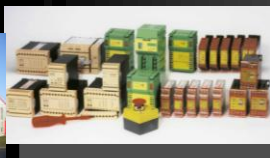
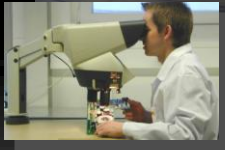
- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss

Anwendung - SIL

- ⌘ Ermitteln des benötigten SIL/PL
- ⌘ Einsetzen von Geräten, die zusammen diesem SIL/PL entsprechen, hierbei sind Berechnungen notwendig
→ Hilfsmittel SISTEMA (EN13849)
- ⌘ Prüfung auch der Teilkomponenten explizit gefordert
- ⌘ Fehlerbetrachtung erforderlich
- ⌘ Hohe Ansprüche an Dokumentation, jeder einzelne Schritt muss nachvollziehbar dokumentiert werden, warum, wieviel, wann, wer, ...
- ⌘ Speziell geschulte und qualifizierte Fachkraft erforderlich, die auch eine höhere Verantwortung trägt



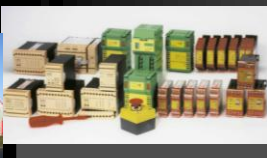
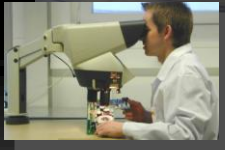
- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss



Abschluss

Während der Laufzeit der EN 954 hat es bereits einige Anpassungen gegeben, die Unterstützung neuer Technologien, wie z.B. der Einsatz von μ Cs, wurde jedoch nie unterstützt, bestenfalls geduldet.

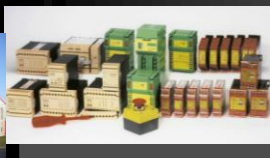
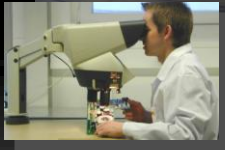
- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss**



Abschluss

Die einfache Betrachtungsweise, einfach Fehler zu zählen, war für eine derart komplexe Technik mit derart vielen unterschiedlichen Fehlermöglichkeiten, denkbar ungeeignet.

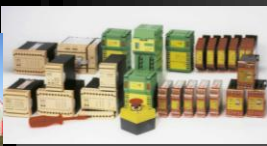
- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss**



Abschluss

- Andererseits brachten die neuen Technologien bedeutende Vorteile, wie
- einfachere Herstellung
 - bessere Geräte auch durch höhere Funktionalität
 - letztlich bessere Sicherheit
 - Manipulation erschwert

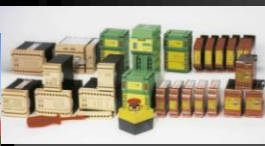
- Allgemeiner Vergleich
- Entwicklung
- Allgemein
- Fehlerbetrachtung
- Funktionalität
- Hilfsmittel
- Hardware
- Anwendung
- **Abschluss**



Abschluss

Die neuen Normen lösten das Problem durch einen probabilistischen Ansatz, nicht die Anzahl der Fehler in einer Kette sind entscheidend, sondern letztlich die Sicherheit des Geräts, ausgedrückt durch die Wahrscheinlichkeit (bzw. auch Unwahrscheinlichkeit) eines gefährlichen Ausfalls pro Zeit.

- Allgemeiner Vergleich
- Entwicklung
 - Allgemein
 - Fehlerbetrachtung
 - Funktionalität
 - Hilfsmittel
 - Hardware
- Anwendung
- Abschluss**



Danke für Ihre Aufmerksamkeit

