Technische Hochschule Georg Agricola

INDUSTRIEAUTOMATION

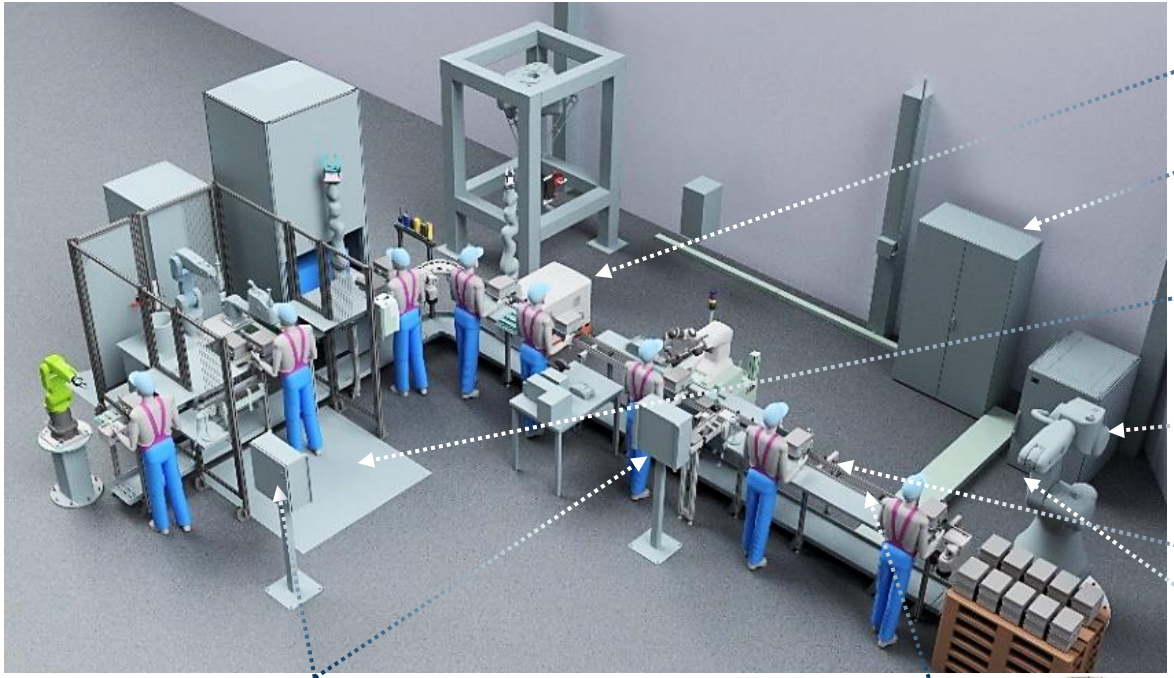
EINFÜHRUNG

Bochum

Prof. Dr.-Ing. Lars N. Josler

BESTANDTEILE EINES AUTOMATISIERUNGSSYSTEMS

Beispiel: Photovoltaik-Schaltkästen produzieren



- Mobile Robotik
- SPS und Bussysteme
- Sicherheitstechnik
- Handhabungssysteme / Bewegungskinematiken (z. B. Roboter)
- Sensortechnik und Wegmesssysteme
- Greifer / Effektoren FA
- Materialfluss-, Förder- und Ordnungseinrichtungen FA
- Mensch-Maschine-Schnittstelle MZR

BESTANDTEILE EINES AUTOMATISIERUNGSSYSTEMS

Schwerpunkt: Sicherheitstechnik / Sensorik und Bildverarbeitung

GRUNDLAGEN DER SICHERHEITSTECHNIK

Einführung

Gesetzliche Regelung

Begriffe und Definitionen

Risikobeurteilung

Konstruktion

Risikoanalytik

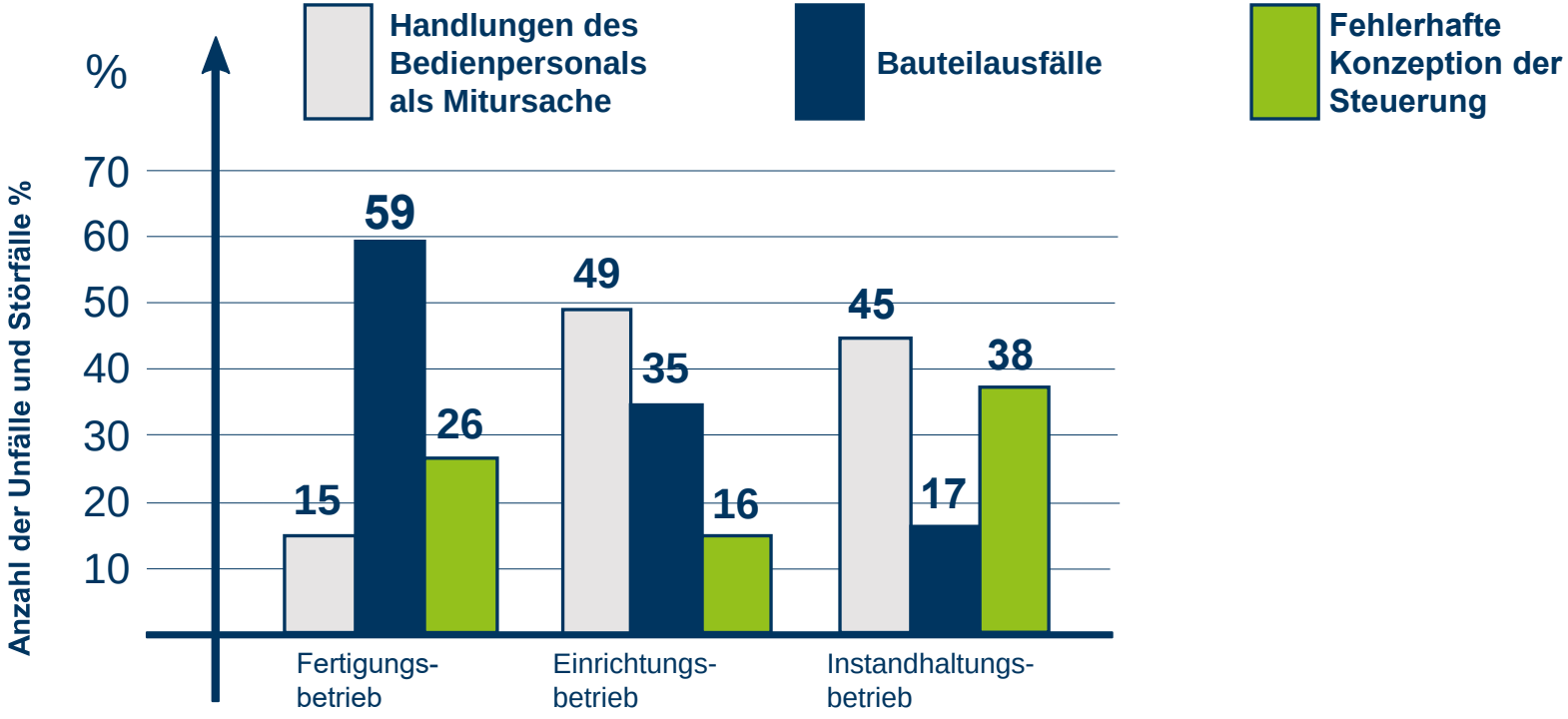
WARUM SICHERHEITSTECHNIK?

- Maschine darf keine Menschen gefährden
- Vollständige Kapselung einer Maschine nicht möglich
  → daher Sicherheitsvorkehrungen notwendig, z. B. Schutztüren

- Regeln für die sicherheitsgerechte Gestaltung vorhanden, z. B. in Normen

- Vereinheitlichung in Europa durch die **Maschinenverordnung**
- Rechtssicherheit für Unternehmen
- Schutz der Beschäftigten und Konsumenten

HAUPTURSACHEN VON UNFÄLLEN UND STÖRUNGEN



Tätigkeit der betroffenen Personen zum Unfall- und Störfallzeitpunkt

Quelle: Unfall- und Störbericht der BIA Nr. 330 250

HAUPTURSACHEN VON UNFÄLLEN UND STÖRUNGEN

Quelle: https://www.youtube.com/watch?v=5ZBaE6s0kOo&ab_channel=c0wcommander

GRUNDLAGEN DER SICHERHEITSTECHNIK

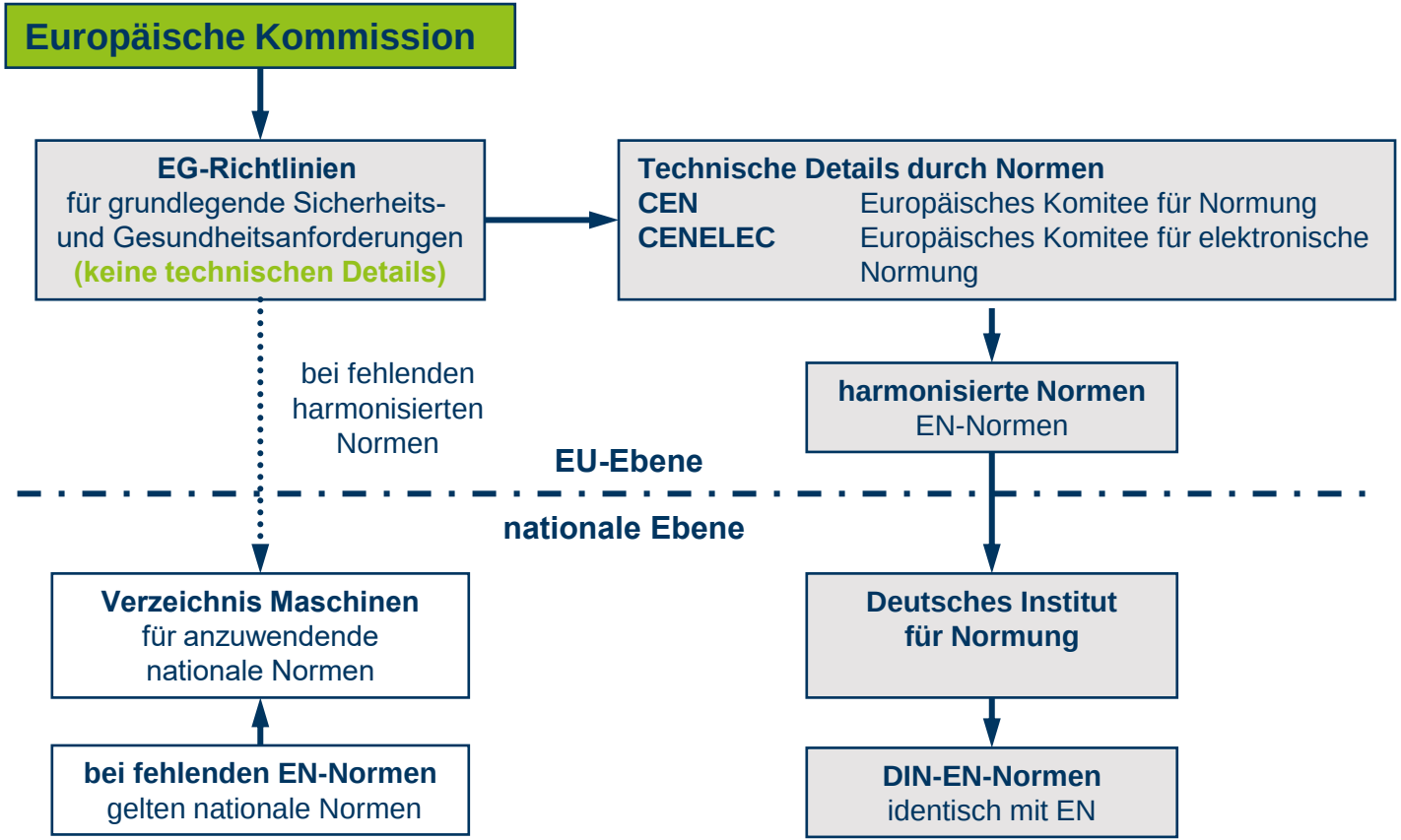
- Einführung
- **Gesetzliche Regelung**
- Begriffe und Definitionen
- Risikobeurteilung
- Konstruktion
- Betriebsanleitung
- EG-Konformitätserklärung

WARUM CE-KENNZEICHNUNG?

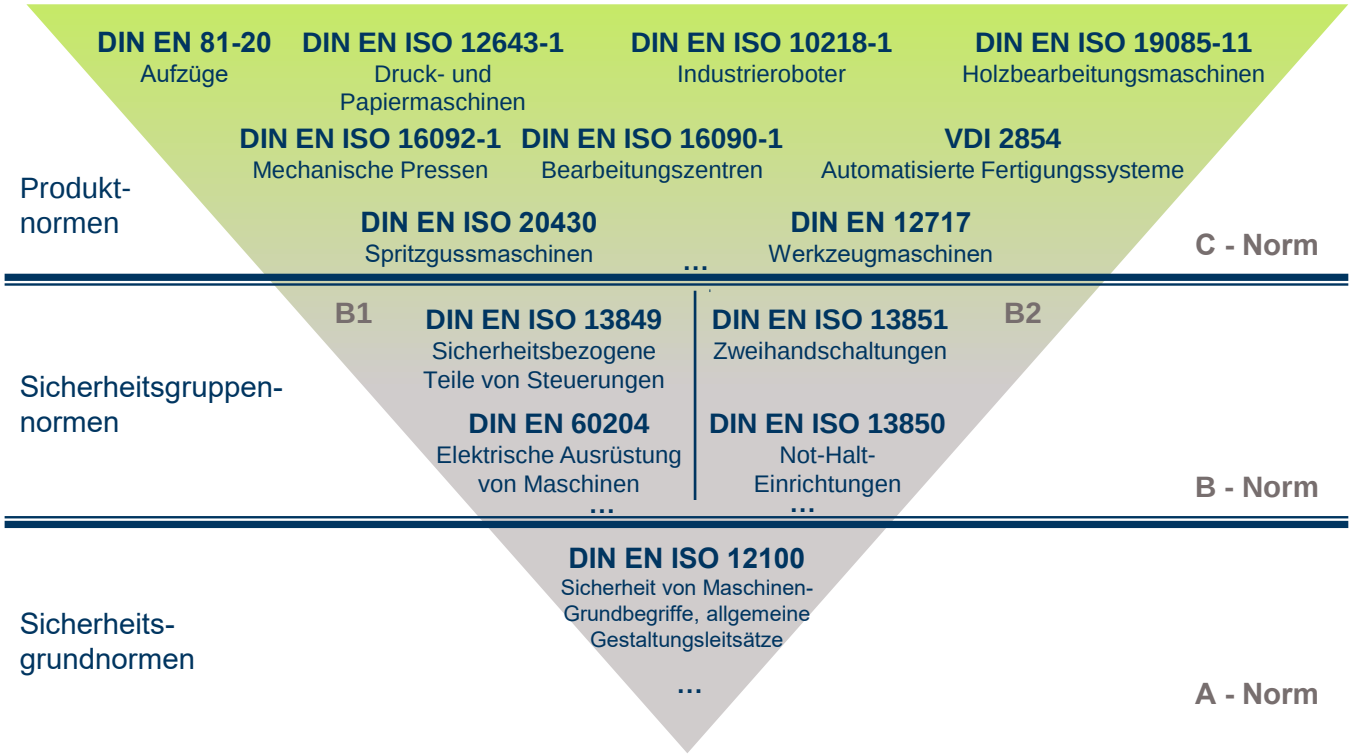
- **Ziele der EU:**
  - **Freier Warenverkehr**
  - Freier Kapitalverkehr
  - Freier Dienstleistungsverkehr
  - Freier Personenverkehr
- **Freier Warenverkehr von Maschinen und Anlagen erfordert:**
  - Vereinheitlichung / Harmonisierung der **Beschaffenheitsanforderungen** für Maschinen
  - Erhalt und Fortentwicklung des in den einzelnen Mitgliedstaaten erreichten hohen **Sicherheitsniveaus** dieser Maschinen
- **Durchsetzung dieser Ziele durch:**
  - Aufgabe/Zurücknahme nationaler Richtlinien
  - **EG-Richtlinien (Maschinen-VO (2023/1230), EMV-RL (2014/30/EU), Niederspannungs-RL (2014/35EU))**
  - Harmonisierte europäische Normen
  - Übernahme in nationales Recht der Mitgliedsstaaten
  - CE = Communauté Européenne

Der **Hersteller** sichert durch das Anbringen des CE-Zeichens zu, dass seine Maschine den entsprechenden Vorschriften genügt. Außerdem bestätigt er, dass er die vorgeschriebene Risikobewertung durchgeführt hat.

DIE EUROPÄISCHE NORMUNG



HARMONISIERTE NORMEN



Sind für eine Maschinengruppe noch keine C-Normen vorhanden, müssen die Sicherheitseinrichtungen in Eigenverantwortung nach den A- und B-Normen (und ggf. nationalen Normen) umgesetzt werden.

GRUNDLAGEN DER SICHERHEITSTECHNIK

- Einführung
- Gesetzliche Regelung
- **Begriffe und Definitionen**
- Risikobeurteilung
- Konstruktion
- Betriebsanleitung
- EG-Konformitätserklärung

DEFINITION RISIKO, GEFAHR UND SICHERHEIT - DIN EN ISO 12100

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes.

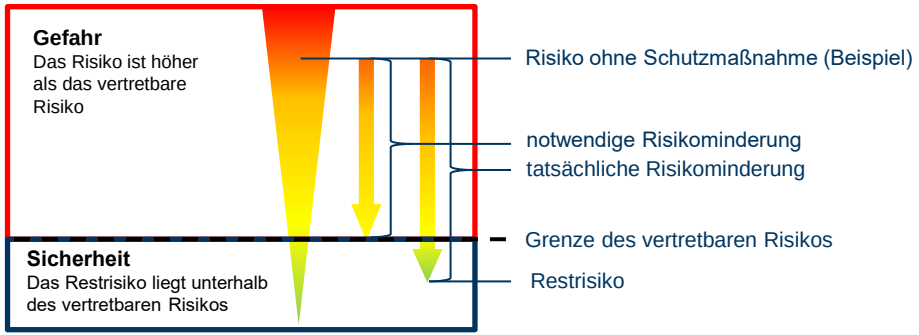
Gefährdung

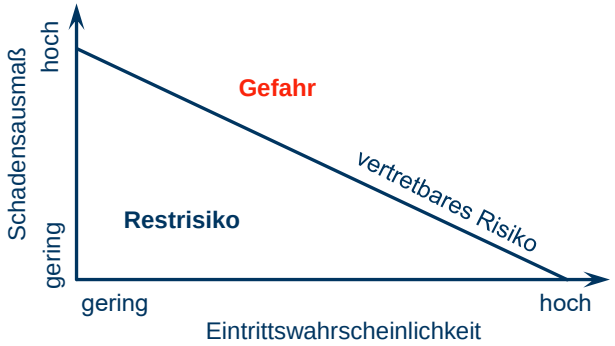
Potentielle Schadensquelle. Spezifizierbar durch Ursprung (z.B. mechanische oder elektrische Gefährdung)
oder Art des erwarteten Schadens (z.B. Gefährdung durch Schneiden, Gefährdung durch Feuer)

Vertretbares Risiko / Restrisiko

Vertretbares Risiko* ist das annehmbare Risiko, das in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird. Restrisiko ist das Risiko, das verbleibt, nachdem Maßnahmen zur Risikominderung getroffen wurden.

* Das vertretbare Risiko wird vom Hersteller der Maschine vor der Risikoeinschätzung festgelegt und begründet.





SICHERHEITSTECHNISCHE BEGRIFFE (1)

Begriff	Bedeutung
Zuverlässigkeit	Zuverlässigkeit ist die Fähigkeit eines Systems, eine **geforderte Funktion** unter **festgelegten Bedingungen** und für einen **vorgegebenen Zeitraum** ohne Ausfall zu erfüllen.
Verfügbarkeit	Die Verfügbarkeit ist eine statistische **Maßzahl für die Zuverlässigkeit**. Die Verfügbarkeit V ist die Wahrscheinlichkeit, dass sich ein System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand befindet. **V = MTBF / (MTBF + MDT)**
Ausfallzeit, Ausfalldauer	Die Ausfallzeit oder Ausfalldauer eines Systems ist die zufällig verteilte Zeitspanne zwischen dem Zeitpunkt des Ausfalls und dem Zeitpunkt, zu dem sie wieder in Betrieb genommen werden kann. Zur Beurteilung einer Betrachtungseinheit wird die mittlere Ausfalldauer, **mean down time (MDT)**, herangezogen. **MDT = mittlere Fehlerentdeckungszeit + mittlere Fehlerreparaturzeit**
Ausfallabstand	Der Ausfallabstand ist die zufällig verteilte Zeitspanne zwischen zwei Ausfällen eines nach Ausfall wieder instandgesetzten Systems. Zur Beurteilung eines Systems wird der mittlere Ausfallabstand, **mean time between failures (MTBF)**, herangezogen.
Validierung	Bestätigen aufgrund einer Untersuchung und durch bereitstellen eines objektiven Nachweises (z.B. Tests), dass die besonderen Anforderungen für eine speziell beabsichtigte Verwendung erfüllt worden sind.
Verifikation	Objektiver Nachweis, dass festgelegte Anforderungen erfüllt worden sind (z.B. durchführen alternativer Berechnungen). **Wurden Forderungen korrekt umgesetzt?**
Falsifizierung	Ausschluss von Produkteigenschaften (z. B. Sicherheitseigenschaften / Gefahrenausschluss)

Quelle: VDI/VDE 2180, DIN EN ISO 12100, DIN EN ISO 13849-1

SICHERHEITSTECHNISCHE BEGRIFFE (2)

Begriff	Bedeutung
fail safe	Fähigkeit eines Systems, beim Auftreten bestimmter Zustände **im sicheren Zustand zu bleiben** oder unmittelbar in einen anderen **sicheren Zustand überzugehen**.
Redundanz	Redundanz ist das Vorhandensein von mehr funktionsbereiten technischen Mitteln als zur Erfüllung der vorgesehenen Funktionen notwendig sind, um erhöhte Sicherheits- oder Verfügbarkeitsanforderungen zu erfüllen. Redundanz ist die Voraussetzung für Fehlertoleranz. ▪ **Homogene Redundanz**: Die redundanten Kanäle sind identisch realisiert. ▪ **Diversitäre (inhomogene) Redundanz**: Die redundanten Kanäle sind unterschiedlich aufgebaut. ▪ **Dynamische Redundanz**: Ersatzkomponenten werden erst im Fehlerfall aktiviert (kalte Reserve). ▪ **Statische Redundanz**: Gleichzeitiger Einsatz aller Komponenten (heiße Reserve).
Diversität	Vorhandensein mehrerer verschiedener Komponenten mit gleichen Soll-Eigenschaften, Konstruktion der Einzelkomponenten durch verschiedene Entwicklungsteams, um systematische Fehler auszuschließen.
Einfehlersicherheit	Das Vorhandensein eines einzelnen Fehlers wird sicher erkannt, erst bei Häufung von mehreren Fehlern kann ein Verlust der Sicherheitsfunktion eintreten.

Quelle: VDI/VDE 2180

GRUNDLAGEN DER SICHERHEITSTECHNIK

- Einführung
- Gesetzliche Regelung
- Begriffe und Definitionen
- **Risikobeurteilung**
- Konstruktion
- Betriebsanleitung
- EG-Konformitätserklärung

FORDERUNGEN DER MASCHINENRICHTLINIE

Forderung nach Funktion

Die Maschine muss ihrer Funktion gerecht werden.

Forderung nach Sicherheit

Maschinen müssen so konstruiert sein, dass Personen zu keiner Zeit einer Gefährdung ausgesetzt sind.

➡ **Durchführung einer <u>Risikobeurteilung</u>**

! Sicherheit muss in dem gesamten Lebenszyklus einer Maschine gewährleistet sein. !

Gesamten Lebenszyklus betrachten

- Transport
- Montage
- Betrieb
- Demontage
- Entsorgung

Alle Arbeiten berücksichtigen

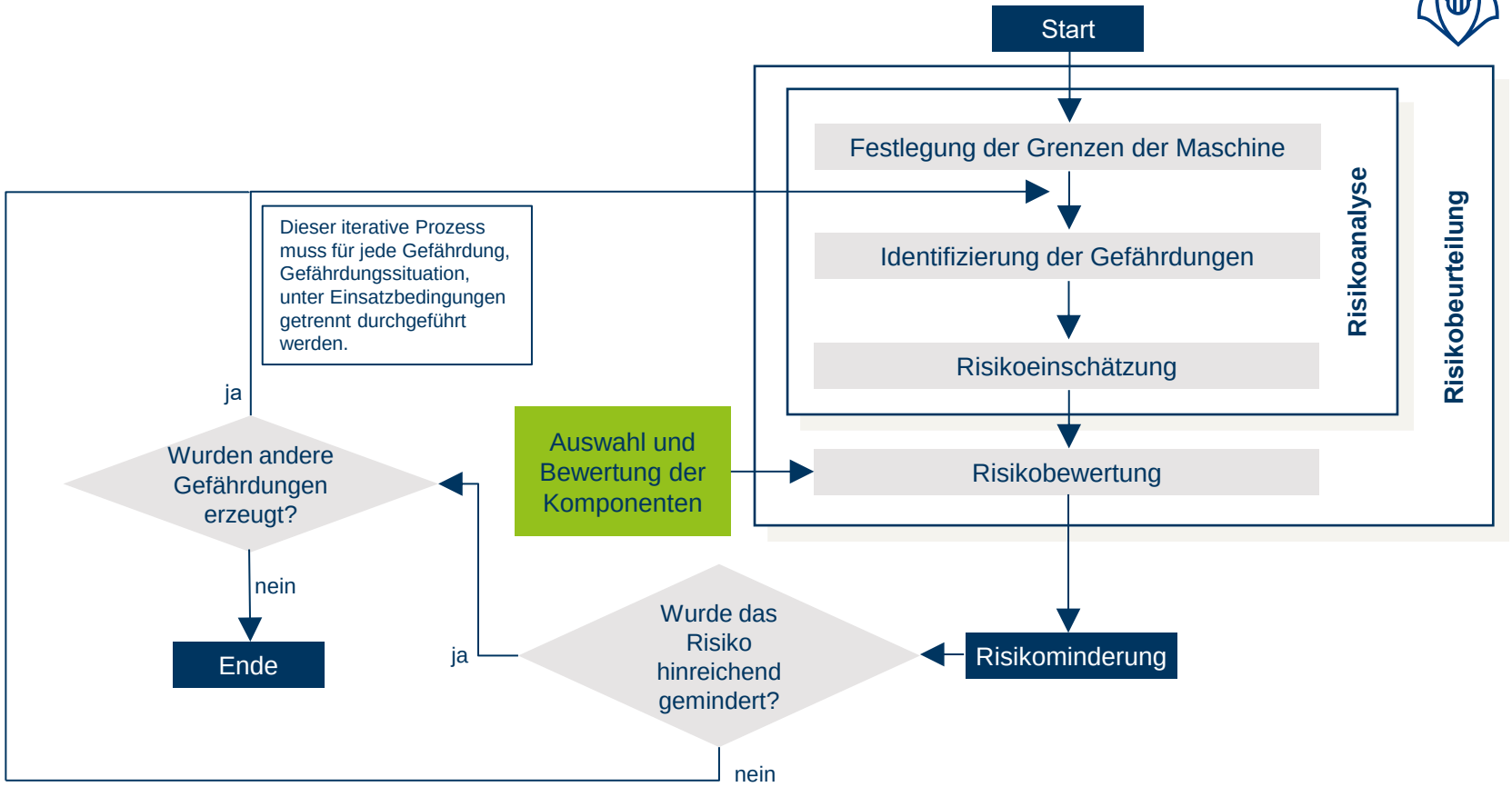
- Normalbetrieb einschließlich
  - Reinigung
  - Wartung
  - Instandhaltung etc.
- Störungsbeseitigung

Alle Situationen berücksichtigen

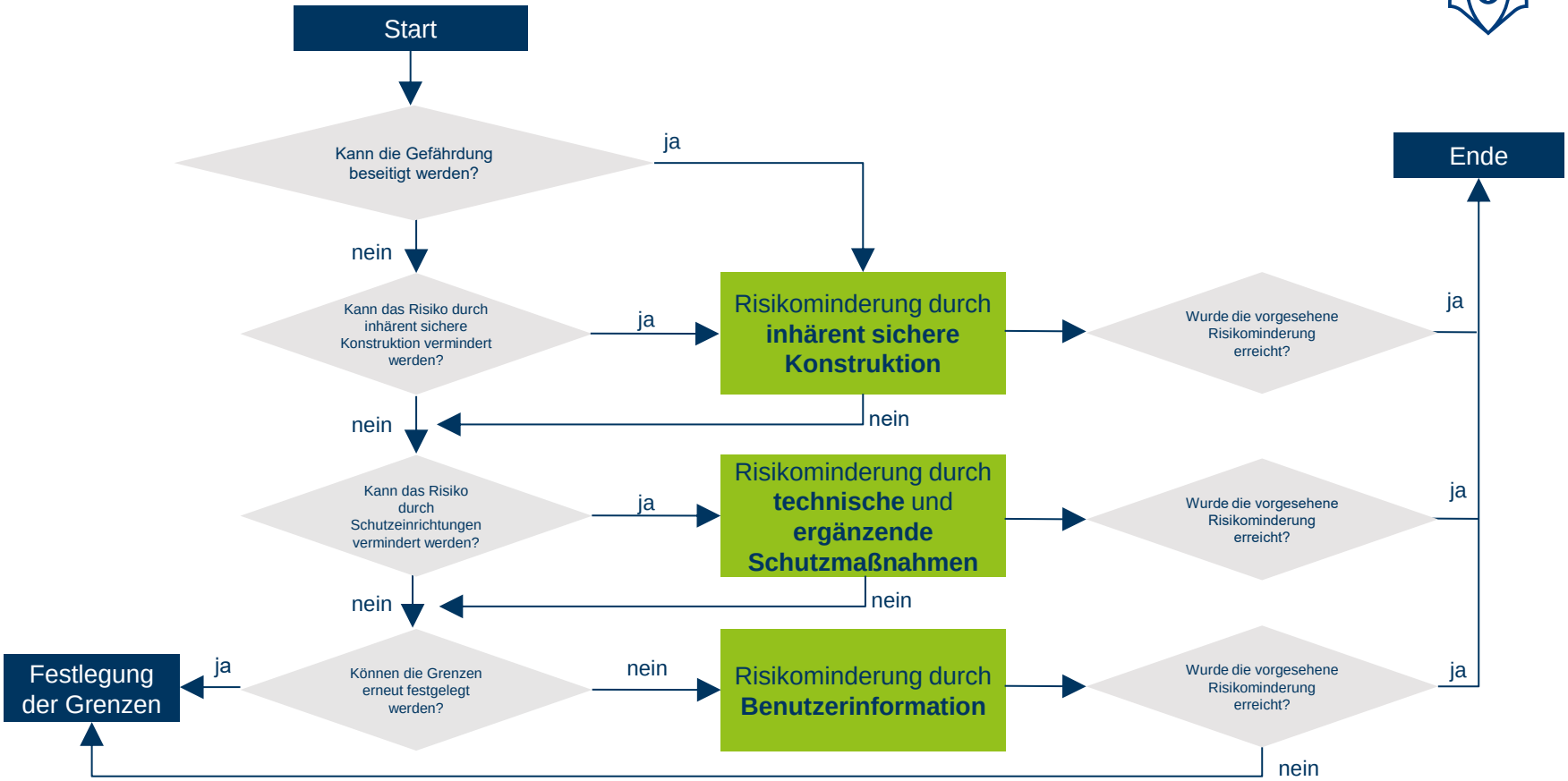
- Bestimmungsgemäße Verwendung
- Vernünftigerweise vorhersehbare Fehlanwendung

In Anlehnung an: CE-Coach

RISIKOBEURTEILUNG



RISIKOMINDERUNG



RISIKOANALYSE

Festlegung der Grenzen

- Verwendungsgrenzen (Betriebsarten, Anwender, Einsatzbereich, …)
- Räumliche Grenzen (Bewegungsraum, Platzbedarf für Installation, …)
- Zeitliche Grenzen (voraussichtliche Lebensdauer, Wartungszyklen, …)

Gefährdungs-ermittlung

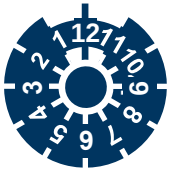
- Physikalische (mechanische, elektrische, …) und chemische Gefährdungen *(siehe DIN EN ISO 12100 Anhang B)*
- Gefährdung durch Benutzereingriffe an der Maschine
- Menschliches Versagen, Unaufmerksamkeit, Ablenkung durch andere Personen
- Ausfall von Funktionen/Bauteilen (**Fehlerbaum**, FMEA)
- Leistungsverlust der Maschine

Risiko-einschätzung

- Schwere des möglichen Schadens
- Häufigkeit und Dauer der Gefahrensituation, Wahrscheinlichkeit des Auftretens
- Möglichkeiten zur Verminderung oder Begrenzung des Schadens → **Risikograph**

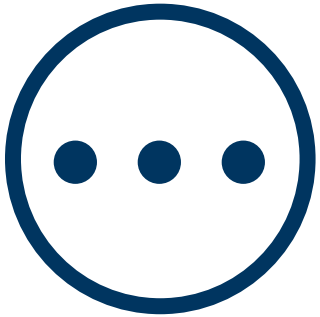
FESTLEGUNG DER GRENZEN EINES ROBOTERSYSTEMS

- **Verwendungsgrenzen:**
  - Betriebsarten, Eingriffsmöglichkeiten für die Bedienpersonen
- **Räumliche Grenzen:**
  - Bewegungsraum, Platzbedarf
- **Zeitliche Grenzen:**
  - Lebensdauer der Einzelkomponenten



FESTLEGUNG DER GRENZEN EINES ROBOTERSYSTEMS

- **Sonstige Grenzen:**
  - Eigenschaften des zu verarbeitenden Materials
  - Der erforderliche Reinlichkeitsgrad
    (z.B. Reinraumbedingungen, oder Informationen zur Sauberhaltung)
  - Umgebungsbedingungen z.B.:
    - Mindest- und Höchsttemperaturen
    - Einsatz im Innenraum oder im Freien
    - nur unter trockenen und/oder nassen Witterungsbedingungen
    - bei direkter Sonneneinstrahlung
    - staub- und nässeverträglich



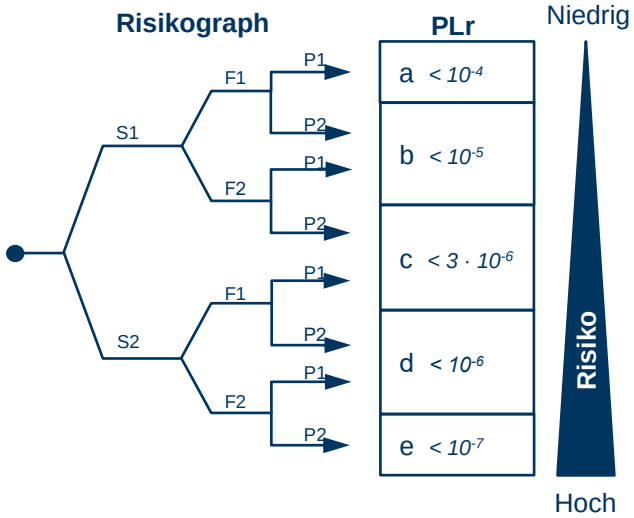
MAßNAHMEN ZUR RISIKOMINIMIERUNG

- **Konstruktive Maßnahmen:**
  - Reduzierung von Stressfaktoren (Überdimensionierung von Bauteilen)
  - Verwendung von Bauteilen mit speziellen, unveränderbaren Eigenschaften (z. B. Masse)
  - Nachweis, dass bestimmte Fehler nicht auftreten können (Sollbruchstellen)
  - Nachweis über die Beherrschung der Fehlerauswirkung (fail-safe, Redundanz)
- **Technische Maßnahmen:**
  - Trennende- und/oder nichttrennende Schutzeinrichtungen
  - Verhindern eines unerwarteten Anlaufs der Maschine und stillsetzen im Notfall
  - Fehlererkennende, -tolerierende Systeme, Selbstüberwachung, Meldesysteme
  - Cybersicherheit
- **Organisatorische Maßnahmen:**
  - Regelmäßige Inspektion
  - Personalschulung (Feuerübungen, Verwendung persönlicher Schutzausrüstung)
  - Nachprüfung durch unabhängiges Personal

Informationen hierzu: DIN EN ISO 12100 – Kapitel 6

RISIKOGRAPH FÜR ALLGEMEINE TECHNISCHE ANWENDUNGEN

Zur Einteilung unterschiedlicher sicherheitstechnischer Leistungsfähigkeit werden in der DIN EN ISO 13849-1 sogenannte erforderliche **Performance Level required (PL_r)** definiert.
Die fünf PL_r (a, b, c, d, e) stehen für unterschiedliche die mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde (PFH).
Dabei wird die **Kette „Sensor“, „Logik“ und „Aktor“** je Sicherheitsfunktion betrachtet.



S – Schwere der Verletzung
- S1 - Leichte Verletzung
- S2 - Schwere irreversible Verletzung oder Tod einer oder mehrerer Personen

F – Häufigkeit / Dauer der Gefährdung
- F1 - Selten bis öfter und/oder kurz
- F2 - Häufig bis dauernd und/oder lang

P – Möglichkeit zur Vermeidung von Gefährdungen
- P1 - Möglich unter bestimmten Bedingungen
- P2 - Kaum möglich

BESTIMMUNG DER SICHERHEITS-ANFORDERUNG NACH DIN EN ISO 13849-1

Kategorie	Kurzbeschreibung	Systemverhalten	Prinzip zum Erreichen der Sicherheit	$MTTF_d$	DC	CCF	max. erreichbarer PL
B	Steuerungen gemäß dem **Stand der Technik**	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch Auswahl von Bauteilen charakterisiert	niedrig bis mittel	nicht relevant	nicht relevant	b
1	Verwendung **sicherheits-technisch bewährter** Komponenten	Wie B, sicherheitsbezogene Zuverlässigkeit größer		hoch	nicht relevant	nicht relevant	c
2	**Prüfung** der Sicherheitsfunktion durch die Maschinensteuerung	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen.	Überwiegend durch die Struktur charakterisiert	niedrig bis hoch	niedrig bis mittel 60 – 99%	mind. 65 Punkte	d
3	**Redundanz** mit partieller Fehlererkennung, soweit nach dem Stand der Technik praktikabel	Ein einzelner Fehler führt nicht zum Verlust der Sicherheit (**Einfehlersicherheit**).	Überwiegend durch die Struktur charakterisiert (Redundanz)	niedrig bis hoch	niedrig bis mittel 60 – 99%	mind. 65 Punkte	e
4	Selbstüberwachung, **frühzeitige Fehlererkennung**	Eine Fehlerhäufung führt nicht zum Verlust der Sicherheit.		hoch	hoch >99%	mind. 65 Punkte	e

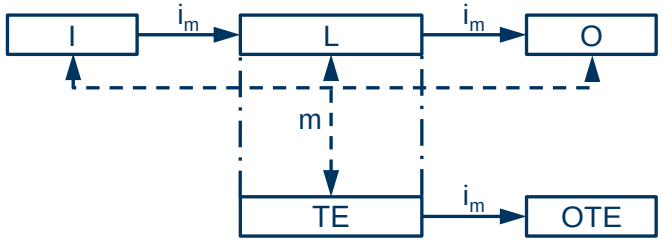
DC (Diagnostic Coverage): Fehleraufdeckungsgrad (low: 60% – 90 %, medium 90% – 99%, high > 99%)
CCF (Common Cause Failure): Ausfallsicherheit infolge gemeinsamer Ursache (> 65 von 100 Punkten)
MTTFd (Mean Time to Failure dangerous): Zeit bis zum gefahrbringenden Ausfalls Low: 3 bis 10 Jahre, Medium: 10 bis 30 Jahre, High: 30 bis 100 Jahre

Quelle: Angelehnt an DIN EN ISO 13849-1 Tabelle 5

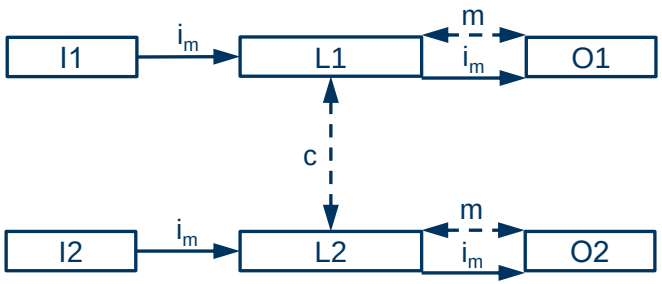
GRUNDSTRUKTUREN DER KATEGORIEN

Kategorie B und Kategorie 1:

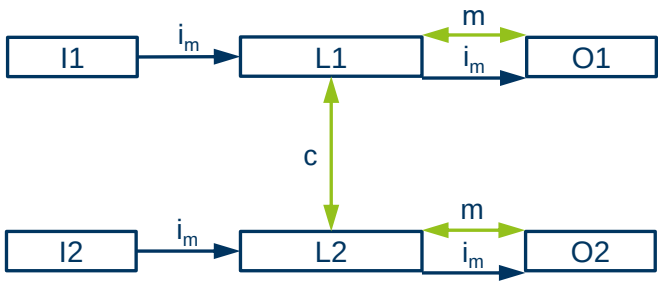
Kategorie 2: Integrierte Testeinheit (Beobachter)



Kategorie 3: Redundanz mit Logik- und Ausgangsüberwachung



Kategorie 4: Redundanz mit intensiver Überwachung



I = Sensor, Eingangssignal
L = Logik, Sicherheitskreis
O = Ausgangssignal, Hauptschütz
TE = Testeinheit

OTE = Ausgang der Testeinheit
i_m = Verbindung
m = Überwachung
c = Kreuzvergleich

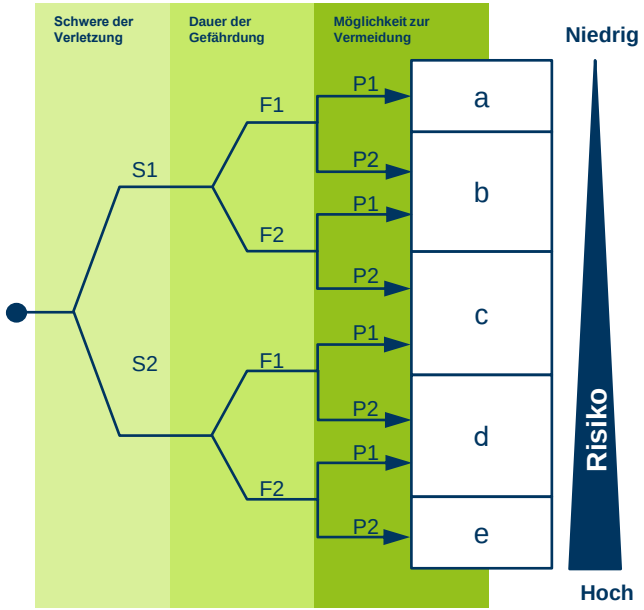
vernünftigerweise durchführbare Fehlererkennung

höherer Diagnosedeckungsgrad

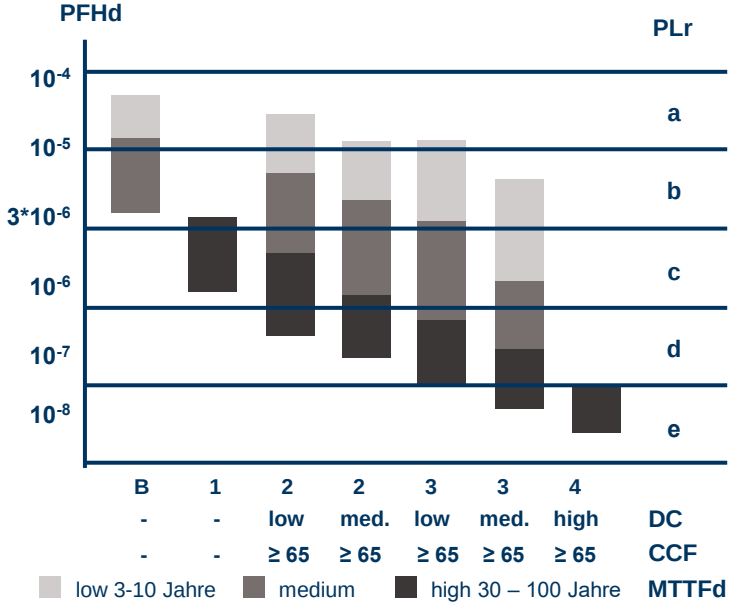
Quelle: DIN EN ISO 13849-1

STEUERUNGSTECHNISCHE MAßNAHMEN (KATEGORIEN B - 4)

Erforderlicher Performance Level PLr



Erreichbarer Performance Level PL



PFHd (Probability of dangerous Failure per Hour): **Berechnete** Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde

DC (Diagnostic Coverage): Fehleraufdeckungsgrad (low: 60% – 90 %, medium 90% – 99%, high > 99%)

CCF (Common Cause Failure): Ausfallsicherheit infolge gemeinsamer Ursache (> 65 von 100 Punkten)

MTTFd (Mean Time to Failure dangerous): Zeit bis zum gefährlichen Ausfall einer Komponente

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (1)

An einer **CNC-Drehmaschine** wird von Hand ein Werkstück in das Spannfutter eingelegt, der Arbeitsvorgang wird gestartet und nach Ablauf des Bearbeitungsvorgangs wird das Werkstück wieder von Hand entnommen. Die Schutztür wird dazu zyklisch betätigt (Zustand ohne Schutzmaßnahmen).

Bildquelle: www.stahlwerk-cnc.com

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (2)

1. Festlegen der Grenzen der Maschine

- **Verwendungsgrenzen:** Die bestimmungsgemäße Verwendung ist das Drehen von Metallteilen, die auf die Größe der Werkzeuge und des Arbeitsbereiches begrenzt sind. Die Maschine kommt nur im gewerblichen Bereich zum Einsatz, sie kann nur von eingewiesenem Personal bedient werden.
- **Räumliche Grenzen:** Definieren sich über die Systemgrenzen, die durch die Einzelmaschine klar gegeben sind.
- **Zeitliche Grenzen:** Die Lebensdauer wird auf 20 Jahre festgelegt.

2. Gefährdungen identifizieren

- **Arbeitsbereich** als potentielle Gefahrenquelle

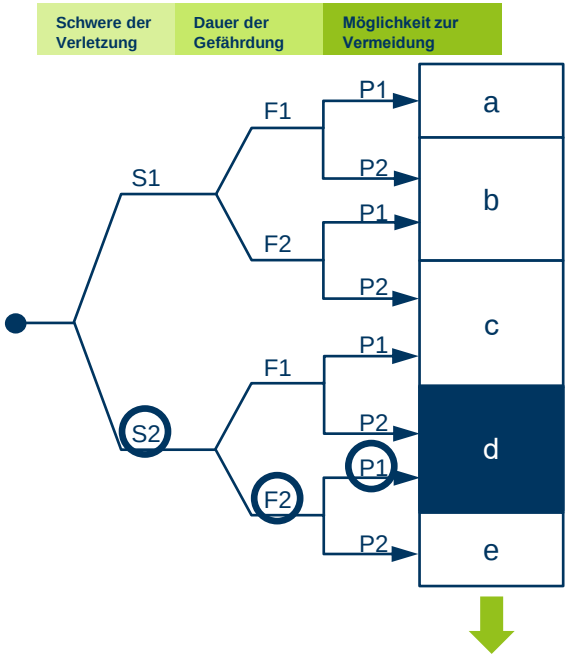
RISIKOANALYSE AM BEISPIEL DREHMASCHINE (3)

3. Risikoeinschätzung

In Anlehnung an: CE-Coach

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (4)

Performance Level required (PLr) für den Arbeitsbereich:



S1 Leichte Verletzung
S2 Schwere irreversible Verletzung oder Tod einer oder mehrerer Personen

F1 Selten bis öfter und/oder kurz
F2 Häufig bis dauernd und/oder lang

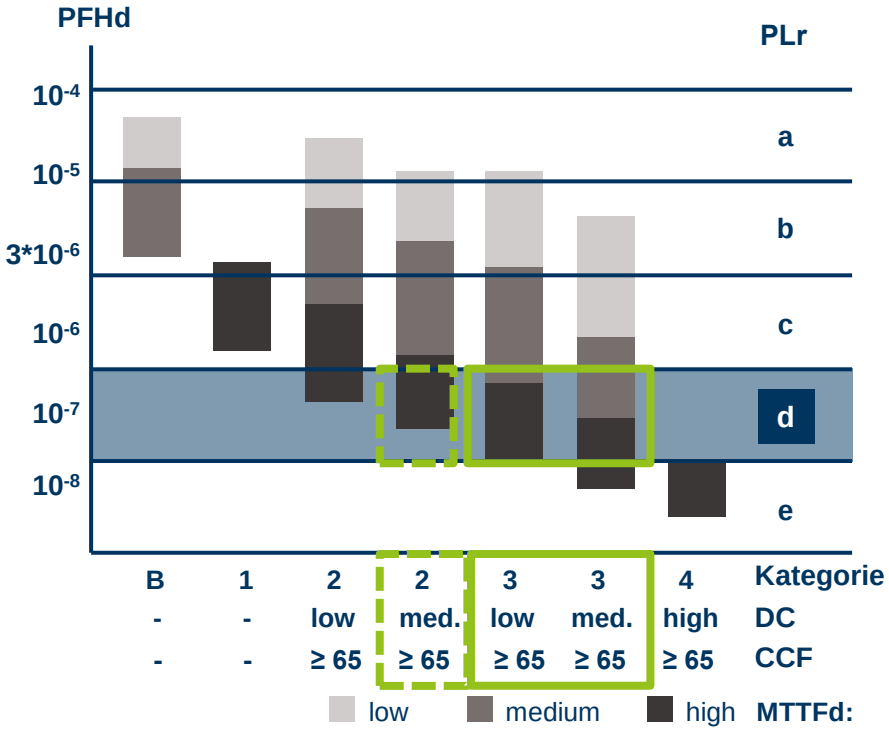
P1 Möglich unter bestimmten Bedingungen
P2 Kaum möglich

PLr = d
Besondere sicherheitsrelevante Maßnahmen erforderlich!

In Anlehnung an: CE-Coach

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (5)

Kategorie bestimmen für Performance Level PLr = d:



PFHd: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

DC: Fehleraufdeckungsgrad (low: 60% – 90 %, medium 90% – 99%, high > 99%)

CCF: Ausfall infolge gemeinsamer Ursache (> 65 von 100 Punkten → sicher bzgl. gem. Ursache)

MTTFd: Zeit bis zum gefährlichen Ausfall
Low: 3 bis 10 Jahre
Medium: 10 bis 30 Jahre
High: 30 bis 100 Jahre

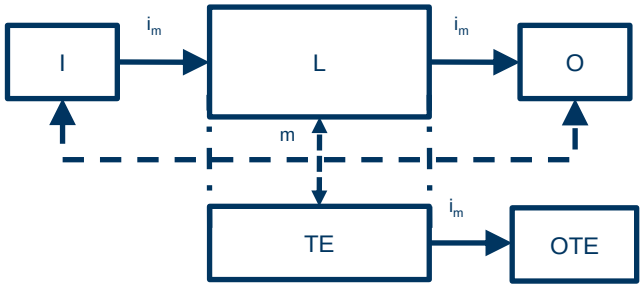
Zur Erfüllung der Sicherheitsfunktion kommen Steuerungskomponenten der **Kategorie 2 <u>oder</u> 3** in Frage

In Anlehnung an: CE-Coach

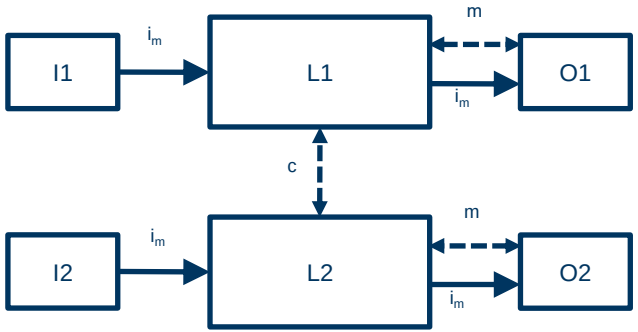
RISIKOANALYSE AM BEISPIEL DREHMASCHINE (6)

Sicherheitsfunktion ableiten:

Kategorie 2
Integrierte Testeinheit



Kategorie 3
Redundante Logik- und Ausgangsüberwachung



I = **Sensor**: Positionsschalter für die Tür mit Öffner und Schließer
L = **Logik, Sicherheitsrelais**: Motor nur einschaltbar, wenn Tür zu
O = **Ausgang**: Motorschütz mit Ruhelageausgang als Öffner
TE = **Testeinheit**: Alarmlampe, wenn Motor bei geöffneter Tür läuft
➔ manuelles Ausschalten über Hauptschalter.
Die Maschine sollte bei einem Funktionsfehler automatisch in den sicheren Zustand überführt werden.
Sicherheitstest bei jedem Einschalten des Motors + zyklische Überwachung.

I1 = Positionsschalter für die Tür
I2 = 2. Rollenschalter
L1 + L2 = zweikanaliges Sicherheitsrelais
O1 + O2 = Motorschütz (2-kanalig)

In Anlehnung an: CE-Coach

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (7)

Leistungsfähigkeit der Sicherheitsfunktion prüfen (Kategorie 2):

Berechnung der Ausfallwahrscheinlichkeit / Stunde (**PFHd**) durch Herstellerdaten für Sensor, Logik und Aktor!

Element	DC	MTTFd	CCF
Sensor I: Schalter an der Schutztür Positionsschalter	90% = medium	13 Jahre = medium	70
Logik L: Sicherheitsrelais	> 99% = high	35 Jahre = high	70
Aktor O: Motorschütz	90% = medium	434 Jahre = high	95
Gesamt	medium	medium	> 65 Punkte

PFHd: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

DC: Fehleraufdeckungsgrad (low: 60% – 90 %, medium 90% – 99%, high > 99%)

CCF: Ausfall infolge gemeinsamer Ursache (> 65 von 100 Punkten → sicher bzgl. gem. Ursache)

MTTFd: Zeit bis zum gefährlichen Ausfall

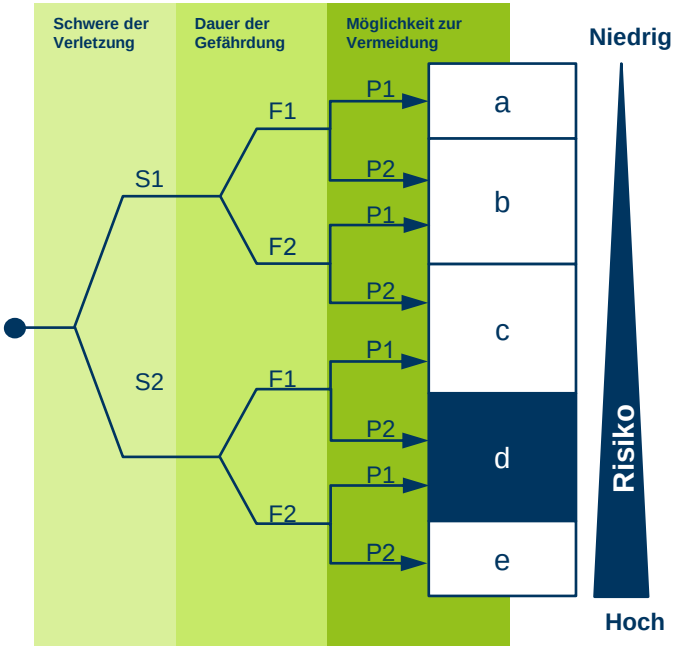
Mit Software* ermittelter **PFHd** = $2{,}59 \cdot 10^{-6}$
→ erreichter PL = c
*bspw. mit Safety Calculator PAScal (Fa. Pilz)

Erforderlich: d
→ Kategorie 3 wählen

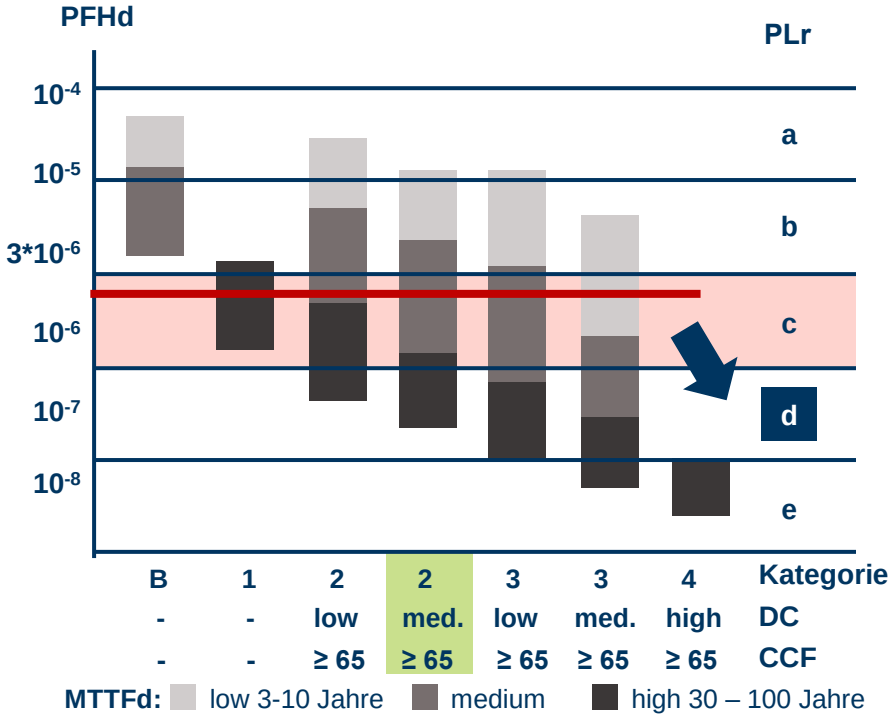
In Anlehnung an: CE-Coach

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (8)

Erforderlicher Performance Level PLr



Erreichbarer Performance Level PL



In Anlehnung an: CE-Coach

RISIKOANALYSE AM BEISPIEL DREHMASCHINE (9)

Leistungsfähigkeit der Sicherheitsfunktion prüfen (Kategorie 3):

Berechnung der Ausfallwahrscheinlichkeit / Stunde (**PFHd**) durch Herstellerdaten für Sensor, Logik und Aktor!

Element	DC	MTTFd	CCF
Sensor I1 (Positionsschalter) + I2 (Rollenschalter)	90% = medium	I1: 13 Jahre, → medium I2: 65 Jahre → high	70%
Logik L1+L2	> 99% = high	50 Jahre	85%
Aktor O1+O2	90% = medium	434 Jahre → high	95%
Gesamt	medium	medium	> 65 Punkte

PFHd: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

DC: Fehleraufdeckungsgrad (low: 60% – 90 %, medium 90% – 99%, high > 99%)

CCF: Ausfall infolge gemeinsamer Ursache (> 65 von 100 Punkten → sicher bzgl. gem. Ursache)

MTTFd: Zeit bis zum gefährlichen Ausfall

Die erneute Risikoeinschätzung für **Kategorie 3** ergibt: **PFHd** = $2{,}9 \cdot 10^{-7}$
Die Sicherheitsfunktion erreicht **PL = d**

In Anlehnung an: CE-Coach

GRUNDLAGEN DER SICHERHEITSTECHNIK

- Einführung
- Gesetzliche Regelung
- Begriffe und Definitionen
- Risikobeurteilung
- **Konstruktion**
- Betriebsanleitung
- EG-Konformitätserklärung

GRUNDSÄTZE FÜR DIE INTEGRATION DER SICHERHEIT (1)

- Die Maschine ist so zu konstruieren und zu bauen, dass sie ihrer Funktion gerecht wird:
  - unter den vorgesehenen Bedingungen
  - unter Berücksichtigung einer vernünftigerweise vorhersehbaren Fehlanwendung der Maschine (z. B. Unachtsamkeit oder Unaufmerksamkeit)

- Betrieb, Einrichtung und Wartung ohne Personengefährdung möglich

- Maßnahmen müssen darauf abzielen, Risiken während der voraussichtlichen Lebensdauer (inkl. Transport, Montage, Demontage und Entsorgung) der Maschine zu beseitigen.

Quelle: Maschinenverordnung (EU) 2023/1230 – Anhang III

GRUNDSÄTZE FÜR DIE INTEGRATION DER SICHERHEIT (2)

- **Bei der Wahl der angemessenen Lösungen sind die folgenden Grundsätze in der angegebenen Reihenfolge anzuwenden:**
  1. Beseitigung bzw. Minimierung der Risiken so weit möglich
     - Beispiel: Sicherstellung der Stabilität der Maschine durch ihre Form
  2. Ergreifen notwendiger Schutzmaßnahmen gegen Risiken, die sich nicht beseitigen lassen
     - Beispiel: Schutzzaun
  3. Unterrichtung des Benutzers über die Restrisiken; Hinweis auf eventuell erforderliche spezielle Ausbildung, Einarbeitung oder persönliche Schutzausrüstung
     - Beispiel: Warnlampe oder Warnton

GRUNDSÄTZE FÜR DIE INTEGRATION DER SICHERHEIT (3)

- Verhinderung einer missbräuchlichen Verwendung
- Belastungen durch notwendige persönliche Schutzausrüstung reduzieren
- Wesentliche Spezialausrüstungen und Zubehörteile müssen mitgeliefert werden.

KONSTRUKTION DER MASCHINE IM HINBLICK AUF DIE HANDHABUNG

- Die Maschine oder jedes ihrer Bestandteile müssen
  - sicher gehandhabt und transportiert werden können,
  - so verpackt oder konstruiert sein, dass sie sicher und ohne Beschädigung gelagert werden können.

- Beim Transport müssen ungewollte Lageveränderungen und Gefährdungen durch mangelnde Standsicherheit ausgeschlossen sein, wenn die Handhabung entsprechend der Betriebsanleitung erfolgt

- Wenn sich die Maschine nicht von Hand bewegen lässt, muss sie eine der folgenden Merkmale aufweisen:
  - Befestigungseinrichtungen für Lastaufnahmeeinrichtungen,
  - Möglichkeit, solche Befestigungseinrichtungen anzubringen,
  - Die Form ist so gewählt, dass übliche Lastaufnahmeeinrichtungen leicht angelegt werden können.

ERGONOMIE

- Minimierung von Belästigung, Ermüdung sowie körperliche und psychische Fehlbeanspruchung

- Berücksichtigung ergonomischer Prinzipien wie:
  - Möglichkeit der Anpassung an die Unterschiede in den Körpermaßen, der Körperkraft und der Ausdauer
  - Ausreichender Bewegungsfreiraum für die Körperteile
  - Vermeidung eines von der Maschine vorgegebenen Arbeitsrhythmus
  - Vermeidung von Überwachungstätigkeiten, die dauernde Aufmerksamkeit erfordern
  - Anpassung der Mensch-Maschine-Schnittstelle an die voraussehbaren Eigenschaften des Bedienungspersonals

SICHERHEIT UND ZUVERLÄSSIGKEIT VON STEUERUNGEN

- Steuerungen müssen Gefährdungssituationen ausschließen. Insbesondere müssen die folgenden Punkte beachtet werden:
  - Betriebsbeanspruchungen und Fremdeinflüsse
  - Keine Gefährdung durch Defekt der Hardware oder Software
  - Keine Gefährdung durch Fehler in der Logik des Steuerkreises
  - Keine Gefährdung durch Vernünftigerweise vorhersagbare Bedienungsfehler
  - Nicht unbeabsichtigt in Gang zu setzen
  - Keine unkontrollierte Änderung der Parameter der Maschine möglich, wenn dies zu einer Gefährdungssituation führen kann
  - Stillsetzen der Maschine nicht vermeidbar, wenn ein solcher Befehl bereits erteilt wurde
  - Herausschleudern oder Herabfallen beweglicher Teile
  - Automatisches oder manuelles Stillsetzen von beweglichen Teilen darf nicht verhindert werden
  - Nichttrennende Schutzeinrichtungen müssen uneingeschränkt funktionsfähig bleiben oder aber ein Stillsetzen auslösen
- Kabellose Steuerungen

STELLTEILE

- Deutlich sichtbar und erkennbar
- Betätigung sicher, unbedenklich, schnell und eindeutig
- Betätigen des Stellteils mit Steuerwirkung kohärent
- Außerhalb der Gefahrenbereiche (Ausnahme: NOT-Halt)
- Keine zusätzlichen Risiken durch Betätigung
- Falls mit Gefährdung verbunden, nur absichtliche Betätigung möglich
- Standhaltung vorhersehbaren Beanspruchungen
- Eindeutige Anzeige bei mehreren verschiedenen Wirkungen
- Berücksichtigung ergonomischer Prinzipien
- Notwendigen Anzeigeeinrichtungen und Hinweisen müssen vorhanden und einsehbar sein.
- …

STILLSETZEN

- **Normales Stillsetzen**
  - Befehlseinrichtung zum sicheren Stillsetzen der gesamten Maschine muss vorhanden sein
  - Jeder Arbeitsplatz muss mit entsprechender Befehlseinrichtung ausgestattet sein
  - Stillsetzen muss Vorrang vor in Gang setzen haben
  - Unterbrechung der Energieversorgung nach Stillsetzen

- **Betriebsbedingtes Stillsetzen**
  - Wenn Unterbrechung der Energieversorgung nicht möglich, muss eine Überwachung stattfinden

STILLSETZEN IM NOTFALL

- Jede Maschine muss mit einem oder mehreren NOT-HALT-Befehlsgeräten ausgerüstet sein
- Das NOT-HALT-Befehlsgerät muss
  - deutlich erkennbare, gut sichtbare und schnell zugängliche Stellteile haben,
  - den gefährlichen Vorgang möglichst schnell zum Stillstand bringen, ohne dass dadurch zusätzliche Risiken entstehen,
  - erforderlichenfalls bestimmte Sicherungsbewegungen auslösen oder ihre Auslösung zulassen.
- Wiederanlauf erst nach Freigabe möglich
- Die NOT-HALT-Funktion muss unabhängig von Betriebsart, jederzeit verfügbar und betriebsbereit sein und Vorrang vor allen anderen Funktionen haben.
- NOT-HALT-Befehlsgeräte müssen andere Schutzmaßnahmen ergänzen, aber dürfen nicht an deren Stelle treten.

DIN EN ISO 13850

INGANGSETZUNG

- Nur durch absichtliches Betätigen einer hierfür vorgesehenen Befehlseinrichtung
  - Wiederingangsetzung nach einem Stillstand
  - Wesentliche Änderung des Betriebszustands

- Wiederingangsetzung oder die Änderung des Betriebszustands durch absichtliches Betätigen einer anderen Einrichtung als der hierfür vorgesehenen Befehlseinrichtung möglich, falls keine Gefährdung

- Bei Maschinen im Automatikbetrieb nach einer Abschaltung oder Änderung des Betriebszustands ohne Bedienereingriff möglich, falls keine Gefährdung

INGANGSETZUNG

- Nur durch absichtliches Betätigen einer hierfür vorgesehenen Befehlseinrichtung
  - Wiederingangsetzung nach einem Stillstand
  - Wesentliche Änderung des Betriebszustands

- Wiederingangsetzung oder die Änderung des Betriebszustands durch absichtliches Betätigen einer anderen Einrichtung als der hierfür vorgesehenen Befehlseinrichtung möglich, falls keine Gefährdung

- Bei Maschinen im Automatikbetrieb nach einer Abschaltung oder Änderung des Betriebszustands ohne Bedienereingriff möglich, falls keine Gefährdung

- Bei mehreren Bedienplätzen darf nur einer die Steuerhoheit zum Ingangsetzen besitzen (Stillsetzen sollte von allen Bedienplätzen möglich sein)

STÖRUNG DER ENERGIEVERSORGUNG

Ausfall, Wiederherstellung nach einem Ausfall oder Änderung der Energieversorgung darf nicht zu gefährlichen Situationen führen.

- Maschine darf nicht unbeabsichtigt in Gang gesetzt werden können und der automatische Wiederanlauf nach Wiederherstellung der Energieversorgung muss verhindert werden.
- Parameter dürfen sich nicht unkontrolliert ändern können, wenn dies zu Gefährdungssituationen führen kann
- Stillsetzen der Maschine darf nicht verhindert werden können, wenn der Befehl zum Stillsetzen bereits erteilt wurde
- Bewegliche Teile dürfen nicht herabfallen oder herausgeschleudert werden können
- Automatisches oder manuelles Stillsetzen von beweglichen Teilen jeglicher Art darf nicht verhindert werden
- Nichttrennende Schutzeinrichtungen müssen uneingeschränkt funktionsfähig bleiben oder aber einen Befehl zum Stillsetzen auslösen

MECHANISCHE GEFÄHRDUNGEN

- Verlust der Stabilität
- Bruchrisiko beim Betrieb
- Herabfallende oder herausgeschleuderte Objekte
- Oberflächen, Kanten und Ecken
- Kombinierte Maschinen
- Veränderliche Arbeitsumgebungen
- Bewegliche Teile
- Unkontrolliert bewegende Teile

SONSTIGE GEFÄHRDUNGEN

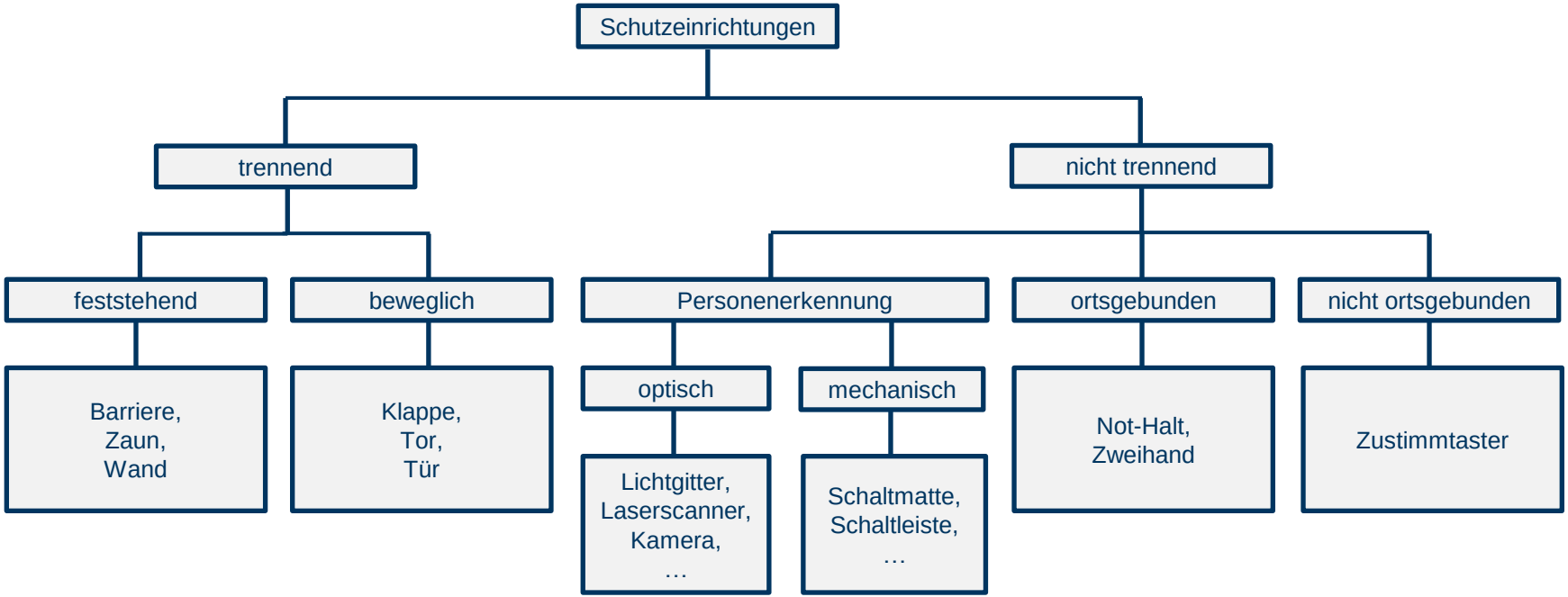
- Elektrische Energieversorgung, nichtelektrische Energieversorgung
- Statische Elektrizität
- Montagefehler
- Extreme Temperaturen
- Brand
- Strahlung von außen
- Explosion
- Lärm
- Vibrationen
- Laserstrahlung
- Risiko, in einer Maschine eingeschlossen zu werden
- Ausrutsch-, Stolper- und Sturzrisiko

ANFORDERUNGEN AN SCHUTZEINRICHTUNGEN

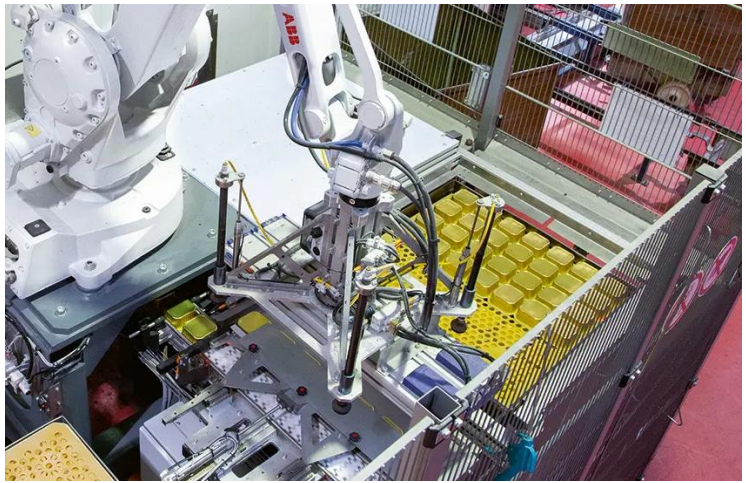
- **Allgemeine Anforderungen:**
  - Trennende und nichttrennende Schutzeinrichtungen
    - stabil
    - sicher in Position
    - keine zusätzlichen Gefährdungen
    - nicht auf einfache Weise umgehbar
    - ausreichend Abstand
    - Beachtung von Werkzeugwechsel, Montage, Wartung, …
    - Schutz vor beweglichen Teilen und Emissionen

→ viele weitere spezielle Anforderungen

MÖGLICHE TECHNISCHE SCHUTZEINRICHTUNGEN



TRENNENDE SCHUTZEINRICHTUNGEN (1)



FESTE EINRICHTUNGEN:
ZAUN, GITTER

BEWEGLICHE EINRICHTUNGEN:
TÜR, KLAPPE, HIER MIT
WARNSCHILD

Quellen: ABB, LS IRPA

TRENNENDE SCHUTZEINRICHTUNGEN (2)

- **Türen, Klappen, Abdeckungen**
  - Bei beweglichen oder abnehmbaren trennenden Schutzeinrichtungen sind meistens Sicherheitsschalter erforderlich, um ein Öffnen zu erkennen oder zu verhindern.

SICHERHEITSSYSTEM MIT TÜRGRIFF, ZUHALTUNG, FLUCHTENTRIEGELUNG UND BEDIENELEMENTEN

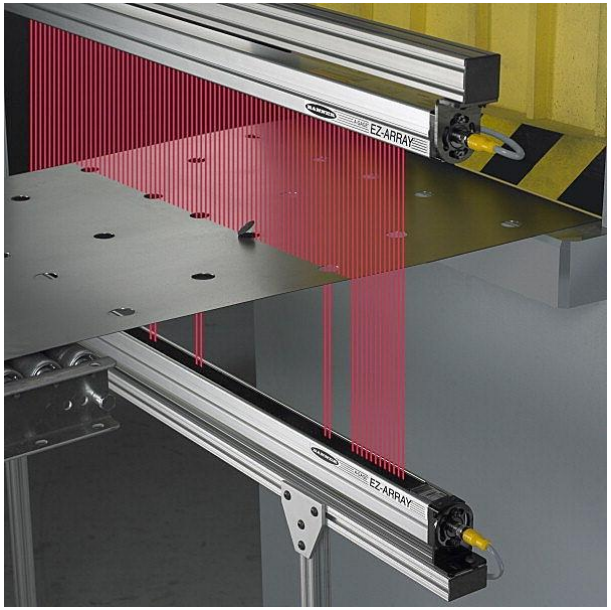
POSITIONSSCHALTER

TRANSPONDER-CODIERTER SICHERHEITSSCHALTER

Quelle: Euchner

NICHTTRENNENDE SCHUTZEINRICHTUNGEN (1)

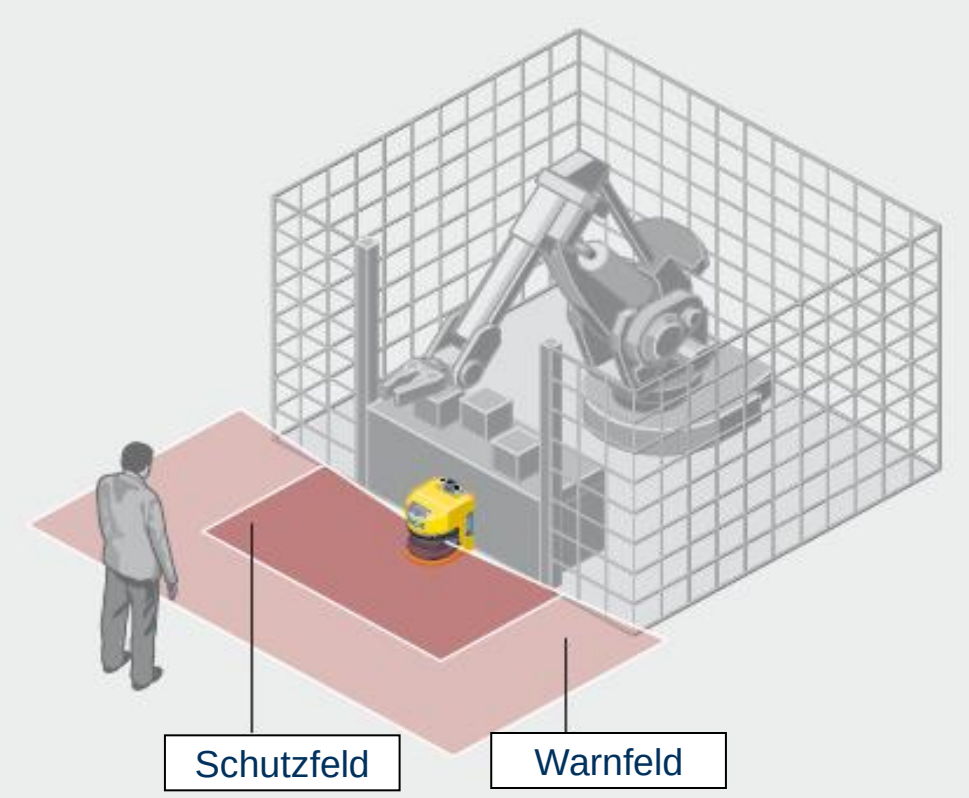
LICHTSCHRANKE



LICHTVORHANG / LICHTGITTER

Quelle: Direct Industries

NICHTTRENNENDE SCHUTZEINRICHTUNGEN (2)



Quelle: Sick, Public Domain

NICHTTRENNENDE SCHUTZEINRICHTUNGEN (3)

KAMERA-SENSOR ZUR ÜBERWACHUNG VON ZUGRIFFSBEREICHEN

ULTRASCHALL-DISTANZ-SENSOR

SICHERES RADARSYSTEM

Quelle: Sick

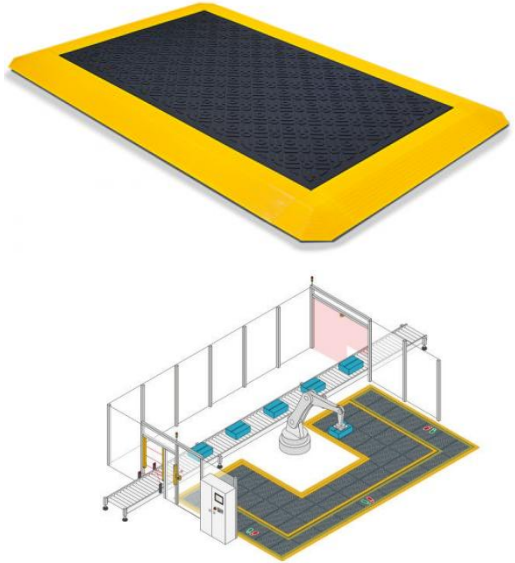
NICHTTRENNENDE SCHUTZEINRICHTUNGEN (4)

- **Sichere Kamerasysteme:**
  - 3D-Time-of-Flight-Kamera
  - Einrichtung von 3-dimensionalen Warn- und Stopp-Zonen
  - Überwachung großer Arbeitsräume
  - Überwachung mehrerer Schutzbereiche (mit entsprechenden Warn- und Stopp-Zonen)

Quelle: Sick

NICHTTRENNENDE SCHUTZEINRICHTUNGEN (5)

Zweihandbedienpult zur ortsgebundenen Steuerung

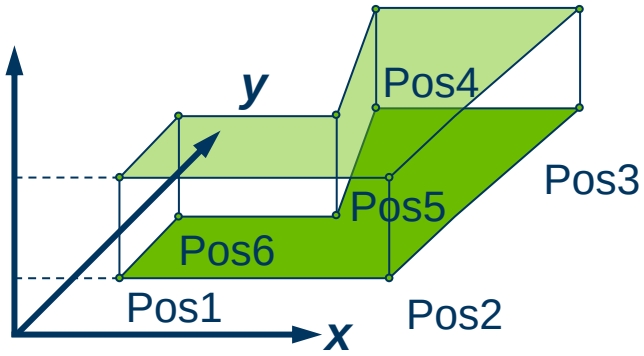


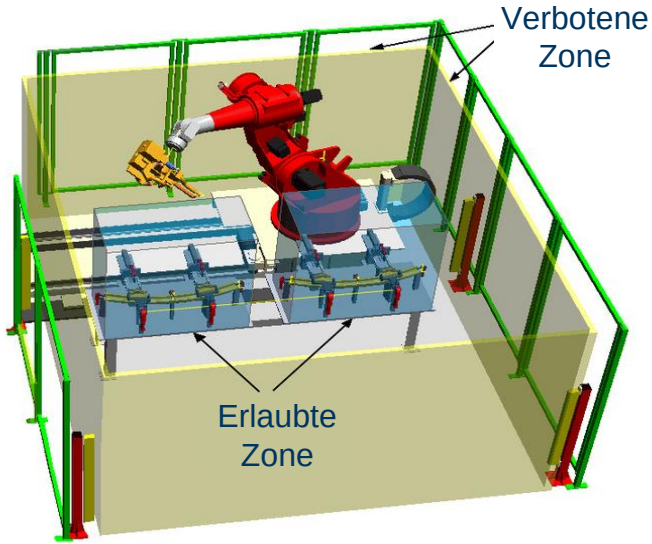
Sicherheitsschaltmatte (drucksensitive Schutzeinrichtung)

Quelle: Schmersal, Pilz

BETRIEB VON ROBOTERN OHNE TRENNENDE SCHUTZEINRICHTUNG (OTS)

- **Softwarebasierte Begrenzung:**
  - Reis – Virtual work envelope / Cartesian safety area





Quelle: Reis

INSTANDHALTUNG

- **Wartung der Maschine:**
  - Einrichtungs- und Wartungsstellen außerhalb der Gefahrenbereiche
  - Einrichtungs-, Instandhaltungs-, Reparatur-, Reinigungs- und Wartungsarbeiten durchführbar bei stillgesetzter Maschine
  - Andernfalls sind geeignete Maßnahmen zu ergreifen, um die Arbeiten sicher zu machen.
  - Bei automatischen Maschinen Schnittstelle zum Anschluss einer Fehlerdiagnoseeinrichtung
  - Teile von automatischen Maschinen, die häufig ausgewechselt werden müssen, sind für einfache und gefahrlose Montage und Demontage nach einem festgelegten Verfahren auszulegen.

INFORMATIONEN UND WARNEINRICH-TUNGEN

- **Informationen und Warnhinweise an der Maschine**
  - Leicht verständlich, wenn möglich Piktogramme
- **Informationen und Informationseinrichtungen**
  - Leicht verständlich, eindeutig, keine Informationsüberflutung
- **Warneinrichtungen**
  - Eindeutige Signale
  - Überprüfbare Funktionsbereitschaft
- **Warnung vor Restrisiken**
  - Erforderliche Warnhinweise vor Restrisiken

KENNZEICHNUNG EINER MASCHINE

- Auf jeder Maschine müssen mindestens folgende Angaben erkennbar, deutlich lesbar und dauerhaft angebracht sein:
  - Firmenname und vollständige Anschrift des Herstellers und gegebenenfalls seines Bevollmächtigten,
  - Bezeichnung der Maschine,
  - CE-Kennzeichnung (ausgenommen unvollständige Maschinen),
  - Baureihen- oder Typbezeichnung,
  - Gegebenenfalls Seriennummer,
  - Baujahr, d. h. das Jahr, in dem der Herstellungsprozess abgeschlossen wurde.

Muss ein Maschinenteil während der Benutzung mit Hebezeugen gehandhabt werden, so ist sein Gewicht und ggf. der Schwerpunkt leserlich, dauerhaft und eindeutig anzugeben.

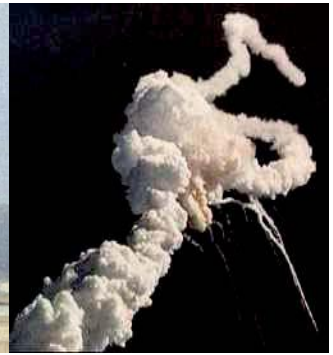
Sicherheitskonzepte

Gefahrenanalyse und Gegenmaßnahmen

- Ein erfahrenes Expertengremium aus erfahrenen Anlagenplanern und –betreibern analysiert jedes einzelne Aggregat in der Anlage, welches auf den Prozess wirkt
- Definition des gewünschten Sollverhalten
- Untersuchungen aller möglichen Abweichungen und den daraus resultierenden Konsequenzen.
- HAZOP-Methode, Hazards and Operability
  Gefahrenanalyse und Gegenmaßnahmen.
- Fehlerbaumanalyse FTA (Fault Tree Analysis)
  Ereignisbaumanalyse (Event Tree Analysis)

Sicherheitskonzepte

Problematik
Für hochzuverlässige oder „neuartige“ Systeme liegen keine direkt nutzbaren Erfahrungen auf Systemebene vor; wegen der Höhe der Investition und involvierten Gefahren sind (Vorab-) Aussagen zur Ausfallwahrscheinlichkeit (Zuverlässigkeit) und zu Risiken nötig.



Lösungsansatz: Zerlegung
Aus den Systemkomponenten, deren Eigenschaften eher bekannt sind, lässt sich über deren funktionelle und logische
Verknüpfung das Gesamtsystemmodellieren und analysieren.

Ansatz der FTA

Ziel: Anlagen sicher machen um Schäden von Mensch, Umwelt und Geräten abzuwe

Steuerungen beeinflussen die Sicherheit von Anlagen auf zwei Arten:

- Überwachen die Anlage und führen sie im Fall einer gefährlichen Situation in einen sicheren Betriebszustand
  i.d.R. schalten die Anlage im Notfall ab
- Fehler in der Steuerung können zu gefährlichen Situationen in der Anlage fuehren oder das herstellte Produkt verderben
  (Nahrungsmittel und Arzneimittelproduktion)

Ansatz der FTA

Ausgangspunkt ist ein definierter Systemzustand ("top event", z.B. Systemausfall), der weiter "top down" (von oben nach unten) über Zwischenzustände bis zu Basisereignissen (Komponentenausfälle) aufgeschlüsselt wird. Die Fragestellung bzw. Vorgehensweise ist deduktiv.

Ziele

- Systematische Identifizierung möglicher Ausfallkombinationen und dahinterliegender Basisereignisse, die zu einem vorgegebenen "top-event" führen können.
- Zusätzliche Ermittlung der Eintrittswahrscheinlichkeit von Ausfallkombinationen und des "top-event", nach Zuweisung von Zuverlässigkeitskenngrössen für Basisereignisse (Ausfallwahrscheinlichkeit).

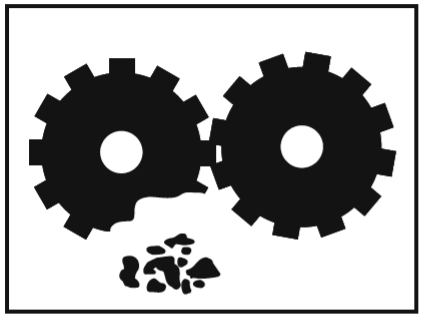
Normen

- Fehlerbaumanalyse, Methode und Bildzeichen, DIN 25 424, Teil 1 (Berlin, Beuth Verlag GmbH: 1981),
- Fehlerbaumanalyse, Handrechenverfahren zur Auswertung eines Fehlerbaums, DIN 25 424, Teil 2 (Berlin, Beuth Verlag GmbH: 1990).

Sicherheitskonzepte

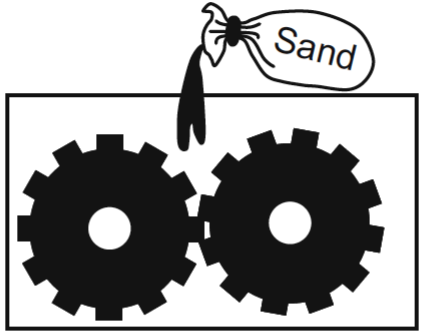
Ausfallarten

primärer Ausfall



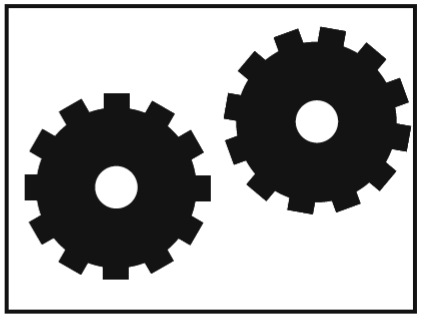
Komponentenausfall durch eigene Schwäche

sekundärer Ausfall



Komponentenausfall durch entsprechende Umgebungs- oder Einsatzbedingungen (nur bei offenen Systemen)

kommandierter Ausfall



Ausfall trotz funktionsfähiger Komponente, infolge einer falschen oder fehlenden Ansteuerung

Arbeitsschritte der FTA

Qualitativ

1. Festlegen des "top-event" (nicht immer einfach),
2. Identifizierung aller Ereigniskombinationen, die zum "top-event“ führen, und zugehöriger Basisereignisse

Qualitativ und Quantitativ

3. Ermittlung und Zuweisung von Zuverlässigkeitkenngrössen zu jedem Basisereignis, Systemmodellierung und Berechnung der Eintrittswahrscheinlich von Verzweigungen und des "top-events",
4. Analyse der dominierenden Ereigniskombinationen und –Beiträge
5. (Importanzanalyse), Vorschläge zur Systemoptimierung.

Sicherheitskonzepte

zu 1. "top-event"

Festlegung

- Allgemein: Systemausfall, z.B. Ausfall eines sicherheitstechnisch wichtigen Kühlsystems
- speziell: Ausfall bestimmter Funktionen, die einem Systemausfall gleichkommen, z.B. Bersten eines Gastanks.

zu 2. Ereigniskombinationen

Verknüpfungen bilden die logische Struktur des betrachteten Systems bzw. des daraus abgeleiteten Modells (Fehlerbaum) mit

- Ereigniseingängen: Art der Ereignisse,
- logischen Verknüpfungen: UND, ODER, NICHT,
- Ereignisausgängen: Ereignisfolgen.

Die Regeln der Verknüpfungen sind durch Boolesche Algebra festgelegt.

Sicherheitskonzepte

Boolean-Modellierung und Wahrscheinlichkeitsberechnur

Zusammenfassung der Annahmen/Voraussetzungen :

- Ein technisches System besteht aus Einheiten (Komponenten): S={K1, … Kn}
- Die Einheiten werden sowohl technisch als auch logisch verbunden, Fehler von Komponenten sind stochastisch unabhängig.
- Der Zustand jeder Einheit folgt einer binären Logik (WAHR/FALSCH, Ein/Aus-, intakt / defekt)
- Verfügbare logische Operatoren sind:
- Konjunktion: UND (∩)
- Disjunktion: ODER (∪)

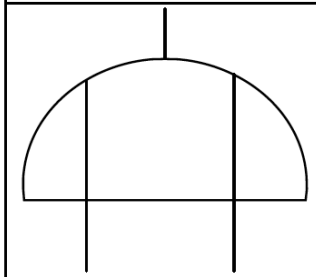
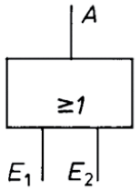
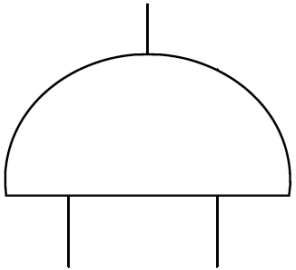
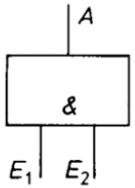
Bezeichnung der Wahrscheinlichkeiten :

p_i: Wahrscheinlichkeit des Überlebens der i-ten Einheit

q_i: Wahrscheinlichkeit des Misserfolgs der i-ten Einheit

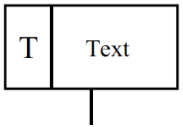
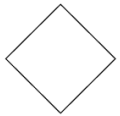
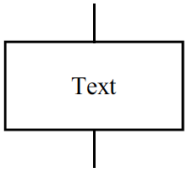
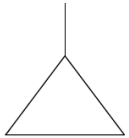
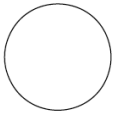
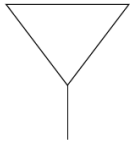
Sicherheitskonzepte

Logische Verknüpfungen

Symbol	Alternative Symbole		Benennung
			**ODER-Verknüpfung** logische Vereinigung einer Menge
			**UND-Verknüpfung** logischer Durchschnitt einer Menge

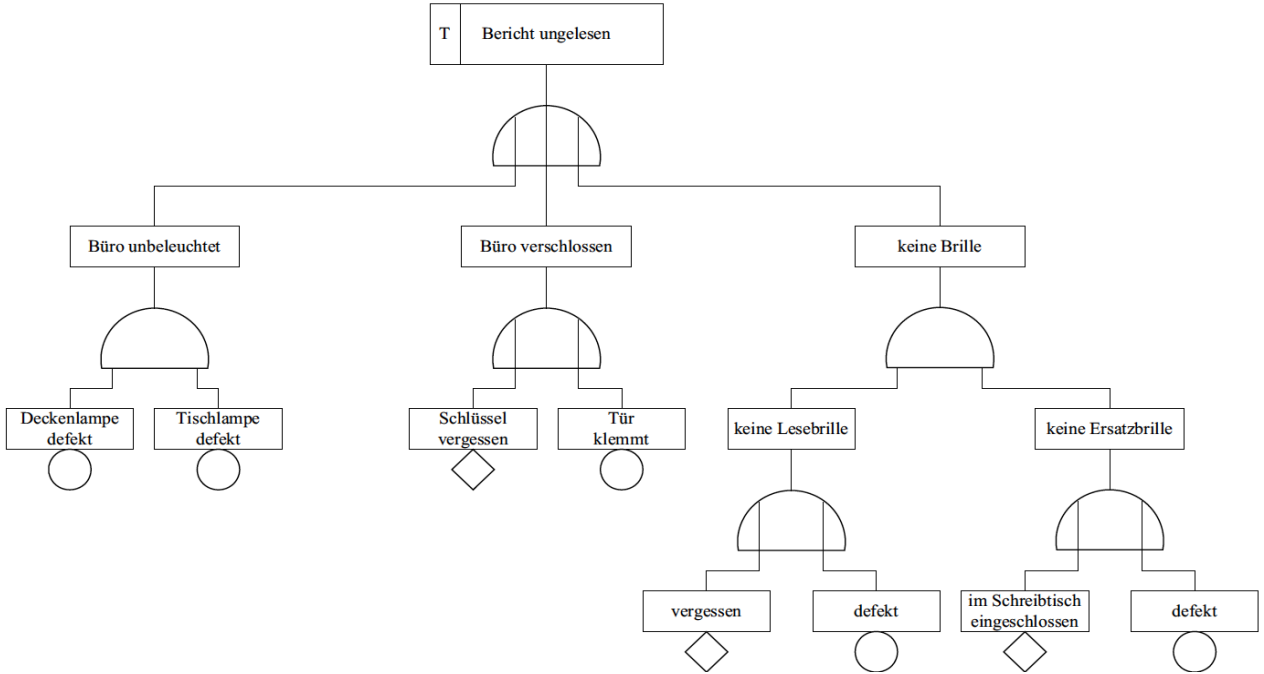
Sicherheitskonzepte

Zur Besseren Handhabung dienen:

Symbol	Benennung	Symbol	Benennung
	Bezeichnung des „top event“		nicht weiter entwickeltes Ereignis
	Kommentar, Beschreibung		Transfer zu einem separaten Fehlerbaum
	Basisereignis		Transfer von einem separaten Fehlerbaum

Beispiel: Fehlerbaum Lesebrille

Beispiel:
Herr K. möchte um Mitternacht in seinem Büro einen Bericht lesen.
Er benötigt eine Lesebrille; eine Ersatzbrille ist im Schreibtisch eingeschlossen.



Sicherheitskonzepte

Benötigte Informationen für eine FTA

- Verschiedene relevante Ausfallarten der einzelnen Komponenten,
- Komponentenexterne relevante Einflussgrößen, z.B. Instandhaltungsmaßnahmen Umwelteinwirkungen
- Zuverlässigkeitskenngrössen (Ausfallwahrscheinlichkeiten),
- Definition des zu untersuchenden Betriebszustandes der Anlage und deren Abgr (Systemgrenzen).

Sicherheitskonzepte

Zu 3: Zuweisung von Wahrscheinlichkeiten

Die Ausfallwahrscheinlichkeit ist eine von mehreren Zuverlässigkeitskenngrössen
ZKG sind quantitative Merkmale, die das mit Versagen zusammenhängende stoc
Verhalten einer Einheit (Hard-, Software etc.) technischer Systeme unter bekannt
Leistungsbedingungen kennzeichnen.

Problematiken

Allgemeiner Datenmangel; besonders ausgeprägt bei Zuverlässigkeitskenngröss
hochzuverlässige Spezialanfertigungen in der Kernenergie, für Komponenten unt
wechselnden Betriebsbedingungen in der Chemie, für abhängige Ausfälle etc.

Sicherheitskonzepte

zu 4. Modellierung technischer Systeme

Zusammenfassung der Annahmen/Voraussetzungen:

- Ein technisches System besteht aus Betrachtungseinheiten BE (Komponenten),
- die BE sind sowohl technisch als auch logisch untereinander verbunden,
- jede BE kann nur zwei Zustände annehmen (binäre Logik).

Zur Verfügung stehende logische Operatoren:

- Konjunktion: UND ($\cap$),
- Disjunktion: ODER ($\cup$).

Bezeichnung der Wahrscheinlichkeiten:

- p_i: Überlebenswahrscheinlichkeit der i-ten Einheit,
- q_i: Ausfallwahrscheinlichkeit der i-ten Einheit.

Elementare Struktur eines Fehlerbaumes

Systemausfall oder Unglücksfall
(Top Event)

Der Fehlerbaum besteht aus Ereignisabfolgen,
die zum Top-Event führen

Die Ereignisabfolge wird durch UND-, ODER oder andere
logische Operatoren aufgebaut

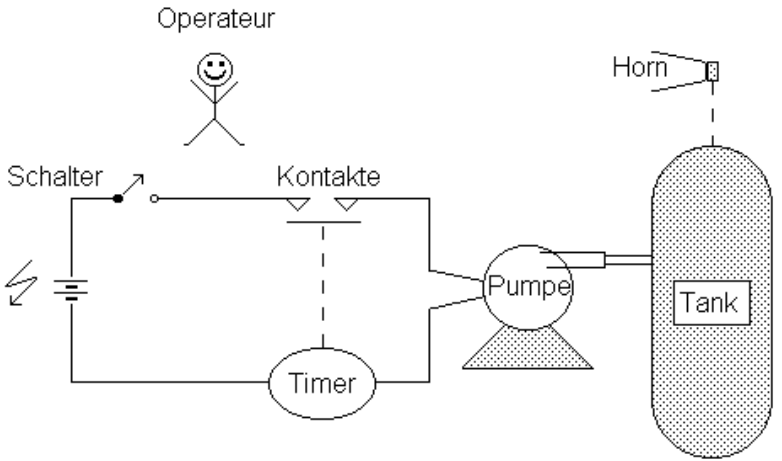
Die Ereignisse oberhalb der Operatoren und alle Ereignisse, die mehr
als ein Basisereignis haben, werden durch ein Rechteck markiert. Dort
wird das Ereignis näher beschrieben.

Die Ereignisabfolgen führen schließlich zu elementaren Komponenten, deren Zuver.-
Kenngrößen bekannt sind. Diese Basisereignisse werden durch Kreise markiert, die
Auflösungsvermögen des Fehlerbaums zeigen

Sicherheitskonzepte

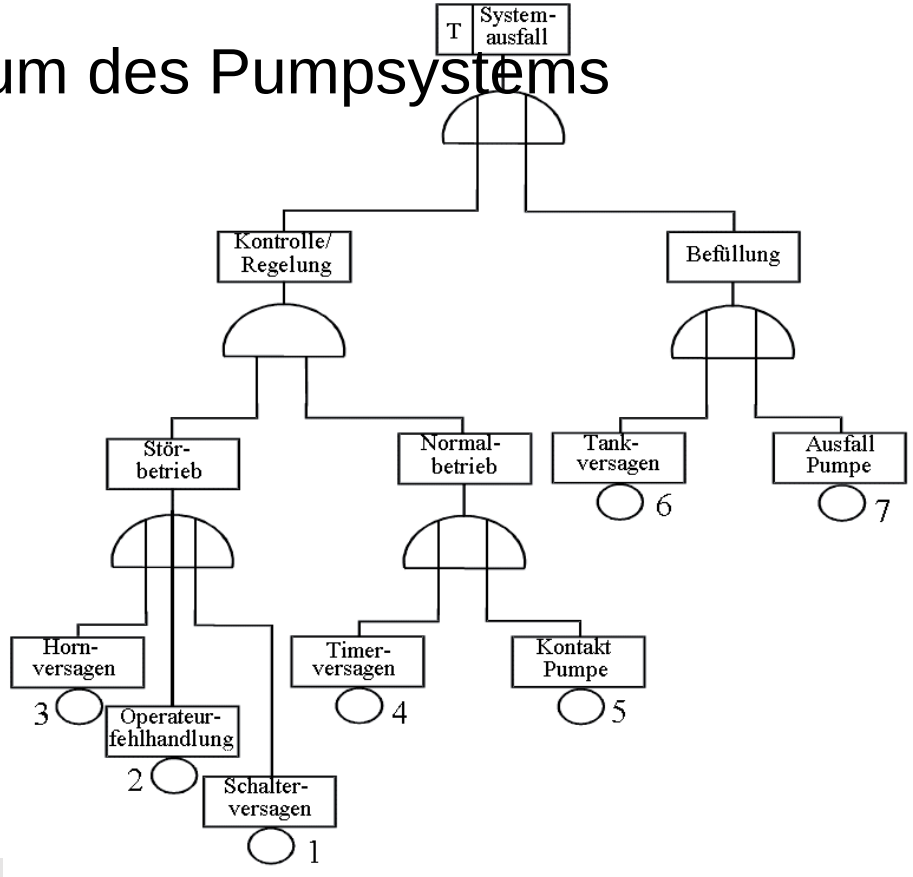
Beispiel: Fehlerbaum für ein Pumpsystem

Im Pumpsystem wird der Speicher in 10 Minuten gefüllt und in 50 Minuten entleert; ein vollständiger Zyklus umfasst also 1 Stunde. Nachdem der Schalter geschlossen
Hilfe des Timers nach10 Minuten ge
Mechanismus, so ertönt ein Alarms
den Schalter, um ein Tankversagen
vermeiden.



Sicherheitskonzepte

Beispiel: Fehlerbaum des Pumpsystems



Sicherheitskonzepte

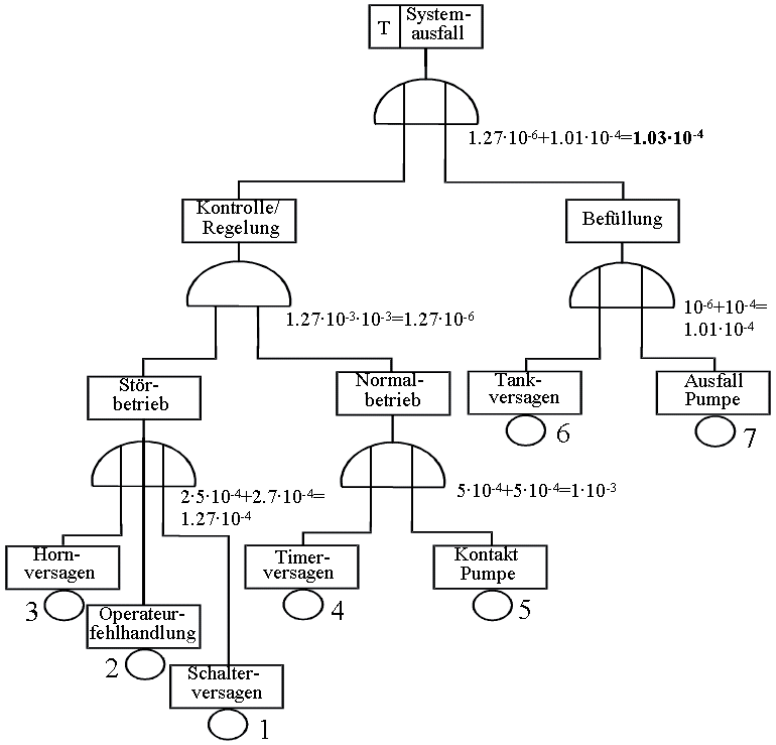
Wahrscheinlichkeiten zur Quantifizierung des Fehlerbaums (Richtwerte)

Einheiten bzw. Funktionselemente in (): Nr. des Basisereignisses im Fehlerbaum	Überlebenswahr-scheinlichkeit p_i	Ausfallwahr-scheinlichkeit q_i
elektromechanische Teile: Schalter, Timer, Horn, Kontakte	0.9995	$5 \cdot 10^{-4}$
passives Element: Tank	0.999999	10^{-6}
aktives Element: Pumpe	0.9999	10^{-4}
„Funktionselement Mensch“: Operateur	0.99973	$2.7 \cdot 10^{-3}$

- $q_{Operatuer}$: Wahrscheinlichkeit, dass der Operateur auf ein wahrgenommenes Signal gar nicht oder falsch reagiert,
- q_{Pumpe}: Wahrscheinlichkeit, dass die Pumpe trotz geöffnetem Schalter weiterfördert.

Sicherheitskonzepte

Quantitativer Fehlerbaum



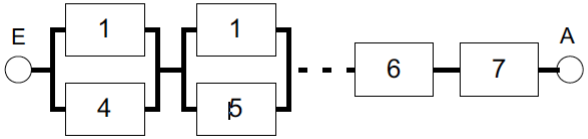
Boolesche Gleichung - Ausfall

$$\bar{y} = [(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_4 \vee \bar{x}_5)] \vee (\bar{x}_6 \vee \bar{x}_7)$$

ausmultiplizieren

$$\bar{y} = \bar{x}_1\bar{x}_4 \vee \bar{x}_1\bar{x}_5 \vee \bar{x}_2\bar{x}_4 \vee \bar{x}_2\bar{x}_5 \vee \bar{x}_3\bar{x}_4 \vee \bar{x}_3\bar{x}_5 \vee \bar{x}_6 \vee \bar{x}_7$$

Kombination Serien-Parallel- und Seriensystem



Berechnung

$$F_{SP} = 1 - \prod_{i=1}^{6}(1 - q_{1i}q_{2i}) = 1 - \left[(1 - q_1q_4)(1 - q_1q_5)....\text{etc}\right]$$

$$F_s = 1 - \left[(1 - q_6)(1 - q_7)\right]$$

$$F = F_{SP} + F_s = ... = 1.0227 \cdot 10^{-4}$$

Sicherheitskonzepte

Vor-/Nachteile FTA

Vorteile	Nachteile
• Gut geeignet zur Modellierung mechanischer, dualer Vorgänge, z.B. Ventil geöffnet oder geschlossen. • Es können Ereignisse betrachtet werden, die durch das Zusammenwirken mehrerer Ausfälle oder Fehler auf Komponentenebene zustande kommen. • Bei ausreichender Datenbasis ist eine Quantifizierung möglich. • Es bestehen breite Einsatzmöglichkeiten, die eine Systemoptimierung einschliessen.	• Zeitabhängige und dynamische Änderungen sind schwer zu modellieren; die Systembeschreibung ist „statisch“. • Komplexe Systeme führen zu „unüberschaubar“ vielen Verzweigungen, weshalb Beschränkung auf das Wesentliche notwendig ist. • Die einzelnen Eintrittswahrscheinlichkeiten sind z.T. schwer zu ermitteln und mit erheblichen (Daten-) Unsicherheiten behaftet.

Sicherheitskonzepte

Berechnung von Fehlerbäumen für größere Systeme

Problematik

- Oft schwierig, einen kompletten Fehlerbaum zu erstellen und exakt zu berechnen.

Lösungsansatz

- Ermittlung jener Komponenten, die mindestens betriebsfähig sein müssen, damit das Gesamtsystem funktioniert (Positiv-Logik).

oder

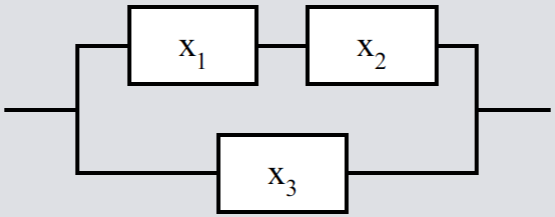
- Ermittlung jener Komponenten, die bei Ausfall das Gesamtsystem ausfallen lassen (Negativ-Logik).

➢ Minimalschnitte bzw. Minimalpfade.

Bezeichnung

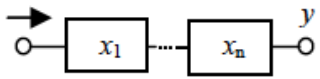
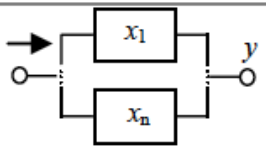
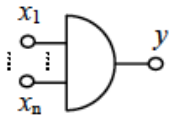
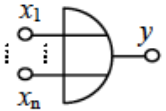
- Zustand x_i der Komponente i:

$$x_i = \begin{cases} 0: \text{Zustand "Ausfall" (kurz: } \overline{x_i}) \\ 1: \text{Zustand „Funktion“ (kurz: } x_i) \end{cases}$$

Minimalschnitte (Cut Sets)	Minimalpfade (Path Sets)
Kleinste Menge ausgefallener Einheiten, die im Zuverlässigkeitsblockdiagramm den Weg vom "Eingang" zum "Ausgang" versperrt.	Kleinste Menge (funktionierender) Einheiten, die im Zuverlässigkeitsblockdiagramm einen Weg vom "Eingang" zum "Ausgang" offen hält.
Beispiel 	
Schnitte σ_i: $\sigma_1 = \{\overline{x}_1; \overline{x}_3\}; \sigma_2 = \{\overline{x}_2; \overline{x}_3\}$	Pfade π_j: $\pi_1 = \{x_1; x_2\}; \pi_2 = \{x_3\}$

Sicherheitskonzepte

Positivlogik

Systemstruktur	Reihenanordnung	Parallelanordnung
Blockschaltbild		
Funktionsbaum		
Boolesche Funktion	$y = x_1 \wedge x_2 \wedge \ldots \wedge x_n = \bigwedge_{i=1}^{n} x_i$	$y = x_1 \vee x_2 \vee \ldots \vee x_n = \bigvee_{i=1}^{n} x_i$
Systemzu-verlässigkeit	$R_S(t) = \prod_{i=1}^{n} R_i(t)$	$R_S(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$

Sicherheitskonzepte

Negativlogik

Systemstruktur	Reihenanordnung	Parallelanordnung
Blockschaltbild		
Funktionsbaum		
Boolesche Funktion	$\overline{y} = \overline{x_1} \vee \overline{x_2} \vee \ldots \vee \overline{x_n} = \bigvee_{i=1}^{n} \overline{x_i}$	$\overline{y} = \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n} = \bigwedge_{i=1}^{n} \overline{x_i}$
Systemausfall-wahrscheinlichkeit	$F_S(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t))$	$F_S(t) = \prod_{i=1}^{n} F_i(t)$

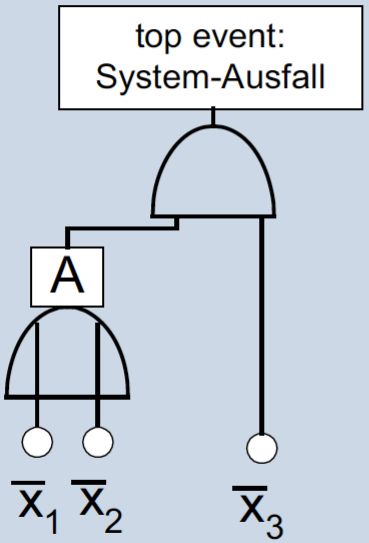
Sicherheitskonzepte

für jede Schnitt-Menge *i* gilt	für jede Pfadmenge *j* gilt
$\sigma_i = \bigcap_{k=1}^{l} \overline{x}_k$	$\pi_j = \bigcap_{m=1}^{r} x_m$
Systemausfall: Verknüpfung der Schnitte σ_i $\overline{y} = \bigcup_{i=1}^{n} \sigma_i$	**Systemfunktion**: Verknüpfung der Pfade π_j $y = \bigcup_{j=1}^{s} \pi_j$
de-Morgansches Theorem	
$\overline{y} = 1 - \bigcap_{j=1}^{n} \left(1 - \sigma_j\right) = 1 - \left[\left(1 - \overline{x}_1\overline{x}_3\right)\left(1 - \overline{x}_2\overline{x}_3\right)\right]$	$\overline{y} = \bigcap_{j=1}^{s} \left(1 - \pi_j\right) = \left(1 - x_1x_2\right)\left(1 - x_3\right)$
ausmultiplizieren, Idempotenzgesetz: $x \cap x = x$; $x \cup x = x$	
$\overline{y} = 1 - \left[\left(1 - \overline{x}_1\overline{x}_3\right)\left(1 - \overline{x}_2\overline{x}_3\right)\right]$ $= 1 - \left(1 - \overline{x}_1\overline{x}_3 - \overline{x}_2\overline{x}_3 + \overline{x}_1\overline{x}_3\overline{x}_2\overline{x}_3\right)$ $= \overline{x}_1\overline{x}_3 + \overline{x}_2\overline{x}_3 - \overline{x}_1\overline{x}_2\overline{x}_3$	$\overline{y} = 1 - x_1x_2 - x_3 + x_1x_2x_3$

Sicherheitskonzepte

Einsetzen der Ausfallwahrscheinlichkeiten $q_i(t)$	Einsetzen der Ausfallwahrscheinlichkeiten $p_i(t)$
…	zum Vergleich mit Minimalschnitt $\bar{y} = 1-(1-\bar{x}_1)(1-\bar{x}_2)-(1-\bar{x}_3)+(1-\bar{x}_1)(1-\bar{x}_2)(1-\bar{x}_3)$ =...ausmultiplizieren... $= \bar{x}_1\bar{x}_3 + \bar{x}_2\bar{x}_3 - \bar{x}_1\bar{x}_2\bar{x}_3$
System-Ausfallwahrscheinlichkeit	
$F = q_1q_3 + q_2q_3 - q_1q_2q_3$	$F = q_1q_3 + q_2q_3 - q_1q_2q_3$

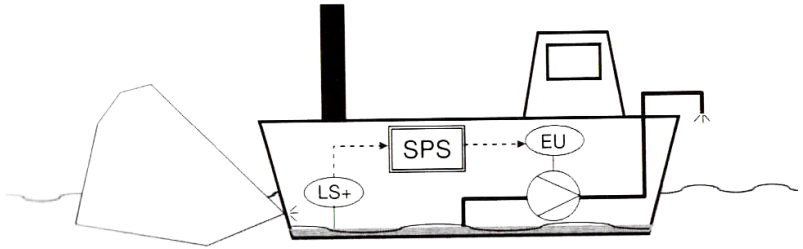
Sicherheitskonzepte

Fehlerbaum	Algorithmus
	Beginnend beim „top event“ werden die Eingänge des ODER-Gatters zeilenweise, bei einem UND-Gatter spaltenweise aufgelistet. Beim Ersetzen eines ODER-Gatters gibt es für jeden neuen Eingang eine neue Zeile, wobei die restliche Zeile erhalten bleibt. Beachte innerhalb einer • Zeile: Idempotenzgesetz, • Spalte: Absorptionsgesetz $Z_1 \square (Z_1 \cdot Z_2) = Z_1$, Beispiel 1. Schritt (eine Zeile) $\{A, \overline{x}_3\}$ 2. Schritt: ersetze ODER-Gatter A, füge eine Zeile hinzu $\{\overline{x}_1; \overline{x}_3\}$ $\{\overline{x}_2; \overline{x}_3\}$ q.e.d.

Sicherheitskonzepte

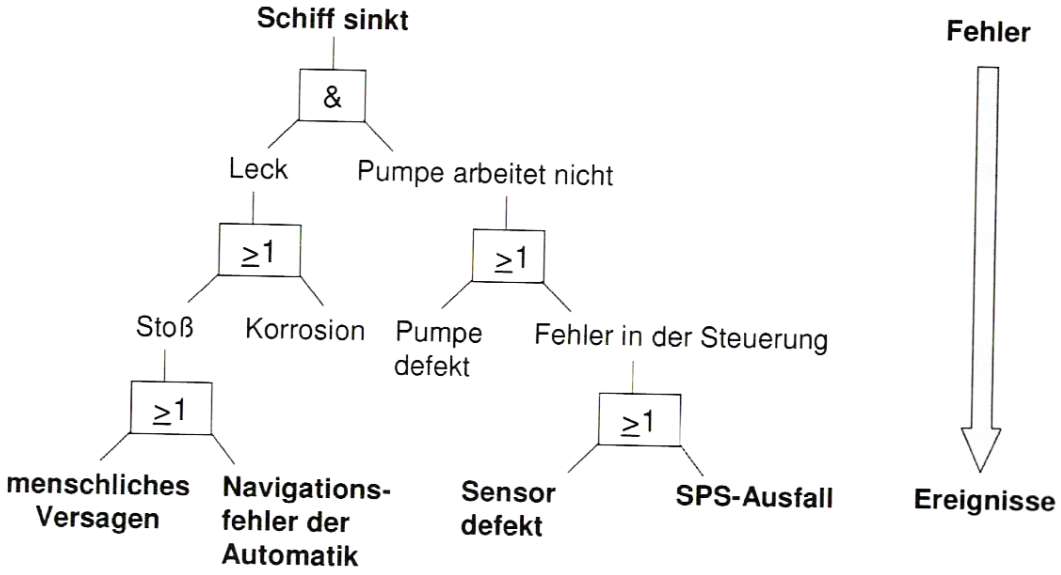
Ereignisbaumanalyse (Event Tree Analysis ETA)

Die Ereignisbaumanalyse geht von möglichen unerwünschten Ereignissen während des Anlagenbetriebs aus und betrachtet die daraus entstehenden Konseque



Sicherheitskonzepte

Fehlerbaum



Sicherheitskonzepte

Ereignisablaufanalyse (ETA)
(„event tree analysis“, Störfallablaufanalyse, incident sequence analysis).

Norm
Ereignisablaufanalyse, Verfahren, graphische Symbole und Auswertung, DIN 25419 (Berlin, Beuth Verlag GmbH: 1985).

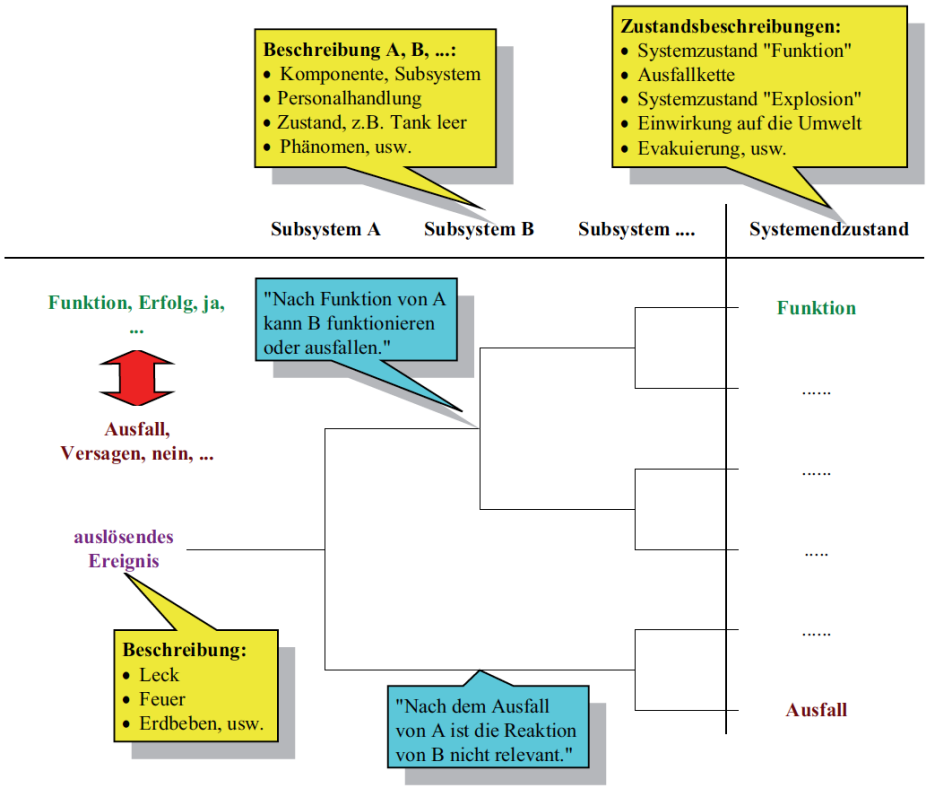
Ziele einer Ereignisablaufanalyse (induktiv)
Erfassen der Ereignisabläufe in einem (größerem) System, die nach einem auslösenden Ereignis durch die Reaktion nachfolgender (sicherheitstechnischer) Subsysteme entstehen können:

- Graphische Darstellung des logischen und physikalischen Ineinandergreifens aufeinanderfolgender Ereignisse in einem System,
- Ermittlung von Systemendzuständen, die aus einer bestimmten Ursache folgen,
- Berechnung der Eintrittshäufigkeiten resultierender Systemendzustände.

Merke: ETA ist auch auf menschliche Handlungen, physikalische / chemische

Sicherheitskonzepte

Prinzipieller Aufbau eines Ereignisbaumes



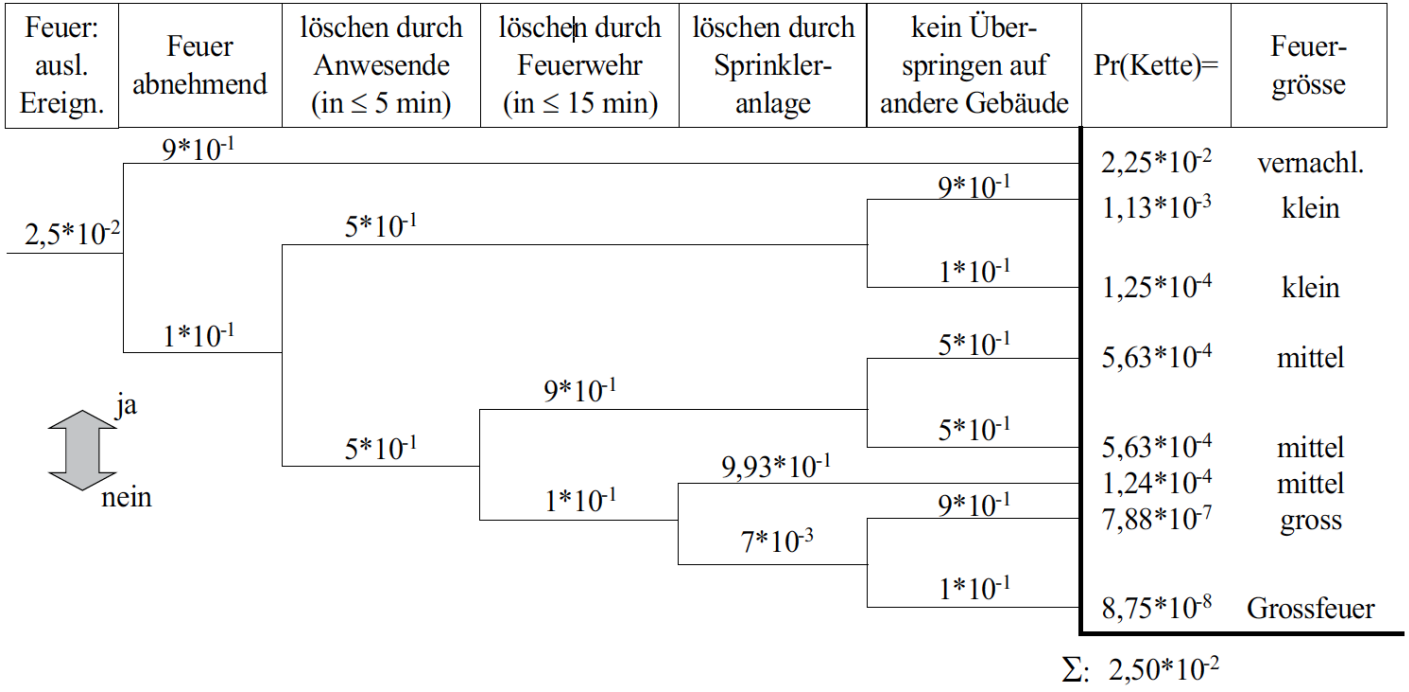
Sicherheitskonzepte

Arbeitsschritte einer quantitativen Ereignisablaufanalyse

1. Auflisten aller auslösenden Ereignisse
2. Identifizierung der direkten (funktionellen) Systemantworten, die jeweils durch die Funktion oder Nichtfunktion eines Subsystems bzw. Eintreten oder Nichteintreten von Ereignissen entstehen,
3. Zusammenfügen der auslösenden Ereignisse mit allen Systemantworten,
4. Bestimmung von Ereignisketten: Jede Systemantwort hat eine zugehörige Verzweigung, die Erfolg oder Misserfolg anzeigt. Am Ende jeder Kette steht eine Beschreibung der erwarteten Auswirkungen auf das System,
5. Zuweisung von Eintrittshäufigkeit [a-1] für das auslösende Ereignis und „bedingten“ Wahrscheinlichkeiten für Funktion/Ausfall,
6. Berechnung der Eintrittshäufigkeit der Endzustände des Gesamtsystems.

Sicherheitskonzepte

Beispiel: Brandrisiko und Brandschutzmaßnahmen



Sicherheitskonzepte

Berechnungen mit einem Ereignisbaum

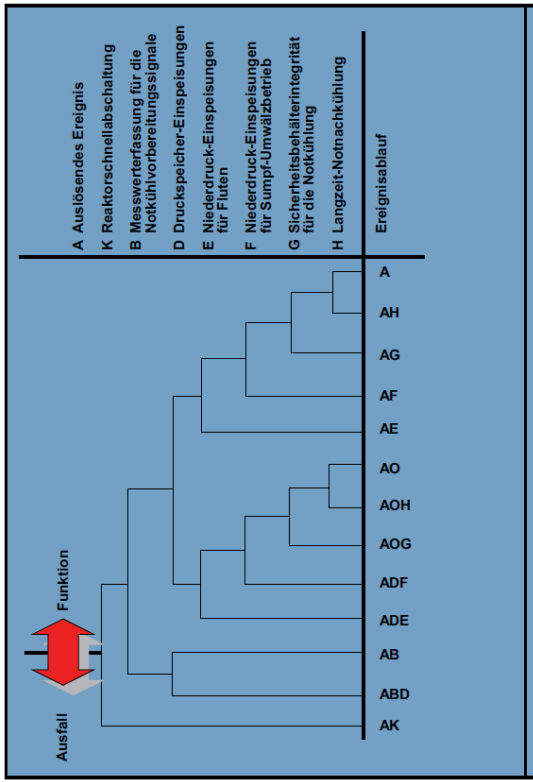
- Die Summe über alle n "Kettenwahrscheinlichkeiten"1) ergibt die Wahrscheinlichkeit des auslösenden Ereignisses.
- Die Eintrittswahrscheinlichkeit am Ende einer Kette A mit n nachfolgenden Subsystemen berechnet sich aus:

$$\Pr(Kette) = \Pr(Subsystem) \cdot \prod_{i=1}^{n} \Pr(Subsystem)$$

- Im Beispiel beträgt die Wahrscheinlichkeit eines Großfeuers:
  Pr(Feuergröße = Großfeuer) = $2.5 \cdot 10^{-2} \cdot 10^{-1} \cdot 5 \cdot 10^{-1} \cdot 10^{-1} \cdot 7 \cdot 10^{-3} \cdot 10^{-1} = 8.75 \cdot 10^{-8}$.
- Die Wahrscheinlichkeit eines bestimmten Ausmaßes ist die Summe der Ketten mit demselben Endergebnis, z. B.:
  Pr(Feuergröße = klein) = $1.13 \cdot 10^{-3} + 1.25 \cdot 10^{-4} = 1.26 \cdot 10^{-3}$.

Sicherheitskonzepte

Beispiel: Leck in der Hauptkühlmittelleitung eines AKWs



Vollständige Funktion

$$Pr = Pr_A \cdot (1-q_K) \cdot (1-q_B) \cdot (1-q_D) \cdot (1-q_E) \cdot (1-q_F) \cdot (1-q_G) \cdot (1-q_H)$$

q_i: bedingte Versagenswahrscheinlichkeit des Subsystems i,
Pr_A: Eintrittswahrscheinlichkeit des auslösenden Ereignisses,
Pr: Eintrittswahrscheinlichkeit des "Gesamtpfades".

Sicherheitskonzepte

Anmerkungen zur Ereignisablaufanalyse

- Besonders geeignet für größere Anlagen mit aktiven und passiven Sicherheitseinrichtungen sowie ungewissen physikalisch-chemischen Zuständen
- Praktische Erfahrungen und vorausgehende Systemuntersuchungen erforderlich
- Methode für alle Arten (technischer) Systeme geeignet (Auch) umfassende Ereignisbäume bieten keine Garantie hinsichtlich Fehlerfreiheit und Vollständigkeit.
- Sorgfältiger Review der Ergebnisse Teil einer vollständigen Analyse.

Sicherheitskonzepte

Zusammenfassung: Fehlerbaumanalyse und Ereignisbaumanalyse

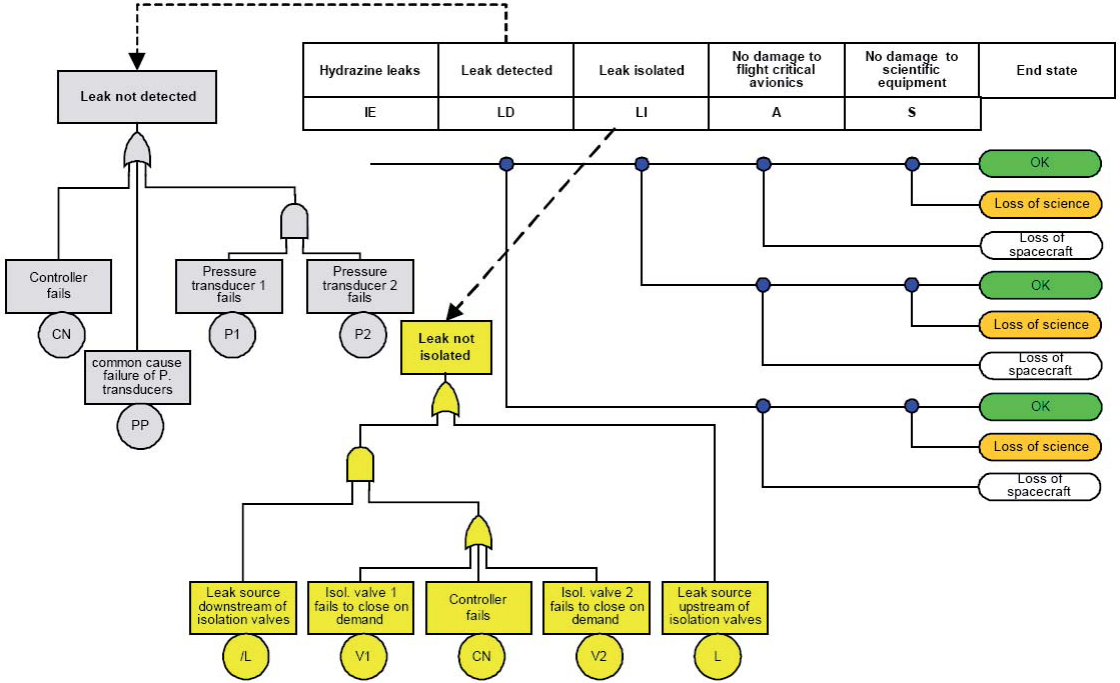
Fehlerbaumanalyse

- Deduktive Logik („Abwärtslogik“)
- Statische Betrachtungsweise
- Eine einzelne Kette von Ereignissen vom "top-event" zu einem Basisereignis hat keine offensichtliche technische Bedeutung (nur Subfehlerbäume)

Ereignisbaumanalyse

- Induktive Logik („Vorwärtslogik“)
- Berücksichtigung dynamischer Prozesse begrenzt möglich
- Jedes Ereignis auf der Kette vom auslösenden Ereignis bis zum Systemendzusta hat eine systemtechnische Bedeutung

Sicherheitskonzepte



Risikographen nach IEC 61508

Risikoanalyse

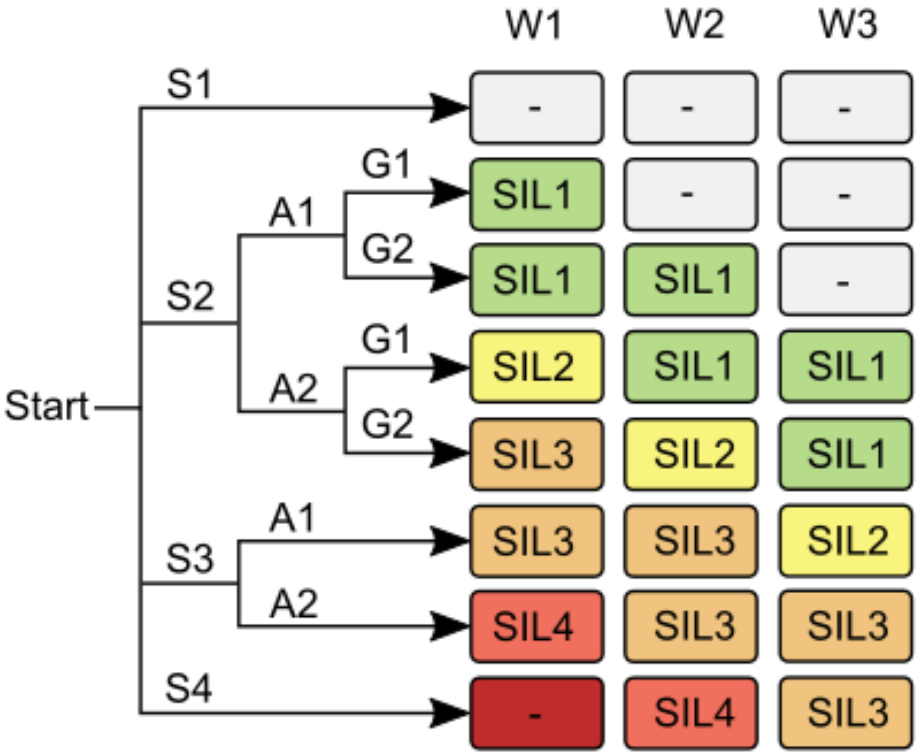
Risiko = S x H

S = Schadensausmaß
H = Häufigkeit des Fehlers

Verwendung eines Risikographen nach IEC 61508

Die Sicherheitsanforderungsstufe ist ein Begriff aus dem Gebiet der Funktionalen Sicherheit und wird in der internationalen Normung IEC 61508/IEC61511 auch als Sicherheits-Integritaetslevel SIL (Safety Integrity Level) bezeichnet.

Sicherheitskonzepte



Sicherheitskonzepte

Schadensausmass (S)

Als erstes muss das Schadensausmass (S) bewertet werden, das beim Eintreten der Gefährdung anzunehmen ist.

Aufenthaltswahrscheinlichkeit (A)

Danach ermittelt man die Wahrscheinlichkeit bzw. Häufigkeit, mit der sich eine Person in Gefahrenbereich aufhält (A).

Gefahrenabwehr (G)

Es folgt die Einschätzung, ob die Möglichkeit besteht eine eintretende Gefahr abzuwehr den Schaden zu begrenzen (z.B. Feuer kann gelöscht werden; ein sich bewegendes Te langsam und man kann noch ausweichen). Hier gibt es nur die beiden Möglichkeiten G1

Eintrittswahrscheinlichkeit (W)

Als letztes muss ermittelt werden, wie wahrscheinlich das Eintreten der betrachteten Gefährdung ist. In diesem Schritt unterscheidet sich der hier gezeigte Risikograph von d Graphen, wie er in der Norm EN ISO 13849 gezeigt wird. Denn die Bewertung der Eintrittswahrscheinlichkeit findet im genannten Pendant nicht statt.

Sicherheitskonzepte

S = Schadensausmaß / Schwere der Verletzung:
S1 = leichte (reversible Verletzung)
S2 = ernste (irreversible Verletzung Tod)
S3 = Tod mehrerer Personen
S4 = katastrophale Auswirkungen mit vielen Toten

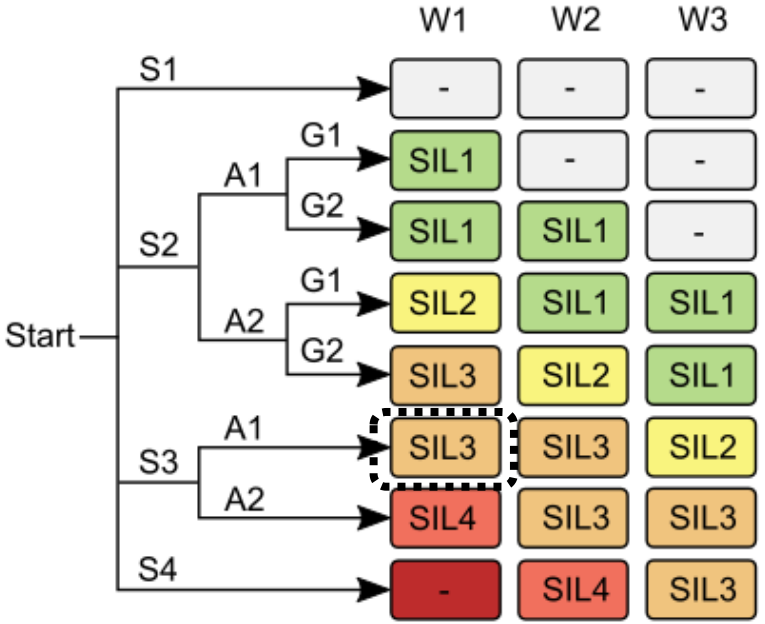
A = Häufigkeit und Dauer des Aufenthalts:
A1 = selten oder kurze Gefährdungsexposition
A2 = häufig (mehr als einmal pro Stunde/Schicht)

G = Möglichkeit zur Vermeidung/Begrenzung des Schadens:
P1 = möglich
P2 = kaum möglich

W = Eintrittswahrscheinlichkeit:
W1 = sehr gering
W2 = gering
W3 = relativ hoch

Sicherheitskonzepte

Beispiel:
Bei einer Brennersteuerung in einem Kraftwerk besteht die Gefahr, dass ein explosives Luft/Gasgemisch im Brennerraum entsteht, wenn die Flamme erlischt und weiterhin Gas ausströmt. Es kann zu einer Explosion komm



S3
A1

S = Schadensausmaß / Schwere der Verletzung:
S1 = leichte (reversible Verletzung)
S2 = ernste (irreversible Verletzung Tod)
S3 = Tod mehrerer Personen
S4 = katastrophale Auswirkungen mit vielen Toten

A = Häufigkeit und Dauer des Aufenthalts:
A1 = selten oder kurze Gefährdungsexposition
A2 = häufig (mehr als einmal pro Stunde/Schicht)

G = Möglichkeit zur Vermeidung/Begrenzung des Schadens:
P1 = möglich
P2 = kaum möglich

W = Eintrittswahrscheinlichkeit:
W1 = sehr gering
W2 = gering
W3 = relativ hoch

Sicherheitskonzepte

PFH - *Probability of Failure per Hour*

SIL	PFH	PFH (power)	RRF
1	0.00001-0.000001	$10^{-5} - 10^{-6}$	100,000–1,000,000
2	0.000001-0.0000001	$10^{-6} - 10^{-7}$	1,000,000–10,000,000
3	0.0000001-0.00000001	$10^{-7} - 10^{-8}$	10,000,000–100,000,000
4	0.00000001-0.000000001	$10^{-8} - 10^{-9}$	100,000,000–1,000,000,000

$$PFH = 1 + \frac{e^{-\lambda T} - 1}{\lambda T}$$

T= Betriebszeit zwischen zwei Wartungen

$\lambda = Ausfallrate$

PFD - *Probability of Failure on Demand*

SIL	PFD	PFD (power)	RRF
1	0.1–0.01	$10^{-1} - 10^{-2}$	10–100
2	0.01–0.001	$10^{-2} - 10^{-3}$	100–1000
3	0.001–0.0001	$10^{-3} - 10^{-4}$	1000–10,000
4	0.0001–0.00001	$10^{-4} - 10^{-5}$	10,000–100,000

Wahrscheinlichkeit eines Ausfalls gerade in dem Moment, wenn eine Schutzfunktion ausgeführt werden soll

Sicherheitskonzepte

Beispiel:
Von 1000 Geräten einer Bau Serie hat innerhalb eines Monats $\Delta n = 1$ Gerät einen Fehler. Berechnen Sie:

PFH
PFD

Sicherheitskonzepte

Gegenmaßnahmen

- Maßnahmen die bis zur Inbetriebnahme entstanden sind. ***(Fehlervermeidung)***
  Umfangreiche Prüfung der Hard- und Software im Rahmen der Qualifizierung.
- Maßnahmen zur ***Fehlerbeherrschung*** während des Betriebs.
  Sowohl Prozessfehler (z.B. Überdruck in einem Behälter) als auch Fehler in der Steuerung (z.B. Ausfall des Eingangskanals des Drucksensors) müssen sicher beherrscht werden.

Sicherheitskonzepte

Sicherheitsgerichtete Steuerungen

Sicherheitsgerichtete Steuerungen können mithilfe von kompakten *sicherheitsgerichteten* SPSen (SSPSen) oder durch Integration von
fehlersicheren Komponenten in Automatisierungssystem realisiert werden.
Sicherheitsgerichtete Steuerung kann durch:

- redundante Aufbau (meistens)
- SSPSen mit Failsafe-Prinzip (neuere Systeme)

realisiert werden.

Sicherheitskonzepte

Sicherheitsgerichtete speicherprogrammierbare Steuerungen (SSPSen) erfüllen im Allgemeinen die Anforderungen bis zur Sicherheitsstufe SIL 3.

Fail-Safe-Prinzip

- Eine SSPS garantiert dass bei Ausfall von Komponenten kein unzulässiger gefährlicher Zustand entstehen kann.
- Sicherheitsfunktion muss durchführt werden wenn die Steuerung selbst einen Fehler hat.
- Zur Erkennung zufälliger Fehler werden umfangreiche Selbsttest durchgeführt.

Sicherheitsgerichtete Steuerung basieren auf dem Prinzip Redundanz und Diversitä

Sicherheitskonzepte

Formen der Redundanz

- Hardware-Redundanz
- Software-Redundanz
- Messwert-Redundanz: redundante Messwerte oder abhängige Messwerte
- Zeit-Redundanz: mehrfache Abfrage des Messwertes in bestimmt Zeitabständen

Sicherheitskonzepte

Formen der Redundanz

- Hardware-Redundanz
- Software-Redundanz
- Messwert-Redundanz: redundante Messwerte oder abhängige Messwerte
- Zeit-Redundanz: mehrfache Abfrage des Messwertes in bestimmt Zeitabständen

Höherer Aufwand führt jedoch zu erhöhter Sicherheit und Verfügbarkeit

Sicherheitskonzepte

Hardware-Redundanz

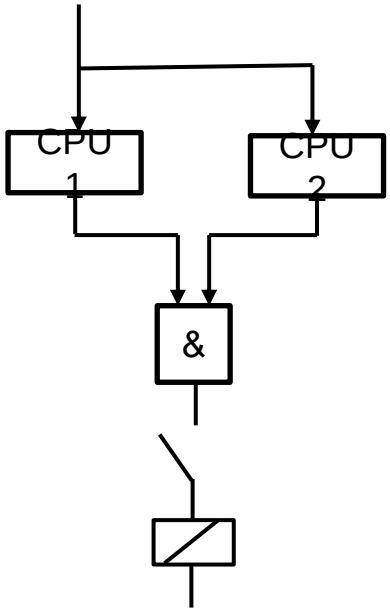
- Ziel: Erkennung von Ausfällen der Hardware

Redundanzmaßnahmen bei Hardware:

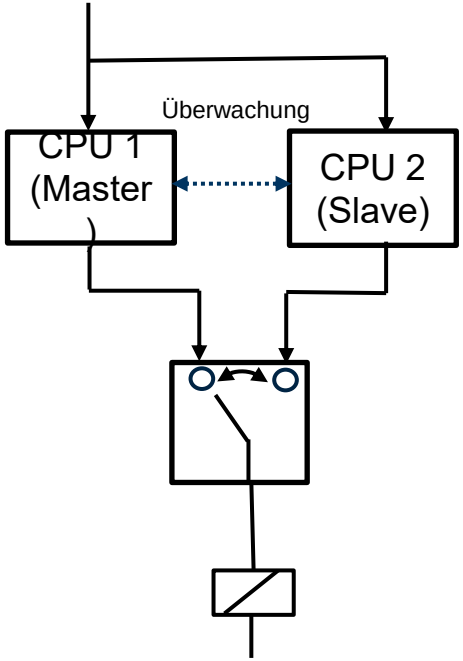
- Statische Redundanz (passive Redundanz) -> alle redundanten Module ständig im Einsatz
- Dynamische Redundanz (aktive Redundanz) -> redundante Module werden erst nach einem Ausfall eingesetzt

Sicherheitskonzepte

Aktive Redundanz

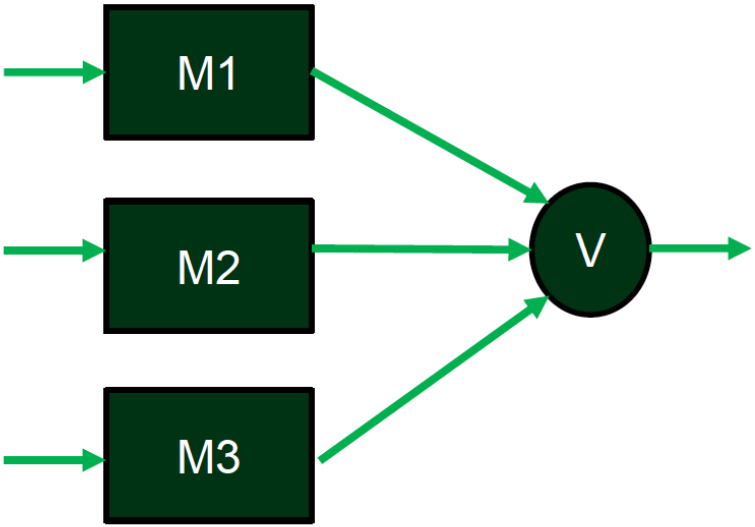


Passive Redundanz



Sicherheitskonzepte

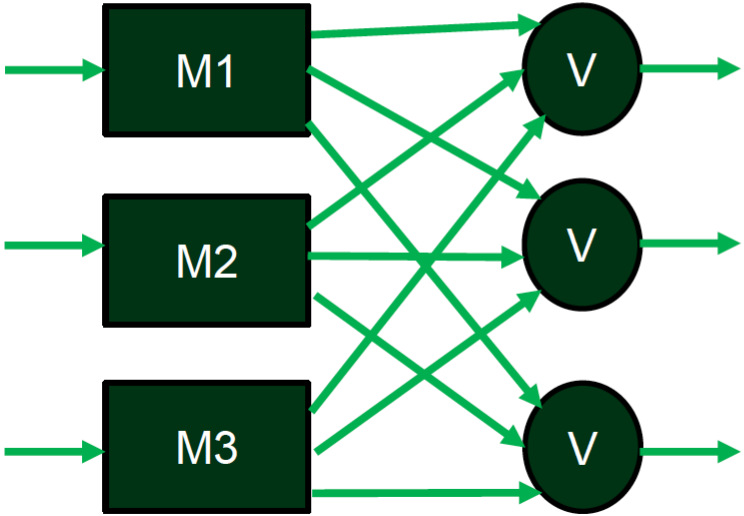
Statische Redundanz z.B. Triple Modular Redundancy (TMR)



- 3 identische Module/Rechner sind ständig im Einsatz
- 1 Vergleicher/Voter – Schwachstelle!!!
- 2- aus-3 Mehrheitsentscheid

Sicherheitskonzepte

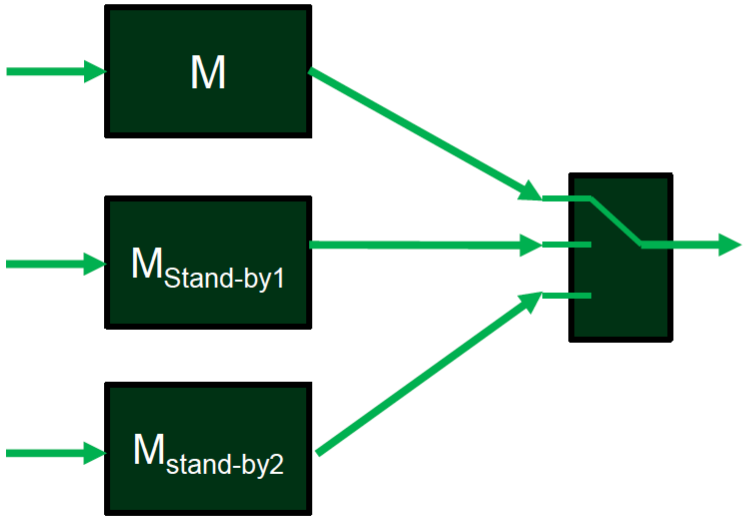
Statische Redundanz z.B. Triple Modular Redundancy (TMR)



- 3 identische Module/Rechner sind ständig im Einsatz
- 3 Vergleicher/Voter – Tolerierung von Voter-Ausfällen
- 2- aus-3 Mehrheitsentscheid

Sicherheitskonzepte

Dynamische Redundanz



- 3 identische Module/Rechner
- 1 Modul ist im Einsatz
- 2 Module sind Stand-by

Sicherheitskonzepte

Software-Redundanz

- Ziel: Erkennung von Fehler in der Software

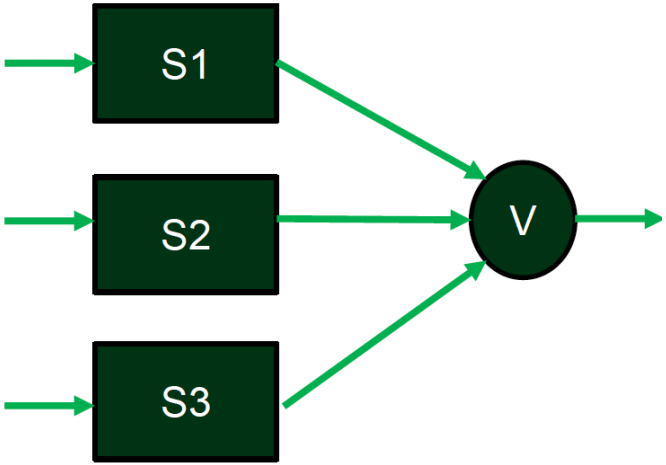
Redundanzmaßnahmen bei Software:

- Diversitäre Software
- Recovery Block

Sicherheitskonzepte

Diversitäre Software :

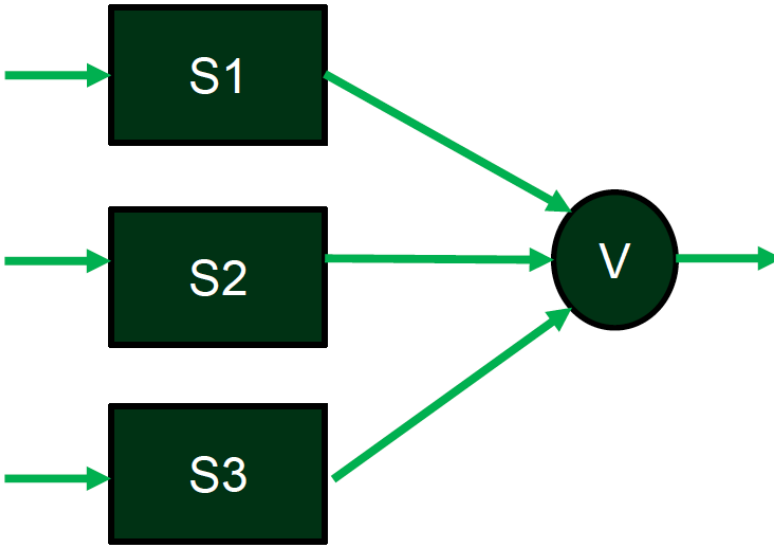
- Unabhängige Entwicklerteams lösen dieselbe Aufgabe
- Gezielte Entwicklung verschiedener Strategien, Algorithmen und Software-Strukturen
- alle Programme laufen gleichzeitig aktiv redundant mit den gleichen Eingaben
- die mehrfache Ausgabe wird durch einen Mehrheitsentscheid (Voter) in eine einzige Ausgabe überführt



Sicherheitskonzepte

Diversitäre Software: Probleme

- ein exakter Vergleich *(Voting)* nicht immer möglich -> eine Berechnung mit Gleitkommazahlen kann mit unterschiedlicher Rechenreihenfolge unterschiedliche Rundungsfehler erzeugen
- die Laufzeit wird immer von der langsamsten Software bestimmt



Sicherheitskonzepte

Recovery Block

- in einer Komponente werden kritische Kodepassagen in mehreren Versionen implementiert
- die Komponente führt zuerst die Primärversion aus und prüft das Ergebnis durch einen Akzeptanztest gegen die Spezifikation
- ist ein Fehler aufgetreten, wird der ursprüngliche Zustand wiederhergestellt und die nächste alternative Version benutzt

Sicherheitskonzepte

Recovery Block: Probleme

- Akzeptanztest = Plausibilitätstest für die Ausgangsgrößen
- Laufzeit wird stark beeinflusst, da die Recovery Block sequentiell aufgerufen werden

FRAGEN

1. Welche Normen und Normengruppen gibt es im Bereich der Maschinenrichtlinie und was beinhalten die Gruppen? Wie geht man bei nicht vorhandenen C-Normen vor?
2. Erläutern Sie die Begriffe fail-safe, Redundanz, Diversität und Einfehlersicherheit mit Hinblick auf Sicherheitsaspekte an einer Maschine.
3. Skizzieren Sie den Zusammenhang zwischen Risiko, Sicherheit und Gefahr. Wie kann das Grenzrisiko bei technischen Produktionsanlagen definiert werden?
4. Nennen Sie Maßnahmen zur Verringerung des Gesamtrisikos an technischen Einrichtungen.
5. Stellen Sie den Ablauf einer Risikobeurteilung schematisch dar.
6. Nennen Sie die drei grundsätzlichen Schritte bei einer Risikoanalyse.
7. Skizzieren Sie den Risikograph zur Risikoabschätzung an Maschinen nach DIN-EN 13849-1.
8. Welche steuerungstechnischen Maßnahmen sind in den Kategorien B, 1, 2, 3 und 4 erforderlich? Welche Folgen durch mögliche Fehler können in den jeweiligen Kategorien auftreten?
9. Nennen Sie Beispiele für trennende und nicht-trennende Schutzeinrichtungen.