Validieren und Verifizieren von Steuerungen

Ist das was funktioniert auch sicher genug ?

Dipl.-Ing. Berthold Heinke

Dipl.-Ing. Berthold Heinke

Berufsgenossenschaft Holz und Metall, Düsseldorf

bis 31.12.2010: Leiter der Fachstelle Elektrotechnik der MMBG

Stellvertr. Leiter der Prüf- und Zertifizierungsstelle MHHW (Notified Body)

- Studium der Elektrotechnik an der Ruhr-Universität Bochum

  Schwerpunkt: elektrische Steuerungs- und Regelungstechnik

- Mehrjährige Industrietätigkeit im Bereich der Entwicklung und Applikation von Automatisierungssystemen

- Seit 1991 tätig bei der Maschinenbau- und Metall BG , seit 2011: BGHM
  - (Pressen-) Sicherheitssteuerungen
  - Optische Schutzeinrichtungen (BWS, Kamerasysteme)
  - Sicherheitsbussysteme
  - Pressen, Kunststoffspritzgießmaschinen, Hebezeuge

- Mitglied im nationalen und internationalen Komitee zu EN ISO 13849-1 ,
- EN ISO 13849-2 sowie im DKE K225 (EN 60204-1 und EN 60204-32)

Haben Sie auch wirklich das gebaut,

was Sie bauen sollten / wollten ?

Validierung

Validierung (von lat. *validus*: *stark, wirksam, gesund*)

Quelle: Wikipedia

- ist die Prüfung einer These, eines Plans oder Lösungsansatzes in Bezug auf das zu lösende Problem,

- ist eine Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind.

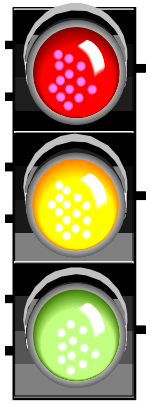
Welche ?

Wie kann der Nachweis erfolgen ?

Nicht nur elektrische Steuerungen.

1.2.1 Sicherheit und Zuverlässigkeit von Steuerungen

(alt: 1.2.1 und 1.2.7)



Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kommt. Insbesondere müssen sie so ausgelegt und beschaffen sein, dass

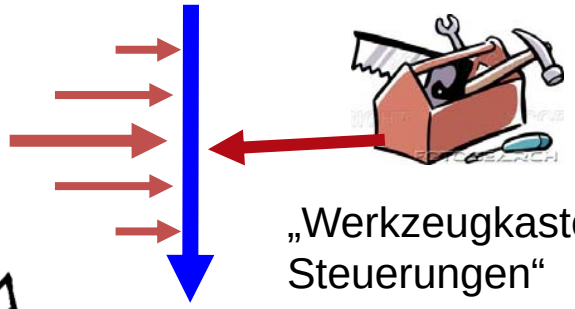
- sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten;
- **Fehler in der Logik** nicht zu Gefährdungssituationen führen.
- ein **Defekt** der Hardware oder der Software der Steuerung nicht zu Gefährdungssituationen führt

ZIEL EG-Konformitätserklärung

Übereinstimmung mit
allen zutreffenden
europäischen Richtlinien

CE

Vielzahl von
Anforderungen



„Werkzeugkasten
Steuerungen“

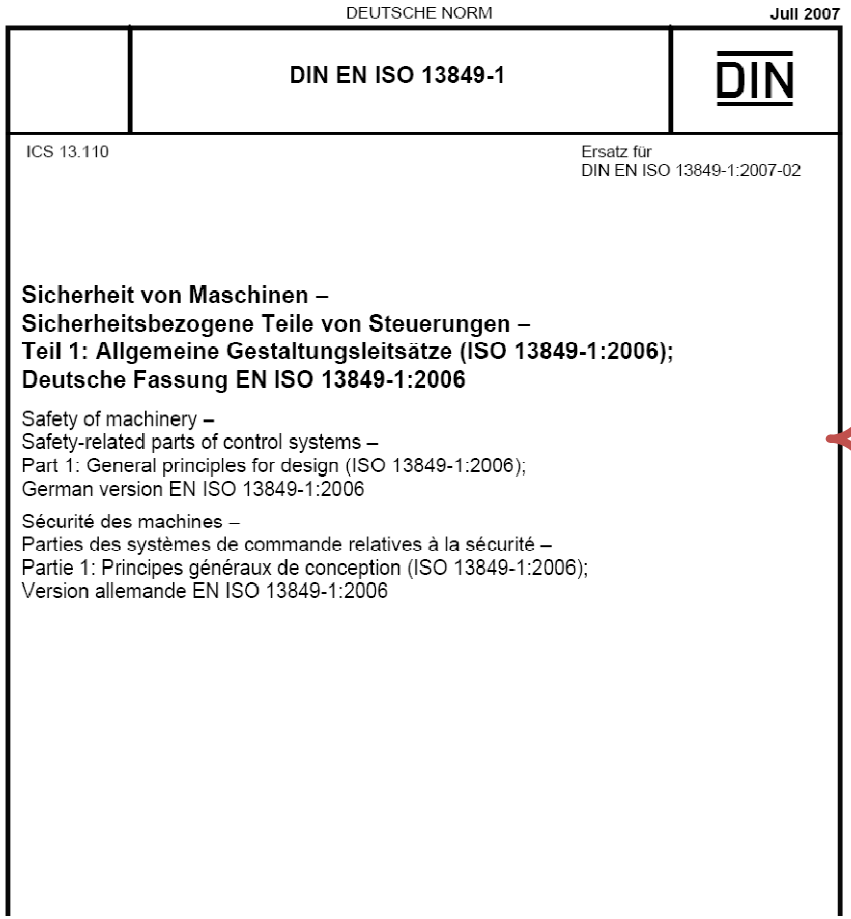
Anforderungen aus der MRL

- C-Norm
  - EN 60204-1
  - EN 954-1
  - EN ISO 13849-2
  - EN ISO 13849-1
  - EN 62061

Fehlervermeidende Maßnahmen,
Fehlerarten, Bewertungsverfahren

Sicherheitsbezogene Teile von Steuerungen- Allgemeine Gestaltungsleitsätze

EN ISO 13849-1



DEUTSCHE NORM Juli 2007

DIN EN ISO 13849-1

DIN

ICS 13.110

Ersatz für
DIN EN ISO 13849-1:2007-02

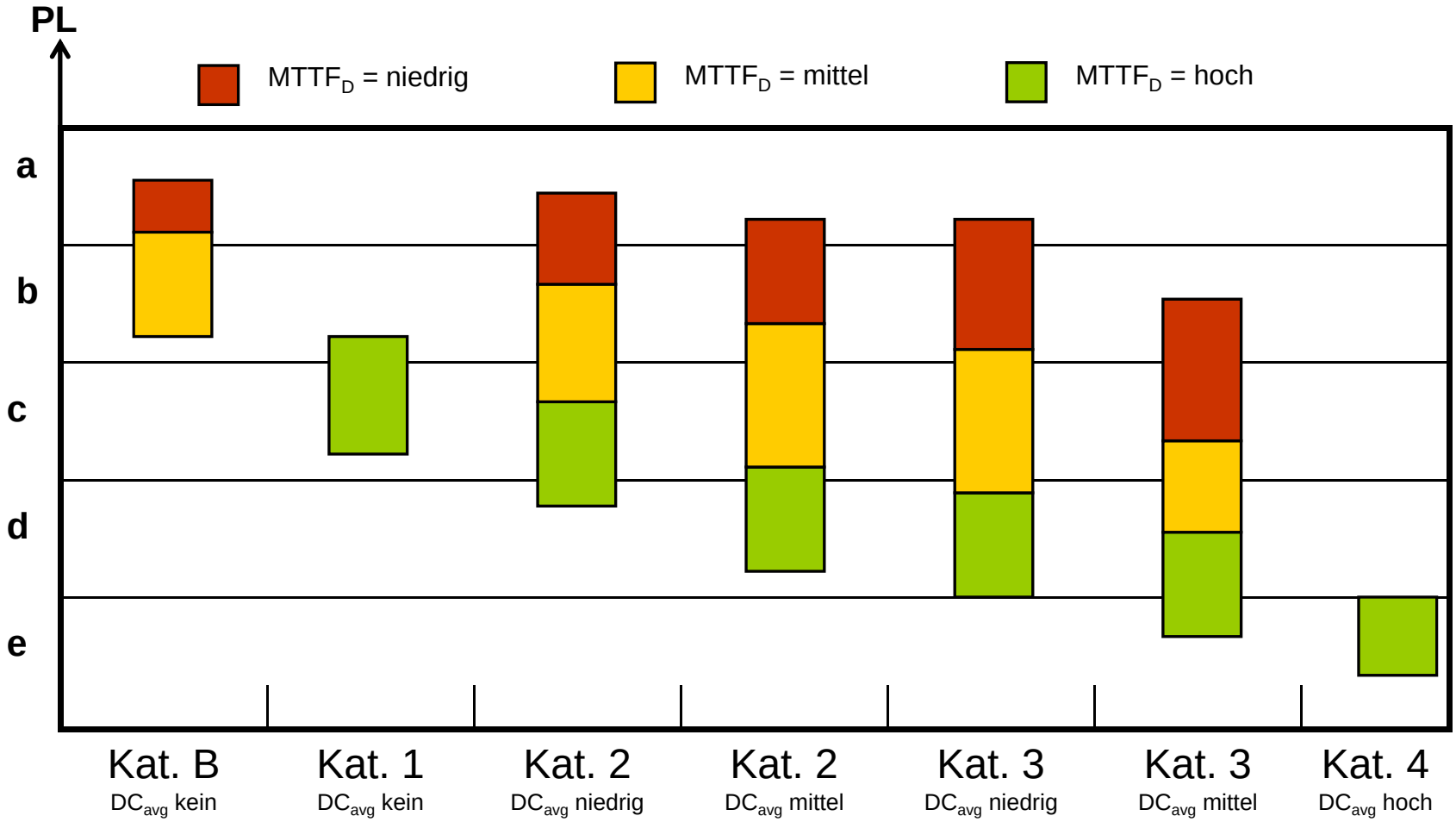
Sicherheit von Maschinen –
Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006);
Deutsche Fassung EN ISO 13849-1:2006

Safety of machinery –
Safety-related parts of control systems –
Part 1: General principles for design (ISO 13849-1:2006);
German version EN ISO 13849-1:2006

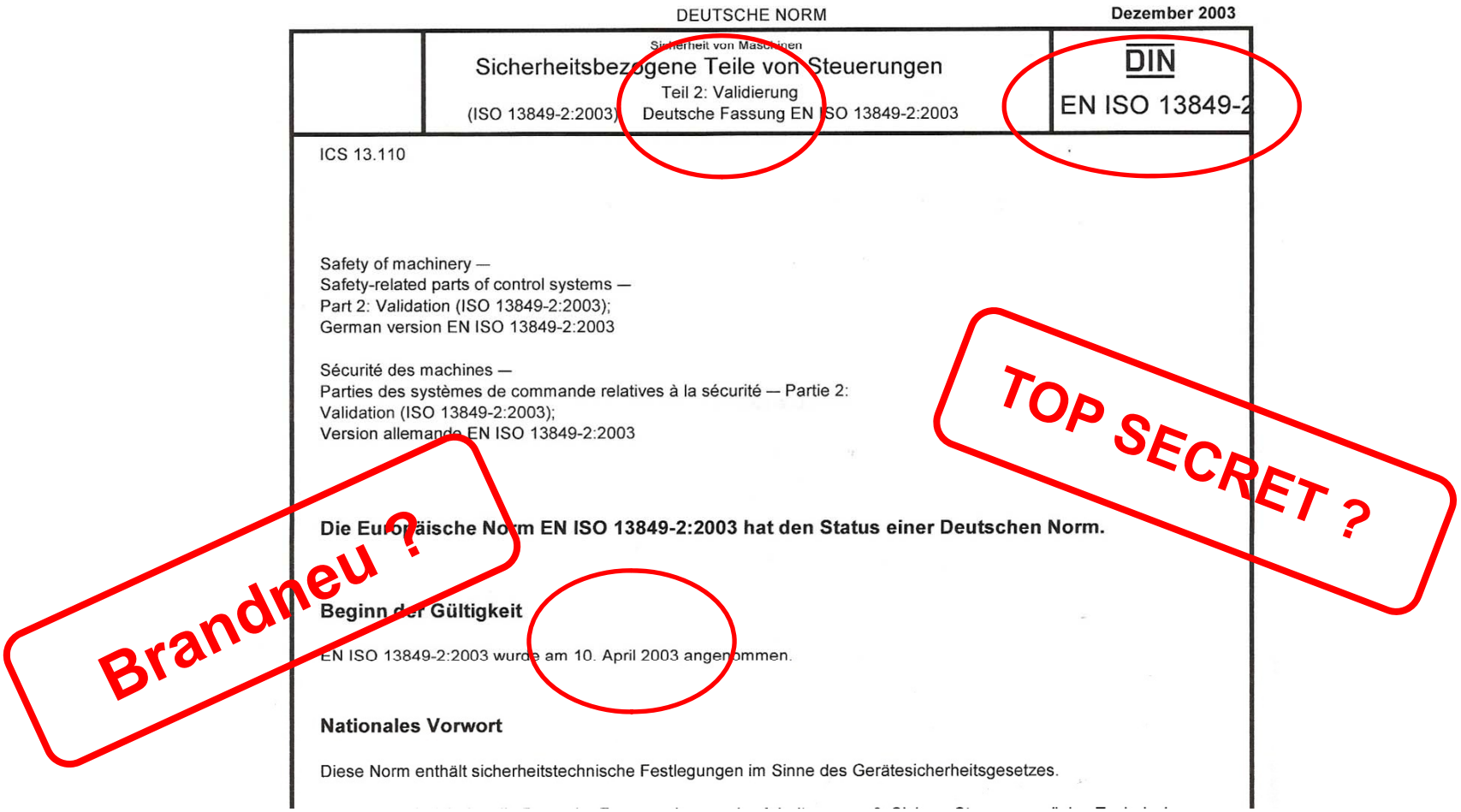
Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité –
Partie 1: Principes généraux de conception (ISO 13849-1:2006);
Version allemande EN ISO 13849-1:2006

- Risikograph
- PL : Performance Level
  - Kategorie
  - $MTTF_d$: „Bauteilgüte“
  - DC : „Fehlererkennung“
  - CCF: Fehler gemeinsamer Ursache
- Software Anforderungen

Beziehungen zwischen den Kategorien, DC_{avg}, $MTTF_d$ jedes Kanals und PL



Validierung: EN ISO 13849-2



DEUTSCHE NORM Dezember 2003

Sicherheit von Maschinen
Sicherheitsbezogene Teile von Steuerungen
Teil 2: Validierung
(ISO 13849-2:2003) Deutsche Fassung EN ISO 13849-2:2003

DIN
EN ISO 13849-2

ICS 13.110

Safety of machinery —
Safety-related parts of control systems —
Part 2: Validation (ISO 13849-2:2003);
German version EN ISO 13849-2:2003

Sécurité des machines —
Parties des systèmes de commande relatives à la sécurité — Partie 2:
Validation (ISO 13849-2:2003);
Version allemande EN ISO 13849-2:2003

Die Europäische Norm EN ISO 13849-2:2003 hat den Status einer Deutschen Norm.

Beginn der Gültigkeit

EN ISO 13849-2:2003 wurde am 10. April 2003 angenommen.

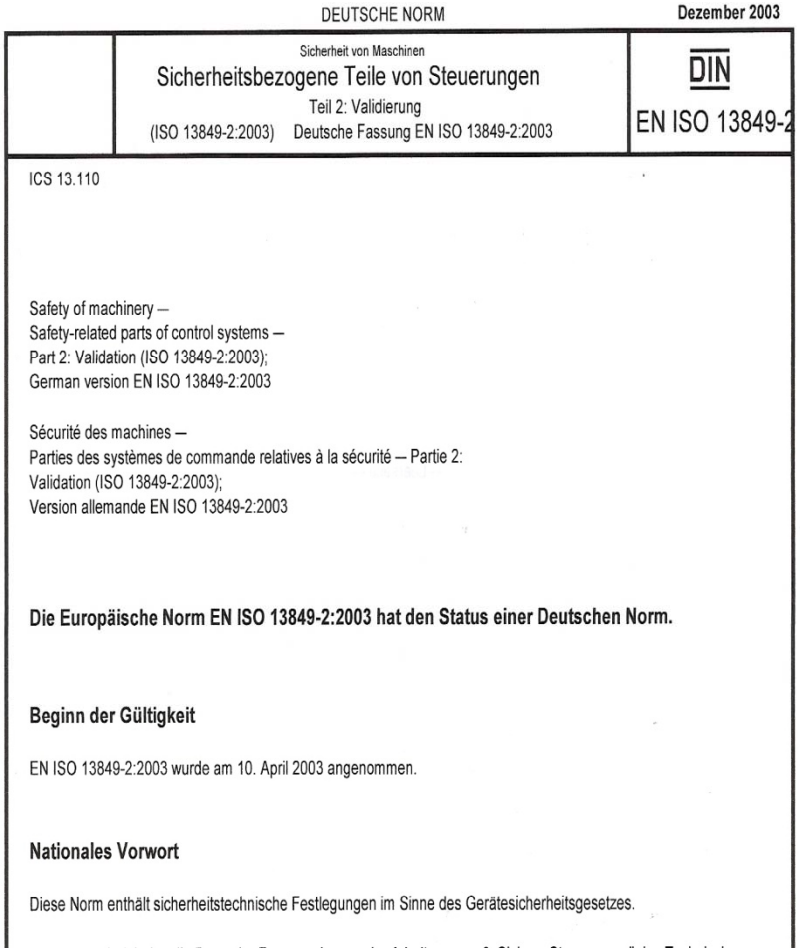
Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Gerätesicherheitsgesetzes.

Brandneu ?

TOP SECRET ?

Validierung: EN ISO 13849-2



DEUTSCHE NORM Dezember 2003

Sicherheit von Maschinen
Sicherheitsbezogene Teile von Steuerungen
Teil 2: Validierung
(ISO 13849-2:2003) Deutsche Fassung EN ISO 13849-2:2003

DIN
EN ISO 13849-2

ICS 13.110

Safety of machinery –
Safety-related parts of control systems –
Part 2: Validation (ISO 13849-2:2003);
German version EN ISO 13849-2:2003

Sécurité des machines –
Parties des systèmes de commande relatives à la sécurité – Partie 2:
Validation (ISO 13849-2:2003);
Version allemande EN ISO 13849-2:2003

Die Europäische Norm EN ISO 13849-2:2003 hat den Status einer Deutschen Norm.

Beginn der Gültigkeit

EN ISO 13849-2:2003 wurde am 10. April 2003 angenommen.

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen im Sinne des Gerätesicherheitsgesetzes.

Derzeitige Version bezieht sich auf EN 954-1

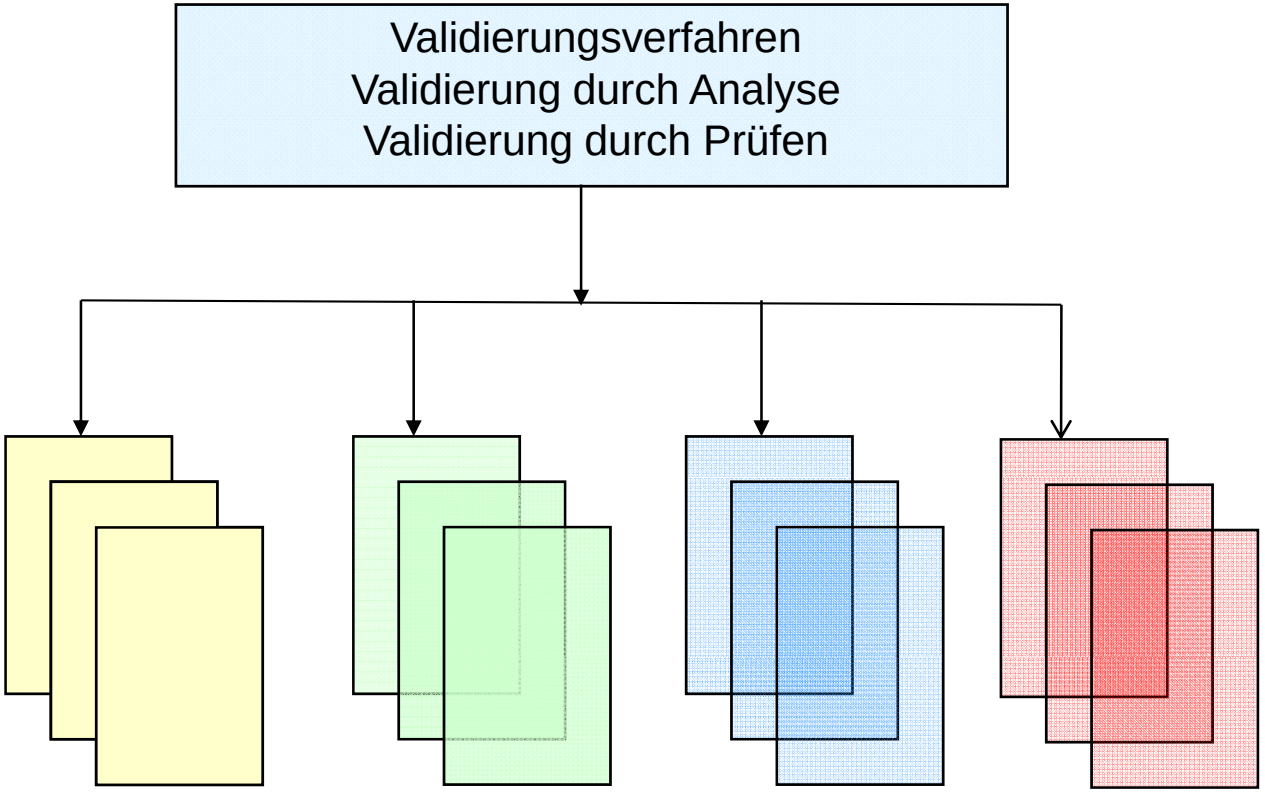
EN ISO 13849-2 ist aktuell in der Überarbeitung, um

Anpassungen an EN ISO13849-1 einzufügen

Hinweise zu $MTTF_d$, DC, CCF aufzunehmen

Aktualisierungen durchzuführen

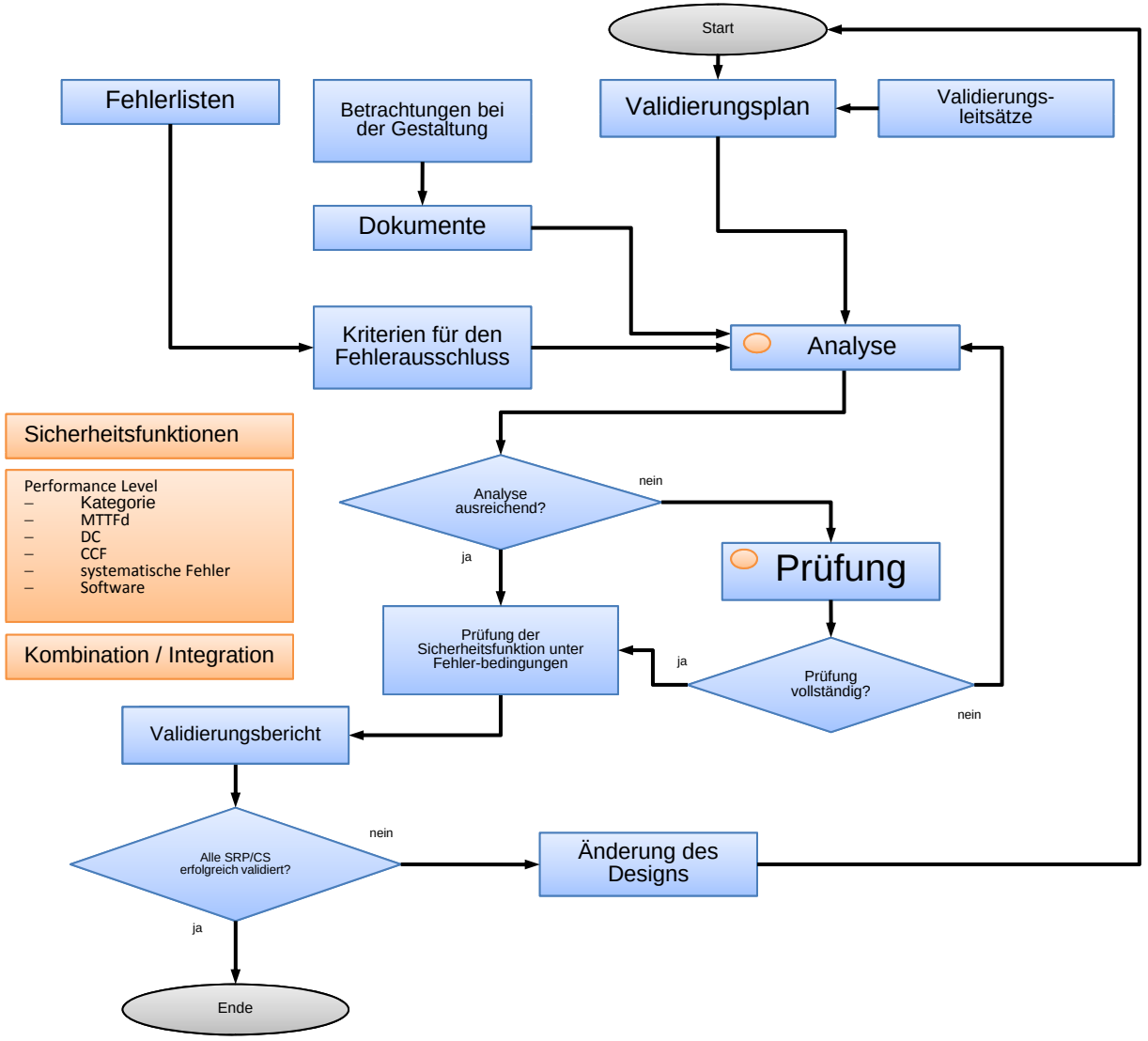
EN ISO13849-2 Validierung



Anhang:	Anhang:	Anhang:	Anhang:
Validierung mechanischer Systeme	Validierung pneumatischer Systeme	Validierung hydraulischer Systeme	Validierung elektrischer Systeme

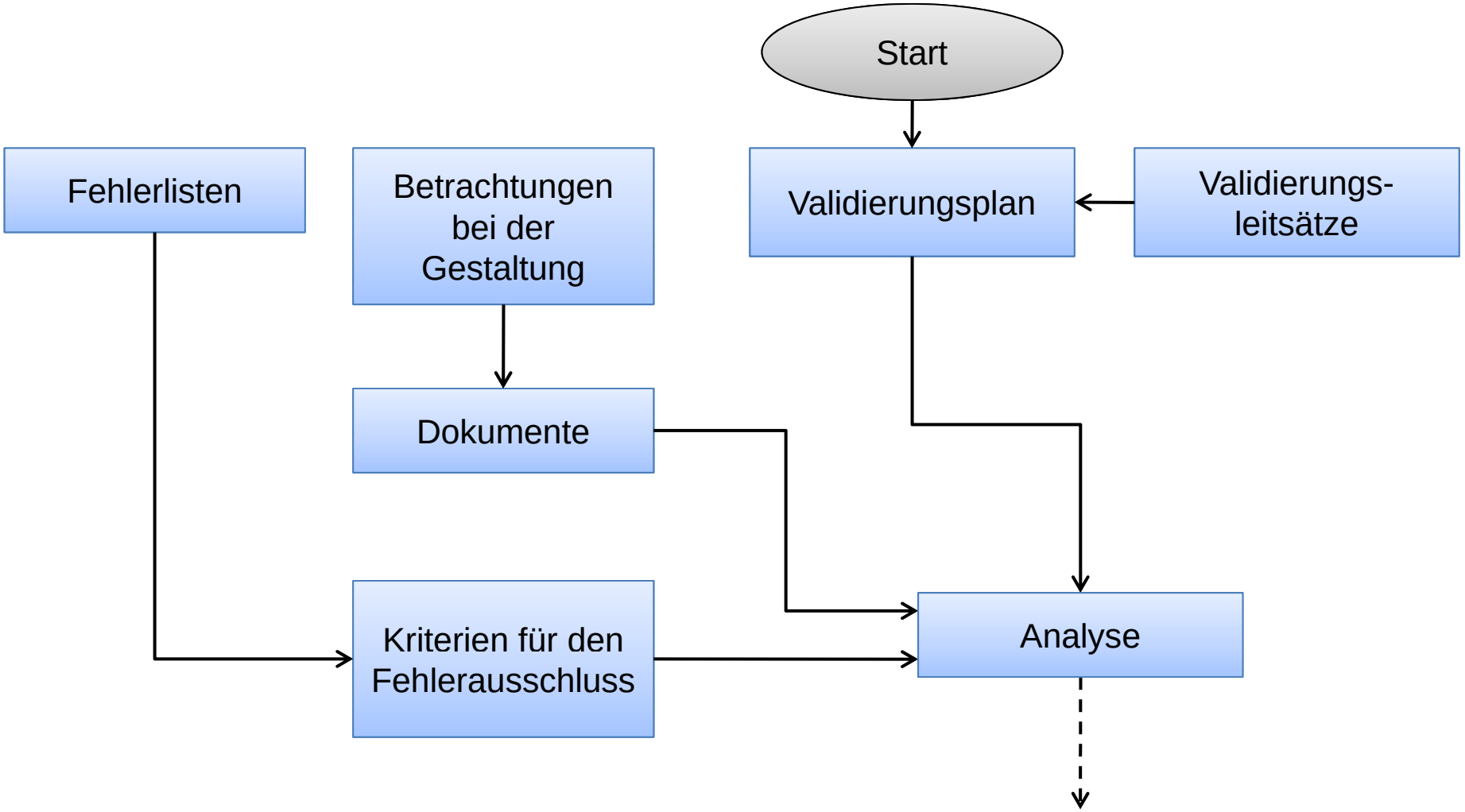
Übersicht über das Validierungsverfahren

Entwurf der Überarbeitung der EN ISO 13849-2



Übersicht über das Validierungsverfahren

Entwurf der Überarbeitung der EN ISO 13849-2



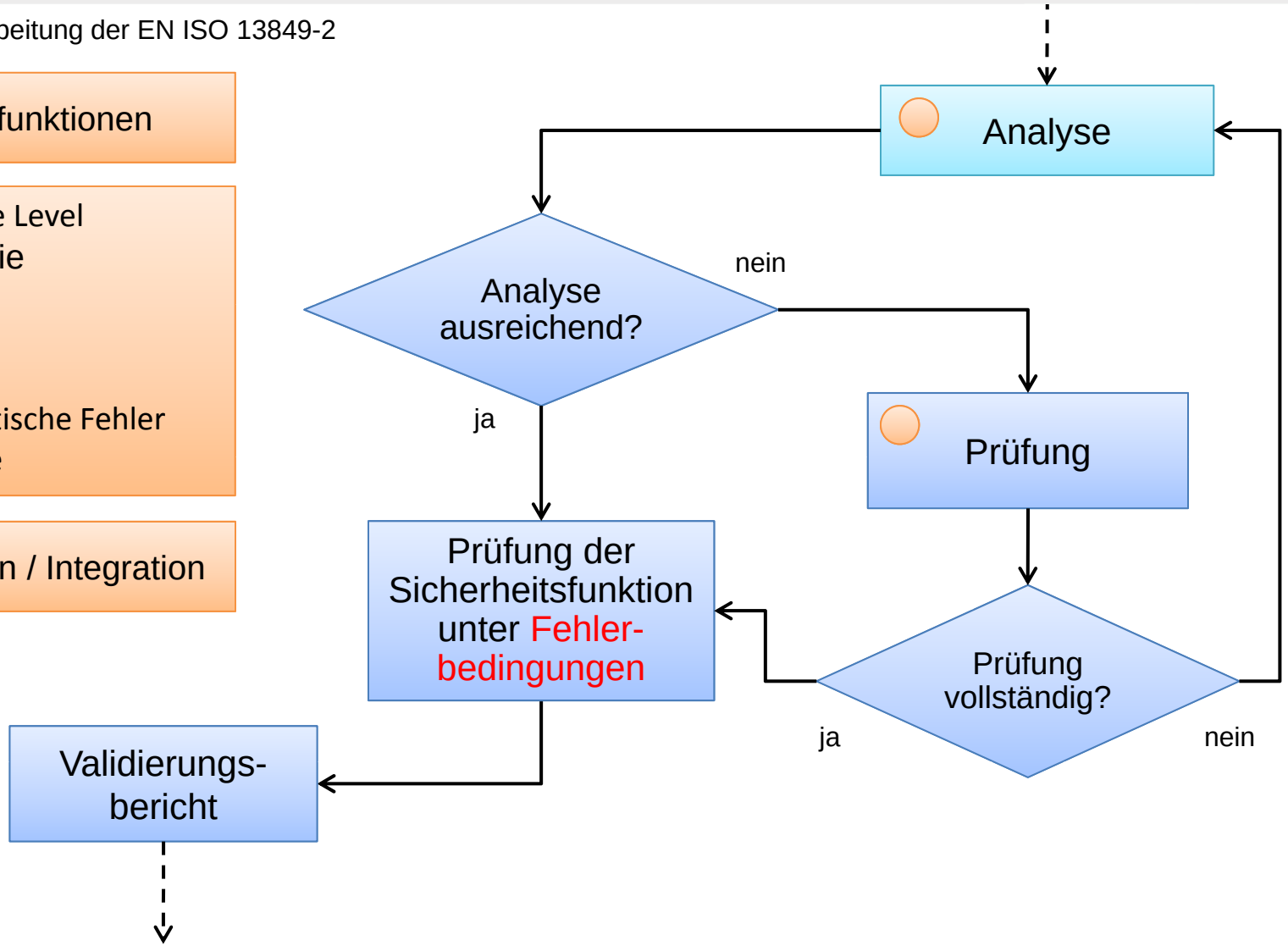
Übersicht über das Validierungsverfahren

Entwurf der Überarbeitung der EN ISO 13849-2

Sicherheitsfunktionen

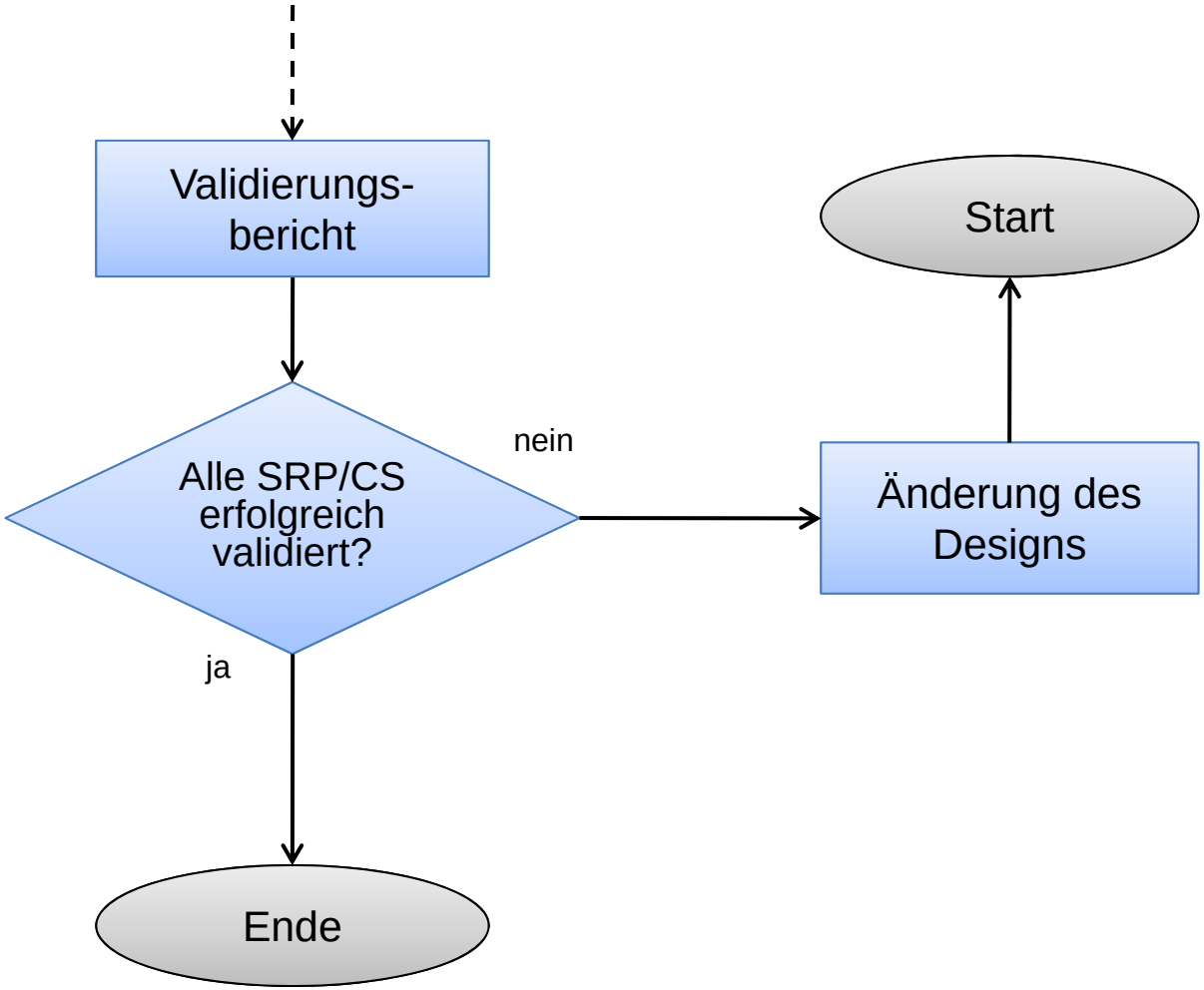
Performance Level
- Kategorie
- MTTFd
- DC
- CCF
- systematische Fehler
- Software

Kombination / Integration



Übersicht über das Validierungsverfahren

Entwurf der Überarbeitung der EN ISO 13849-2



Grundsätzlicher Aufbau der Anhänge

- Liste der grundlegenden Sicherheitsprinzipien
- Liste der bewährten Sicherheitsprinzipien
- Liste der bewährten Bauteile
- Fehlerlisten und Fehlerausschlüsse

Liste der grundlegenden Sicherheitsprinzipien

Validierung elektrischer Systeme : Auszug aus EN ISO 13849-2 Anhang D.2

Grundlegendes Sicherheitsprinzip	Bemerkung
Richtige Schutzleiterverbindung	Eine Seite des Steuerstromkreises ist mit SL zu verbinden
Verträglichkeit	Bauteile verwenden, die für die angewendeten Spannungen und Ströme geeignet sind
Prinzip der Energietrennung	Sicherer Zustand wird durch Abtrennen von der Energiequelle erreicht

Validierung elektrischer Systeme : Auszug aus EN ISO 13849-2 Anhang D.3

Bewährtes Sicherheitsprinzip	Bemerkung
Mechanisch verbundene Kontakte	Anwendung z.B. für Überwachungsfunktionen
Zwangläufiger Betätigungsmodus	Direkte Aktion wird durch Formschluss ohne elastische Elemente übertragen, keine Anwendung von Federn zwischen Stellglied und Kontakten
Fehlervermeidung in Kabeln	Vermeidung von Kurzschlüssen zwischen zwei benachbarten Leitungen • Abschirmung mit Verbindung zu SL an jeder einzelnen Leitung • SL zwischen allen Signalleitungen in Flachkabeln

Validierung elektrischer Systeme : Auszug aus EN ISO 13849-2 Anhang D.4

Bewährtes Bauteil	Bedingung für „bewährt“
Schalter mit zwangläufigem Betätigungsmodus (direktöffnend) z.B. • Tastschalter, Positionsschalter, nockenbetätigter Wahlschalter (z.B. für Betriebsartenwahl)	Norm: EN 60947-5-1
Kabel	Die Verkabelung außerhalb umschlossener Einbauräume sollte gegen mechanische Beschädigung (einschließlich z.B. Schwingung oder Biegung) geschützt werden

Validierung elektrischer Systeme : Auszug aus EN ISO 13849-2 Anhang D.4

Bewährtes Bauteil	Bedingung für „bewährt“
Hilfsschütz (z.B. Relais)	Nur bewährt, wenn: • andere Einflüsse berücksichtigt sind z.B. Schwingungen und • zwangsläufig erregte Funktion vorliegt und • Ausfall durch geeignete Verfahren vermieden ist z.B. Überdimensionierung und • Strom in Kontakten durch Sicherungen oder Schutzschalter begrenzt ist, um ein Verschweißen der Kontakte zu vermeiden und • Kontakte zwangsgeführt sind, wenn sie für Überwachungen angewendet werden

Auszug aus EN ISO 13849-2 Tabelle D.8

D.9 Elektromechanischer Positionsschalter

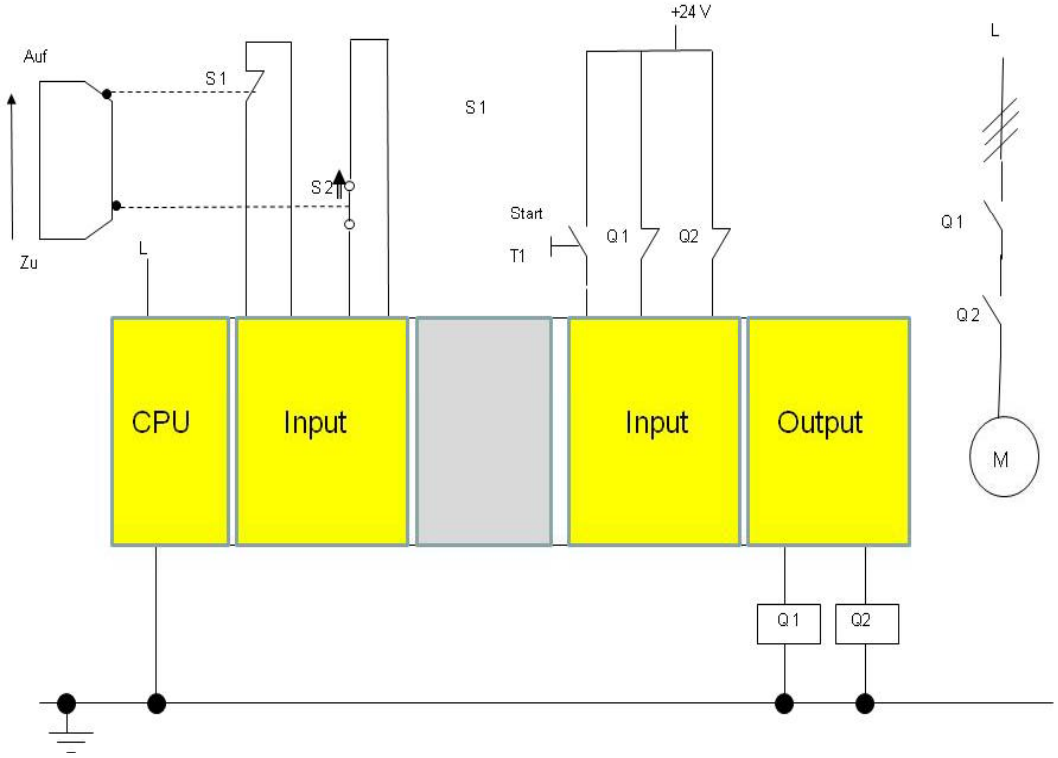
Fehlerannahme	Fehlerausschluss	Bemerkung
Nichtschließen von Kontakten	NEIN	
Nichtöffnen von Kontakten	Kontakte nach IEC 60947-5-1 Anhang K öffnen sich	
Kurzschluss von benachbarten Kontakten, die von einander isoliert sind	Kurzschlüsse für Schalter nach IEC 60947-5-1 (Siehe 1)	1) Leitfähige Teile, die sich lösen, sollten die Isolation zwischen Kontakten nicht überbrücken können
Gleichzeitiger Kurzschluss zwischen den 3 Klemmen von Wechselkontakten	Gleichzeitige Kurzschlüsse für Schalter nach IEC 60947-5-1 (Siehe 1)	

Anmerkung: Fehlerlisten für mechanische Gesichtspunkte siehe Anhang A

D.9 Elektromechanische Einrichtungen (z.B. Relais, Schütze)

Fehlerannahme	Fehleraus-schluss	Bemerkung
Alle Kontakte bleiben unter Spannung, wenn die Spule abgeschaltet ist (z.B. mechanischer Fehler)	NEIN	
Alle Kontakte bleiben abgeschaltet, wenn die Energie ansteht (z.B. mechanischer Fehler, Unterbrechung der Spule)	NEIN	
Nichtöffnen / Nichtschließen von Kontakten	NEIN	
Gleichzeitiger Kurzschluss zwischen zwei Kontakten untereinander und/oder zwischen Kontakt und Wicklung	JA, wenn 1) und 2) zutreffen	1) Kriech- und Luftstrecken entsprechen IEC 60664-1 Verschmutzungsgrad 2 / Einsatzklasse III
Gleichzeitiger Kurzschluss zwischen den 3 Klemmen eines Wechselkontaktes	JA, wenn 1) und 2) zutreffen	2) Leitfähige Teile, die sich lösen , können die Isolation zwischen den Kontakten und der Spule nicht überbrücken
Gleichzeitiges Geschlossensein von NO und NC Kontakten	Ja wenn 3) zutrifft	3) Verwendung zwangsläufig betätigter Kontakte

Stellungsüberwachung einer Beweglichen Schutzeinrichtung



Funktionsbeschreibung:

Sicherung einer Gefahrenstelle durch eine Schutztür.

Stellung der Schutztür wird durch Positionsschalter S1 und S 2 überwacht.

Sicherheits-SPS wertet S1 und S 2 aus.

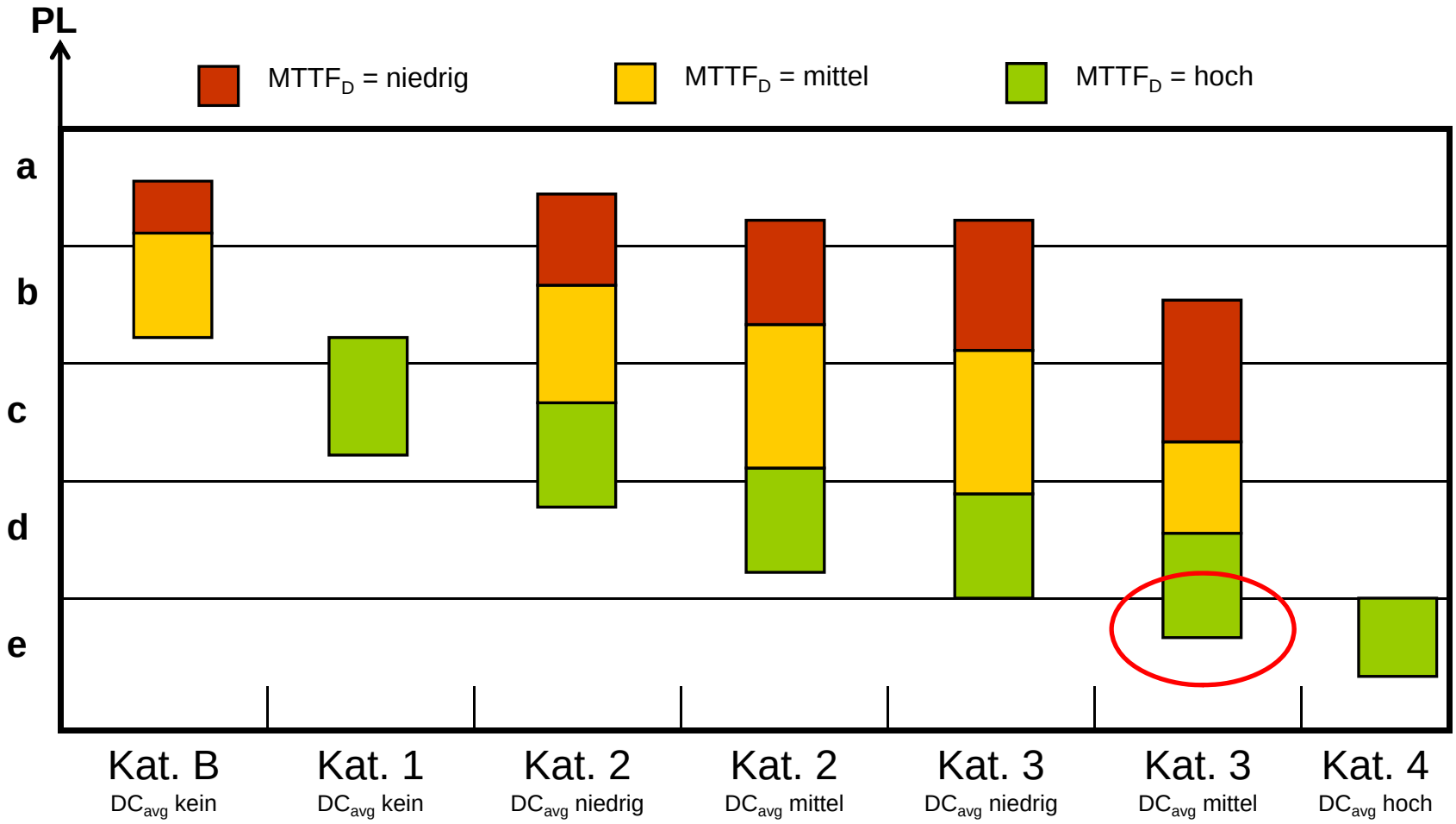
Sicherheits-SPS steuert 2 Schütze Q1 und Q 2 durch deren Abfallen der Motor M gestoppt wird und ein unerwarteter Anlauf verhindert wird.

Q1 und Q2 werden über Sicherheits-SPS überwacht

Sicherheitsfunktion:

Durch Öffnen der Schutztür wird eine sicherheitsgerichtete Stoppfunktion eingeleitet

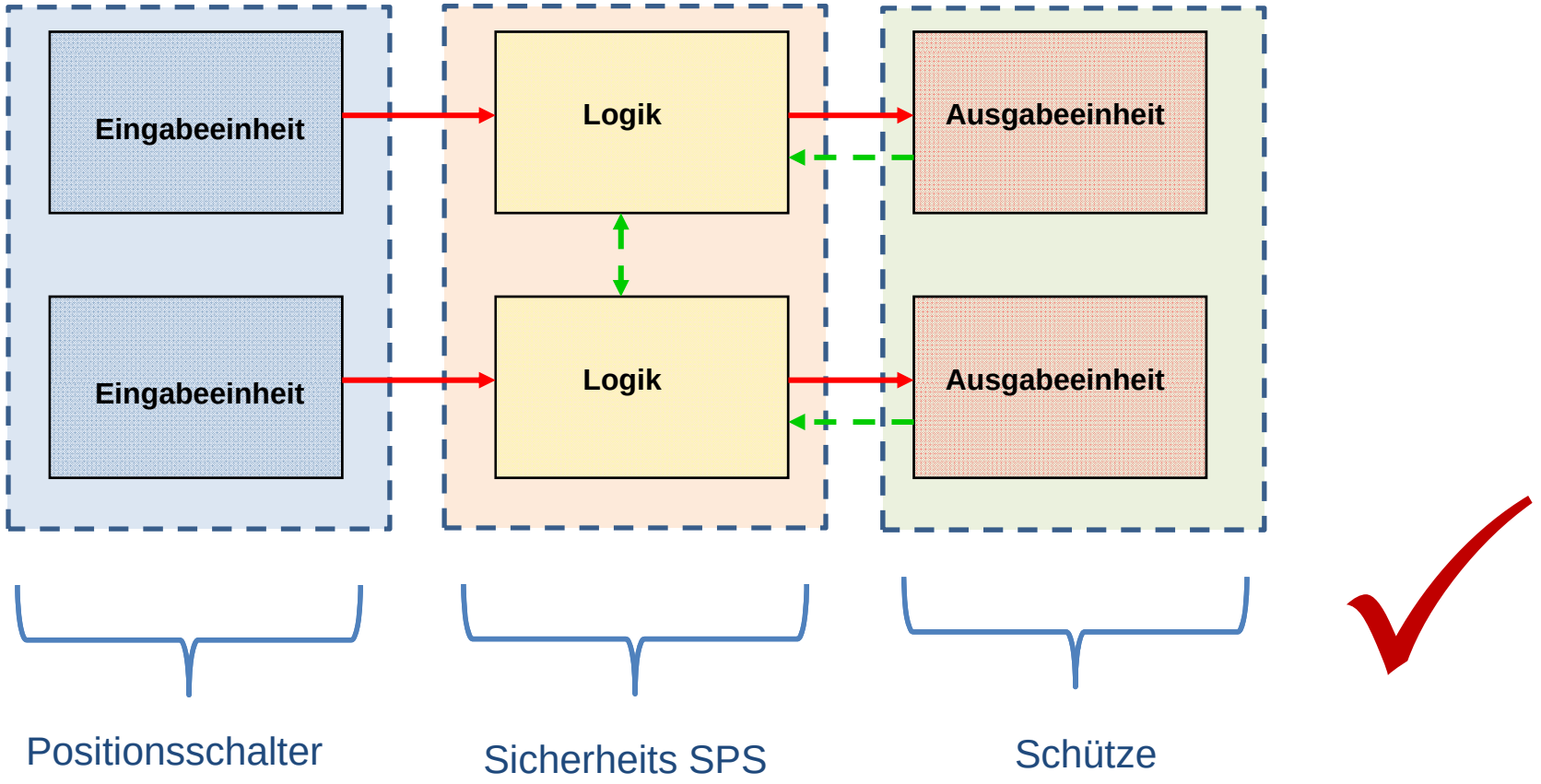
Realisierte Lösung



Es ist zu überprüfen, dass mit der Lösung nachfolgende Bedingungen eingehalten werden:

- Struktur der Lösung entspricht der Kategorie 3
- $MTTF_d$ der Sicherheitsfunktion beträgt mindestens: 62 Jahre
- DC_{avg} der Sicherheitsfunktion ist mittel
- CCF ist besser als 65 Punkte

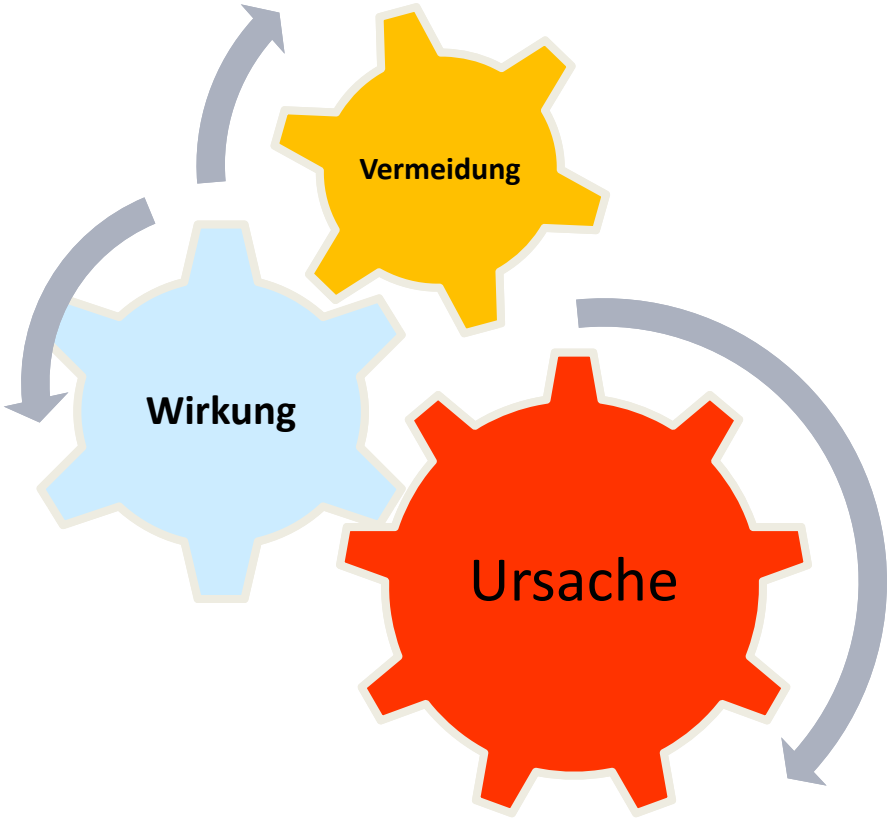
Struktur: Kategorie 3



Kategorie 3	Überprüfung
Anforderungen der Kategorie B sind erfüllt;	• der technischen Dokumentation der verwendeten Bauteile bzgl. der Einsatzbedingungen
bewährte Sicherheitsprinzipien (wenn anwendbar) sind erfüllt	• der technischen Dokumentation (Schaltungsunterlagen)
ein Einzelfehler führt nicht zum Verlust der Sicherheitsfunktion	• Theoretisch und praktisch z.B. durch Fehlermode Effekt Analyse FMEA
Einzelfehler werden erkannt	• Theoretisch und praktisch z.B. durch Fehlermode Effekt Analyse FMEA
$MTTF_d$ jedes Kanals beträgt mindestens 3 Jahre	Siehe Überprüfung von $MTTF_d$ Achtung: in Abhängigkeit vom PL kann höherer Wert erforderlich sein
DC_{avg} beträgt mindestens 60 %	Siehe Überprüfung von DC_{avg} Achtung: in Abhängigkeit vom PL kann höherer Wert erforderlich sein
CCF beträgt mindestens 65 Punkte	Siehe Überprüfung CCF

Analyse und Validierungswerkzeug

FMEA



FMEA : **F**ehler **M**ode **E**ffekt **A**nalyse

Verfahren zur Ermittlung der Art und Weise, in der Komponenten und Systeme ausfallen können und nicht mehr die Sollfunktion erbringen (gem. E DIN IEC 60300-3-9)

- Ausfallarten
- Auswirkungen der Ausfälle
- Ausfallursachen
- Vermeidung oder Verminderung der Ausfälle

FMEA : Anwendung

WANN: In der Entwicklung, Fertigung oder Betriebsphase

WOZU: Auswahl von Entwurfsalternativen

Berücksichtigung aller Ausfallarten und deren Auswirkungen

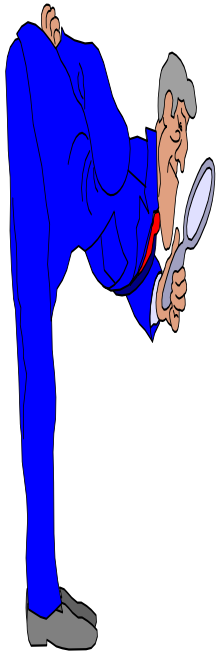
Grundlage für die Prüfplanung und Instandhaltung

Grundlagen für Zuverlässigkeitsanalysen

FMEA: prinzipielle Vorgehensweise

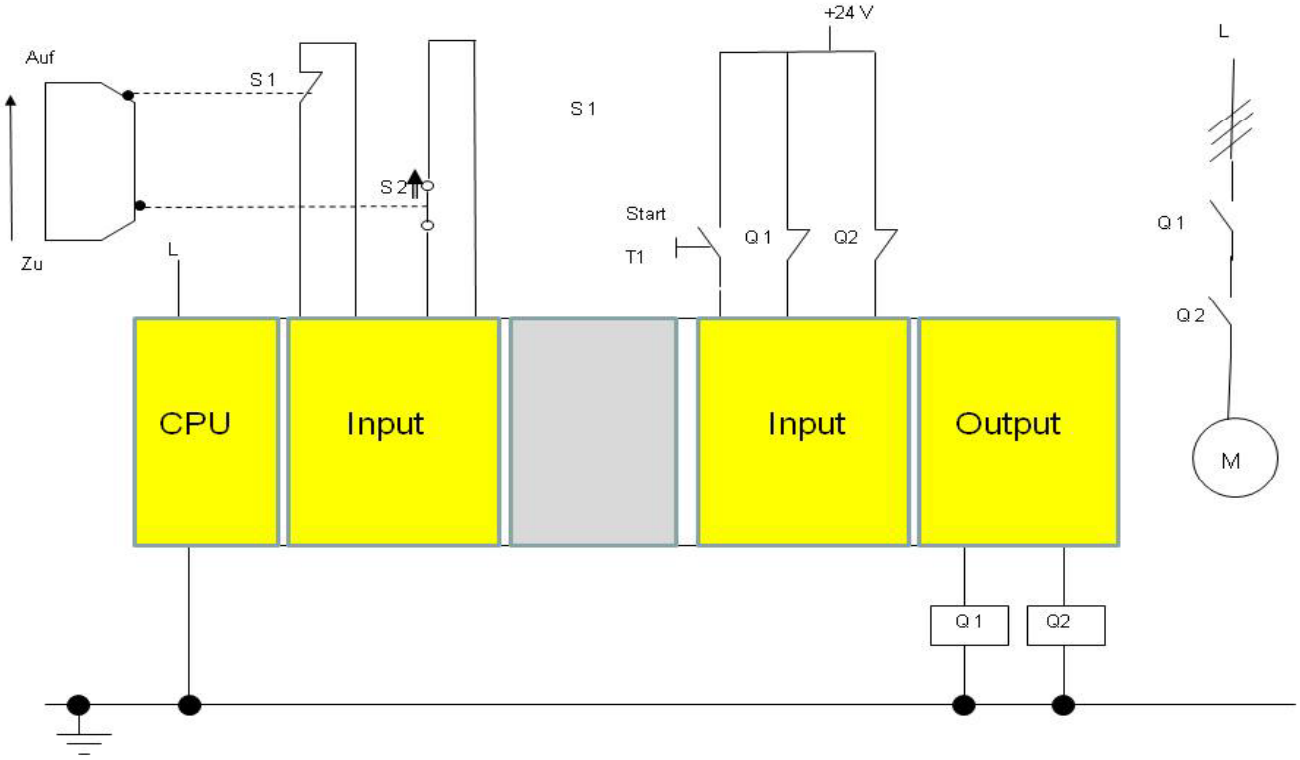
1. System verstehen
2. System in Komponenten aufteilen
3. Analyse jeder Komponente
   - Wie kann das Teil ausfallen ?
   - Wodurch kann das Teil ausfallen ?
   - Was sind die Folgen des Ausfalls ?
   - Geht der Ausfall in die sichere oder unsichere Richtung ?
   - Wird der Ausfall erkannt?
   - Wodurch kann der Ausfall vermieden werden?

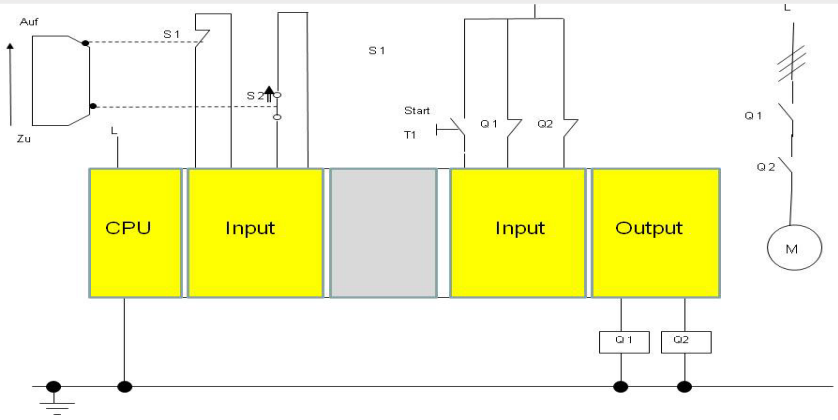
Validierung der sicherheitsbezogenen Teile der Hardware- und Softwarefunktionen



1. Beschreibung der Sicherheitsmechanismen
2. Festlegung der Fehlerreaktionen
3. Hardware FMEA
   - Theoretisch
   - Praktisch
4. Software FMEA
   - Theoretisch
   - Praktisch

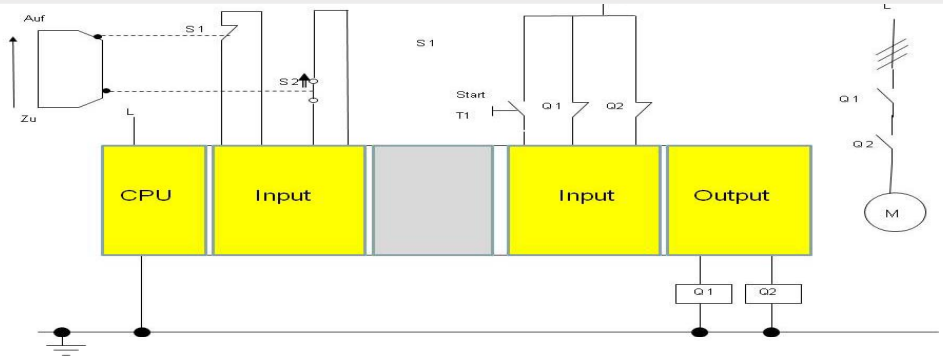
Beispiel einer FMEA





Q1,und Q2

Anzunehmender Fehler	Fehlererkennung
Schütz Q 1 oder Q 2 fällt nicht ab	Fehler wird durch SPS erkannt (Anlauftestung)
Schütz Q 1 oder Q 2 ziehen nicht an	Fehler ungefährlich, da Motor nicht anläuft, Fehler wird durch Prozess erkannt
Leitungsschluss von Q 1 oder Q 2 mit +24 V	Fehler wird durch SPS erkannt (Anlauftestung)
Schluss von Q1 nach Q2	**Fehler wird nicht erkannt,** ungefährlich solange O1 oder O2 fehlerfrei Fehlerausschluss bei getrennter Leitungsverlegung



S1und S2

Anzunehmender Fehler	Fehlererkennung
Schalter S 1öffnet nicht	Fehlerausschluss, zwangsöffnend Fehler wird über SPS erkannt, Plausibilitätsprüfung mit S2
Schalter S 2 schließt nicht	Fehler wird über SPS erkannt, Plausibilitätsprüfung mit S1
Leitungsschluss von S1 oder S2 mit 24V	Fehler wird durch SPS erkannt, geschützte und getrennte Leitungsverlegung
S1 schließt nicht oder S 2 öffnet nicht	Fehler wird durch SPS erkannt, Plausibilitätsprüfung

Sicherheitsbezogene Software	Überprüfung

Dokumentation	• auf Vollständigkeit
	• auf Vermeidung
	  • fehlerhafter Auslegungen,
	  • von Unterlassungen
	  • von Widersprüchen
	• der Maßnahmen und Methoden gegen systematische Softwareausfälle (vereinfachtes V-Modell)

Funktionelles Verhaltens und der Leistungsfähigkeit (z. B. Zeitverhalten)	• durch z.B. Black-Box-Test • durch Prüffälle, die auf Grenzwertanalysen beruhen, (z.B. für für PL d oder e)
Richtige Verwendung sicherheitsbezogener Ein-/Ausgänge	• durch I/O-Prüfungen,
Eignung der Maßnahmen zur Fehlerbeherrschung	• durch Prüffälle • durch Simulation von Fehlern • der erwarteten Reaktion

$MTTF_d$, DC_{avg} , CCF	Überprüfung
$MTTF_d$ Werte der Bauteile	• der Quelle der Daten • der Werte für: B_{10d} , n_{op} , T_{10d}
Berechnung des $MTTF_d$ Wertes jedes Kanals	• der Berechnung einschließlich der Symmetrisierung
DC-Werte von Bauteilen oder Blöcken	• auf umfassende Dokumentation (z. B. nach ISO 13849-1:2006, Anhang E). • der korrekten Durchführung (Hardware und Software) der Fehlererkennung • der angemessenen Fehlerreaktion unter typischen Umgebungsbedingungen • der Berechnung von DC_{avg}
CCF	• der richtigen Durchführung ausreichender Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ursache (z. B. nach ISO 13849-1:2006, Anhang F).

Umgebungsbedingungen	Überprüfung
Übereinstimmung mit den Umgebungsanforderungen • Mechanische Beanspruchungen durch Schock, Schwingung, das Eindringen von Verschmutzungen • elektrische Nennwerte und Energieversorgungen • klimatische Bedingungen (Temperatur und Feuchte) • elektromagnetische Verträglichkeit • (Immunität).	• durch Analyse • durch Prüfung (wenn erforderlich) • ggf. anhand der Vorgehensweisen der entsprechenden Normen

Instandhaltungsanforderungen	Überprüfung
Instandhaltungsanleitungen • Häufigkeit der Überprüfungen, • Zeitintervalle für den Austausch von verschleißbehafteten Bauteilen • Anforderungen an das Personal • Maßnahmen zur Erleichterung der Instandhaltung (z. B. Diagnosewerkzeugen zur Hilfe bei der Fehlererkennung und Reparatur)	Auf Vollständigkeit und Verständlichkeit • durch Analyse
Maßnahmen zur Vermeidung von Fehlern während der Instandhaltung	Auf z. B. Erkennung falscher Eingangsdaten durch Überprüfungen der Plausibilität
Maßnahmen gegen Veränderung	auf z. B. Passwortschutz ,um nicht berechtigte Personen am Zugang zum Programm zu hindern

Zusammenfassung

1. Wenn die notwendige Risikoreduzierung durch eine sicherheitsgerichtete Steuerung erreicht werden soll, so ist die Realisierung eines Performance Levels eine notwendige aber nicht hinreichende Maßnahme.

2. Erst die Durchführung einer Validierung erbringt den Nachweis, dass das zu erreichende Ziel auch hinreichend erreicht wird.

Danke

für Ihre Aufmerksamkeit