
ABSICHERUNG MECHATRONISCHER SYSTEME ÜBER FUNKTIONALE SICHERHEIT UND BESONDERE MERKMALE

4. Jahrestagung ISO 26262, 12.-14. September 2012, Stuttgart
Auswirkungen der Norm auf sicherheitsrelevante E/E-Systeme in Kfz



Dr.-Ing. Alexander Schloske

Senior Expert Quality Management

Leiter Stuttgarter Produktionsakademie

Telefon: +49(0)711/9 70-1890

Fax: +49(0)711/9 70-1002

E-Mail: alexander.schloske@ipa.fraunhofer.de

Internet: www.ipa.fraunhofer.de



Absicherung mechatronischer Systeme

Fragestellungen und Vortragsgliederung

Fragestellungen

- Gibt es vergleichbare Ansätze zur ISO 26262 auf der Mechanikseite?
- Wie kann ich eine integrierte Risikoanalyse für mechatronischer Systeme (elektrisch / elektronisch / mechanisch) durchführen?

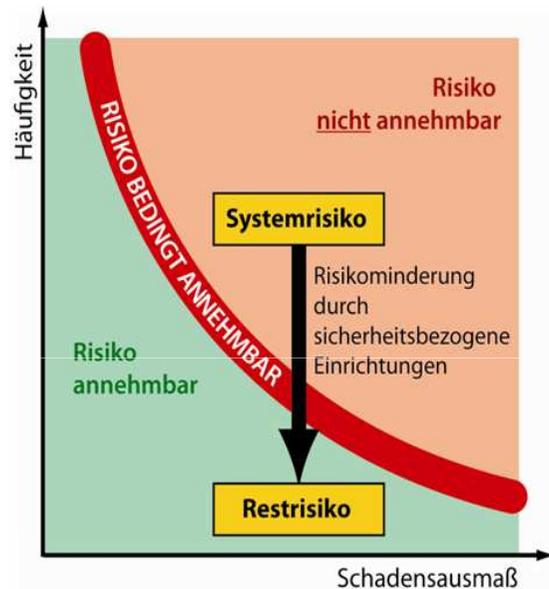
Vortragsgliederung

- Absicherung von E/E-Komponenten
- Absicherung von Mechanik-Komponenten
- Definitionen und Zielsetzungen der verschiedenen Risikoanalysen
- Denkmodell für einen integrierten Ansatz
- Abbildung im Projekt

ZIELSETZUNG FUNKTIONALE SICHERHEIT

Funktionale Sicherheit

Definition und Zielsetzung Funktionaler Sicherheit nach ISO 26262 (11/2011)



Zielsetzung:
„Risikominderung“
auf das technisch
unvermeidbare
Restrisiko

Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbar elektronischen Systems (E/E-System), beim Auftreten

- systematischer Ausfälle (z.B. fehlerhafte Systemauslegung)
- zufälliger Hardwareausfälle (z.B. Alterung von Bauteilen)

mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

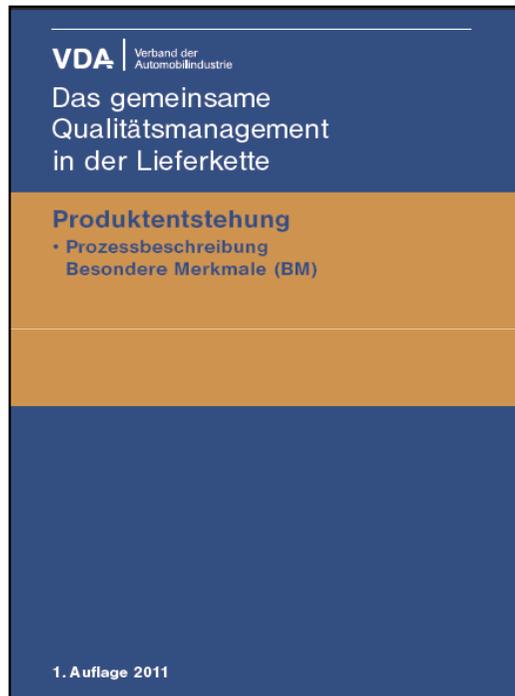
Primärer Fokus: E/E-Systeme

ZIELSETZUNG

BESONDERE MERKMALE

Besondere Merkmale

Definition und Zielsetzung Besonderer Merkmale nach VDA (05/2011)



Zielsetzung:
„Risikovermeidung“

Sicherstellung der technisch relevanter Funktionalitäten eines Produktes durch Vermeidung von Produkten mit fehlerhaften Besonderen Merkmalen:

- BM S = Sicherheitsanforderungen, Produktsicherheit und/oder sicherheitsrelevante Folgen, wie z.B. momentanem Verlust der Straßensicht, Ausfall der Bremsen, Ausfall der Lenkung, ...
- BM Z = Gesetzliche und behördliche Vorgaben zum Zeitpunkt des Inverkehrbringens
- BM F = Funktionen und Forderungen

Primärer Fokus: mechanische Systeme

Quelle VDA-QMC (05/2011)

Besondere Merkmale

Vorgehensweise zum Umgang mit Besonderen Merkmalen

- Festlegung, ob besondere Merkmale zu analysieren sind, erfolgt anhand der Bedeutung (B = 10 -> BM S, B = 9 -> BM Z, B = 8 .. 5 -> BM F)
- Falls kein robustes Design existiert, ist das Merkmal als Besonderes Merkmal zu kennzeichnen
- Falls kein robuster (fähiger und beherrschter) Prozess mit Statistischer Prozessregelung (SPC) bzw. keine Poka-Yoke-Maßnahme zur Herstellung des Merkmals existieren bzw. möglich sind, ist das Merkmal in Abhängigkeit der potenziellen Fehlerursachen zu prüfen
 - Systematische Fehler: Erst- und Letztstückprüfung sowie Stichprobenprüfung (mit Rücksortierung im Fehlerfalle)
 - Zufällige Fehler: 100%-Prüfung

SORGFALTSPFLICHT IM PRODUKT- ENTSTEHUNGSPROZESS (PEP)

Mechatronische Systeme

Sorgfaltspflicht im Produktentstehungsprozess (PEP) zur Sicherstellung technisch relevanter Funktionalitäten

- Sorgfaltspflicht im Entwicklungsprozess
 - Auslegung, Berechnung und Erprobung
 - Verifizierung und Validierung
 - Konzepte zum Umgang mit Fehlern im Betrieb (E/E und Mechanik)
 - Dokumentation und Archivierung

- Sorgfaltspflicht im Produktionsprozess
 - Produktionsplanung und Herstellung
 - Prüfplanung und Prüfung
 - Konzepte zum Umgang mit Fehlern in der Produktion
 - Dokumentation und Archivierung

In Anlehnung an VDA-QMC (05/2011)

9

RISIKOANALYSE NACH STAND DER TECHNIK (VDA 4 KAPITEL 3)

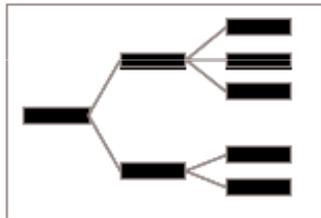
Fehlermöglichkeits- und Einflussanalyse (FMEA)

Vorgehensweise nach VDA 4 Kapitel 3 (2006)

Systemanalyse

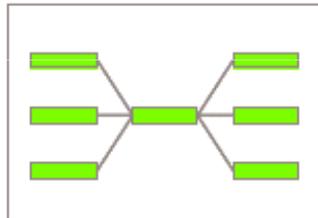
Risikoanalyse und Maßnahmen

1. Schritt Strukturanalyse



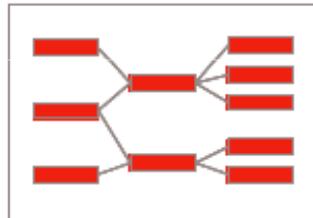
- Beteiligte Elemente erfassen u. strukturieren
- Systemstruktur erstellen

2. Schritt Funktionsanalyse



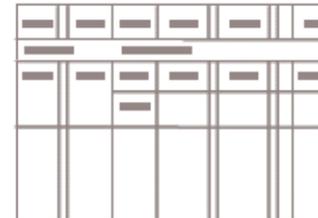
- Funktionen den Strukturelementen zuordnen
- Funktionen verknüpfen

3. Schritt Fehleranalyse



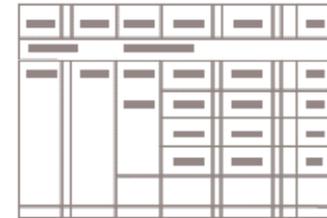
- Fehlfunktionen den Funktionen zuordnen
- Fehlfunktionen verknüpfen

4. Schritt Maßnahmenanalyse



- Aktuelle Vermeidungs-/ Entdeckungsmaßnahmen dokumentieren
- Aktuellen Stand bewerten

5. Schritt Optimierung



- Risiko mit weiteren Maßnahmen mindern
- Geänderten Stand bewerten

Quelle: VDA 4 Kapitel 3 (2006)

11

DEFINITIONEN

Definitionen

System-FMEA (für elektrische, elektronische und mechanische Komponenten)

- Zielsetzung: Überprüfung des Systemkonzepts auf systematische Fehler (Logikfehler)
- Fragestellungen bezogen auf Betrieb
 - Was kann im Betrieb passieren (und nicht warum passiert es)?
 - Wie lässt es sich im Betrieb entdecken?
 - Wie und wie sicher wird im Betrieb reagiert?
- Systemkonzept (Maßnahmen)
 - Definition von Fehlererkennung und Fehlerreaktion (Funktionales Sicherheitskonzept für E/E- und mechanische Systeme)
- Bewertung
 - Sicherheitskonzept
 - Validierung des DC-Wertes (elektrisch, elektronisch und mechanisch)

Definitionen

Konstruktions-FMEA (für elektrische, elektronische und mechanische Komponenten)

- Zielsetzung: Überprüfung der Zuverlässigkeit der Entwicklung
- Fragestellungen bezogen auf Entwicklungsprozess
 - Warum und wie wahrscheinlich kann die Komponente im Betrieb versagen (Analyse der Ausfälle in ppm bzw. FIT)?
 - Wie und wie sicher lässt sich die fehlerhaft entwickelte Komponente noch innerhalb der Entwicklung entdecken?
- Überprüfung des Entwicklungsprozesses
 - Definition von Maßnahmen zur Vermeidung und Entdeckung von fehlerhaft entwickelten Komponenten in der Entwicklung
- Bewertung
 - Zuverlässigkeit des Entwicklungsprozesses
 - Validierung des A-Wertes (elektrisch, elektronisch und mechanisch)

Definitionen

FMEDA (für elektrische und elektronische Komponenten)

- Zielsetzung: Analyse der zufälligen Abweichungen der an einer E/E-System-Sicherheitsfunktion beteiligten Komponenten
- Fragestellungen bezogen auf Betrieb
 - Welche zufälligen Abweichungen kann die Komponente über die Lebensdauer haben und wie wahrscheinlich sind diese (Vorgabe von Fehlermodi und FIT-Werten aus Katalogen, z.B. SN 29500)?
 - Wie und wie sicher lässt sich die Abweichung der Komponente im Betrieb entdecken (Fehlererkennung, Fehlerreaktion und DC-Wert aus System-FMEA)?
- Bewertung
 - Gefährliche (unvermeidbare) zufällige Abweichungen (PMHF)
 - Robustheit gegen zufällige Fehler (SPFM, LPFM)
 - Validierung der Vorgaben aus der ISO 26262

Definitionen

Prozess-FMEA (für elektrische, elektronische und mechanische Komponenten)

- Zielsetzung: Überprüfung der Zuverlässigkeit der Fertigung/Montage
- Fragestellungen bezogen auf Fertigungs-/Montageprozess
 - Warum und wie wahrscheinlich kann die Komponente beim Hersteller fehlerhaft gefertigt/montiert werden (in ppm)?
 - Wie und wie sicher lässt sich die fehlerhaft gefertigte/montierte Komponente noch innerhalb der Fertigung/Montage entdecken?
- Überprüfung des Fertigungs-/Montageprozesses
 - Definition von Maßnahmen zur Vermeidung und Entdeckung von Fehlern in der Fertigung/Montage
- Bewertung
 - Zuverlässigkeit des Fertigungs-/Montageprozesses
 - Durchschlupf fehlerhafter Einheiten über A und E

Definitionen

FIT-Werte und ppm-Werte

■ FIT-Werte

- FIT = Failure In Time (Fehler in 10^9 h)
- Zufällige Fehler eines Bauteils / Produkts in definierter Zeiteinheit
- Über Versuche und Statistik für E/E-Komponenten ermittelt und in Normen je Komponente definiert (z.B. SN 29500)
- Exponentialverteilung (für zufällige Ausfälle) über die Zeit

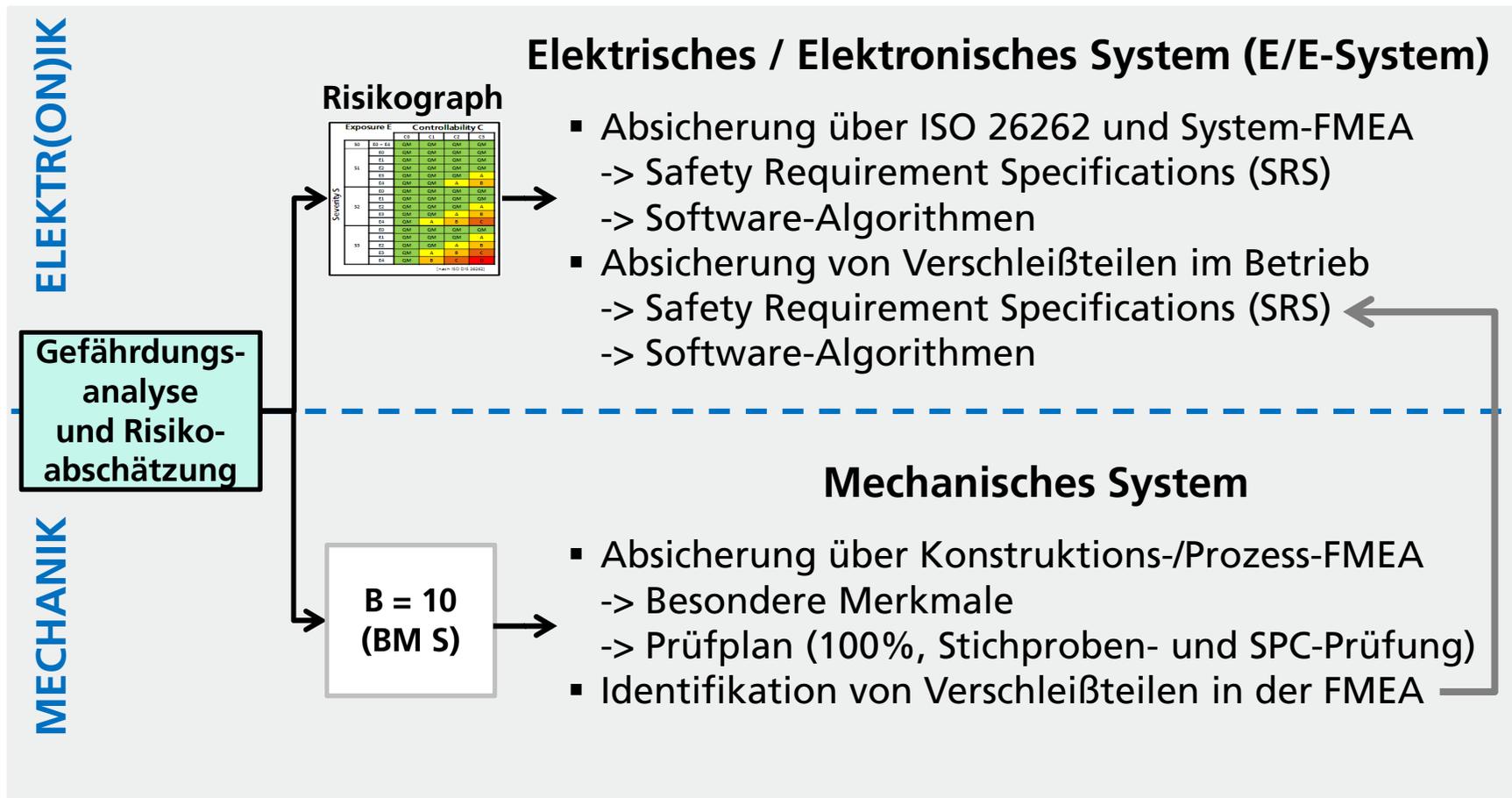
■ ppm-Werte

- ppm = (defective) parts per million
- Anzahl fehlerhafter Bauteile / Produkte
- Binomialverteilung (für n.i.O. Einheiten pro 1 Million) unabhängig von der Zeit

DENKMODELL

Denkmodell zur Analyse von Mechatronischen Systemen

Vorgehensweise zur Analyse und Absicherung funktional sicherer mechatronischer Systeme (E/E und Mechanik)



Analyse von Mechatronischen Systemen

Risikograph zur ASIL-Klassifizierung nach ISO 26262 (warum nicht auch anwendbar für Besondere Merkmale?)

Exposure E Controllability C

		C0	C1	C2	C3	
Severity S	S0	E0 – E4	QM	QM	QM	QM
	S1	E0	QM	QM	QM	QM
		E1	QM	QM	QM	QM
		E2	QM	QM	QM	QM
		E3	QM	QM	QM	A
	S2	E4	QM	QM	A	B
		E0	QM	QM	QM	QM
		E1	QM	QM	QM	QM
		E2	QM	QM	QM	A
		E3	QM	QM	A	B
	S3	E4	QM	A	B	C
		E0	QM	QM	QM	QM
		E1	QM	QM	QM	A
		E2	QM	QM	A	B
		E3	QM	A	B	C
	E4	QM	B	C	D	

[nach ISO 26262]

Schwere (Severity)

S0: keine Verletzungsgefahr

S1: geringe und mäßige Verletzungen

S2: ernste und möglicherweise tödliche Verletzungen

S3: schwere und wahrscheinlich tödliche Verletzungen

Häufigkeit des Ausgesetztseins (Exposure)

E1: selten: Situation tritt für die meisten Fahrer seltener als einmal pro Jahr auf

E2: gelegentlich: Situation tritt für die meisten Fahrer wenige Male pro Jahr auf

E3: ziemlich oft: Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf

E4: oft: Situation die bei nahezu jeder Fahrt auftritt

Beherrschbarkeit (Controllability)

C1: einfach beherrschbar:

mehr als 99% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

C2: durchschnittlich beherrschbar:

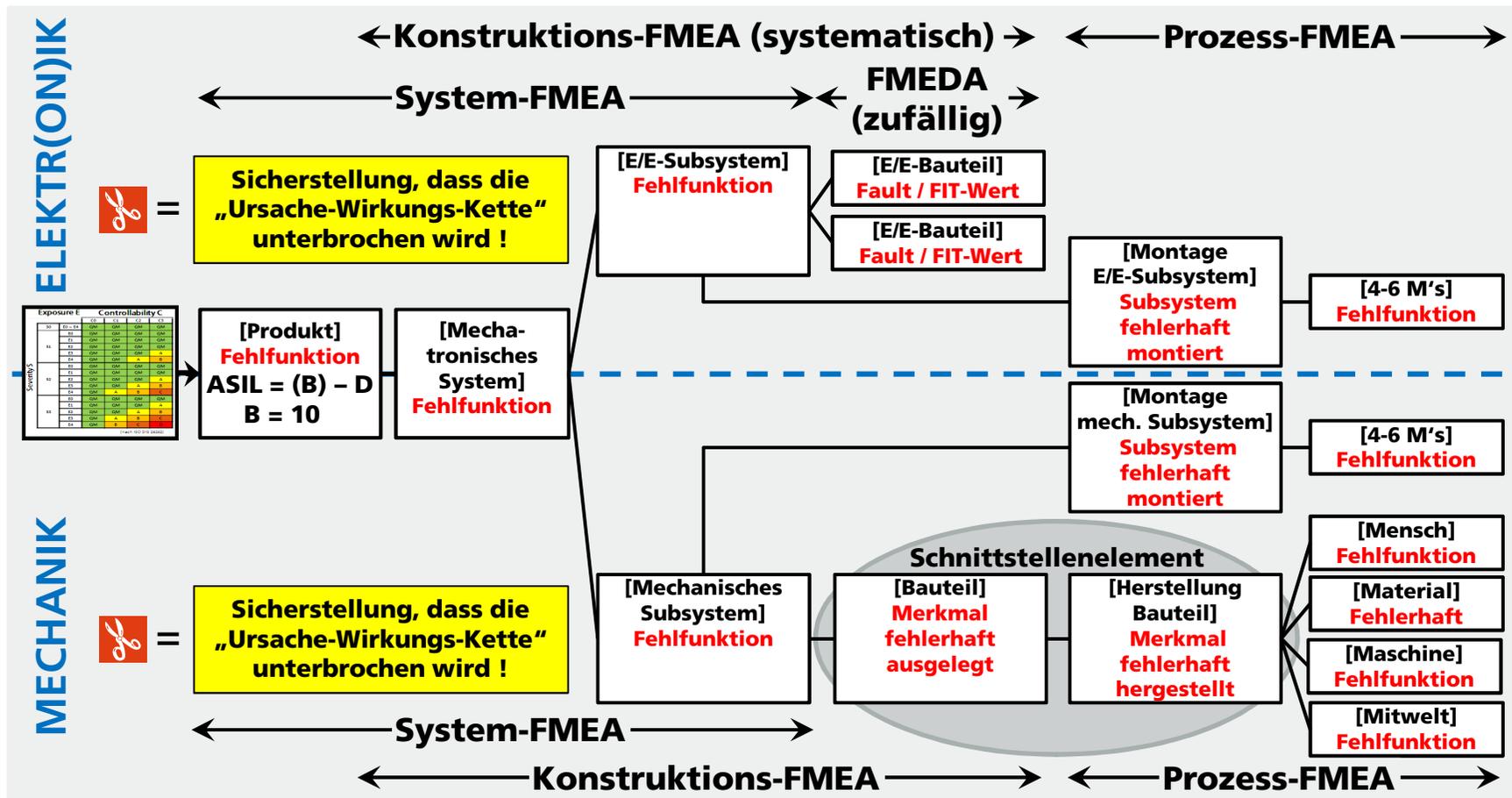
mehr als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

C3: schwierig oder gar nicht beherrschbar:

weniger als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

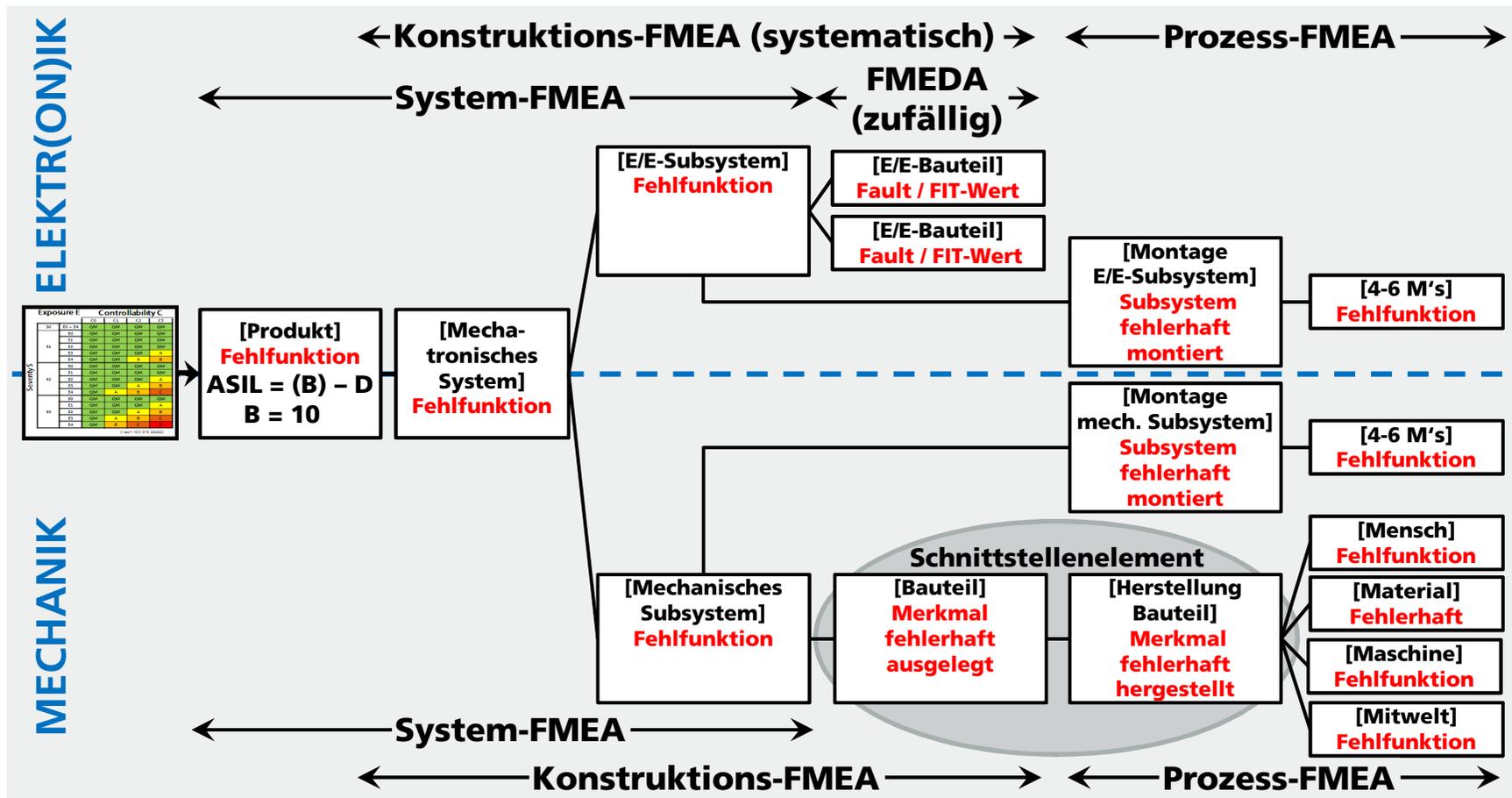
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



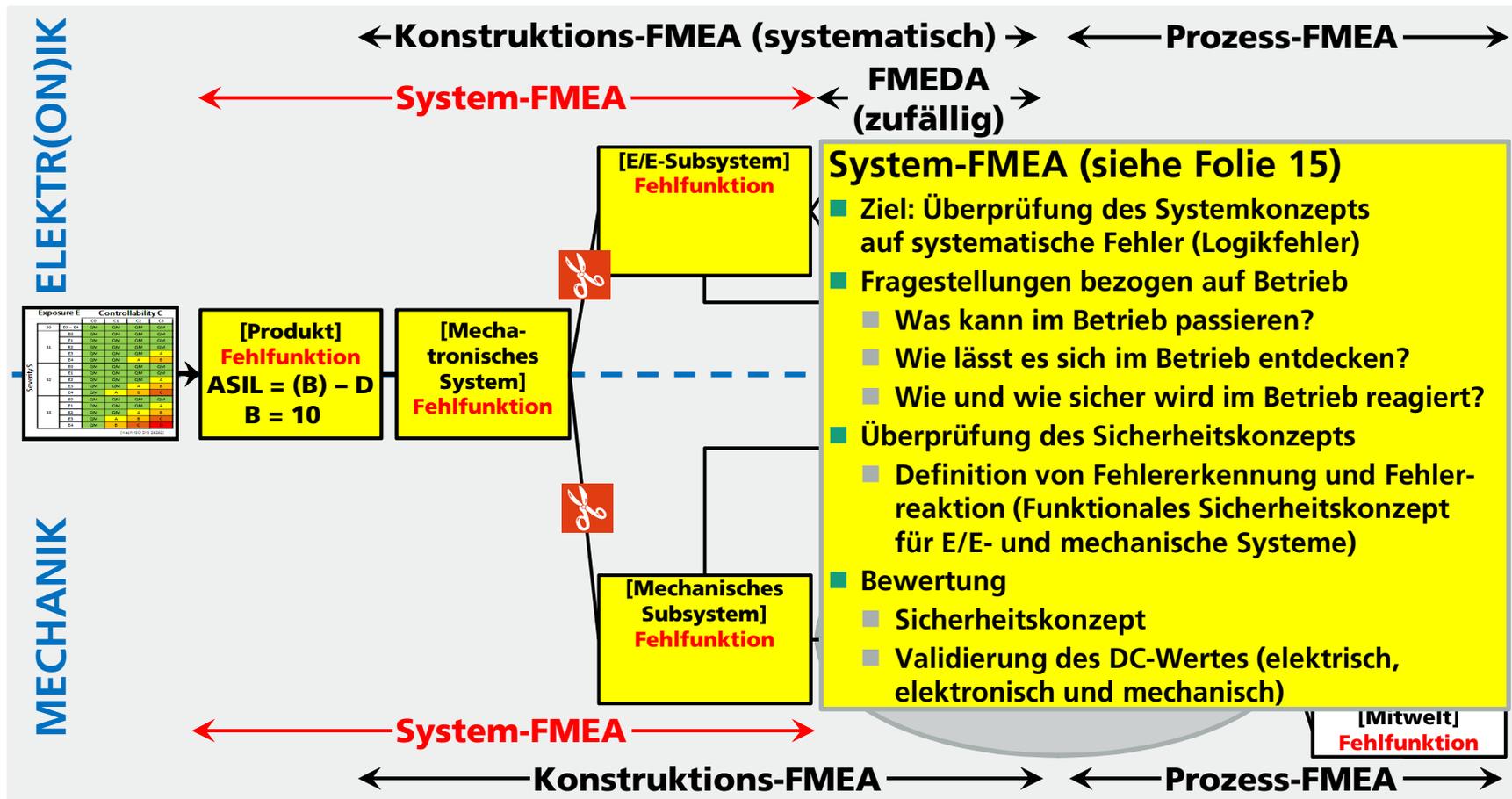
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



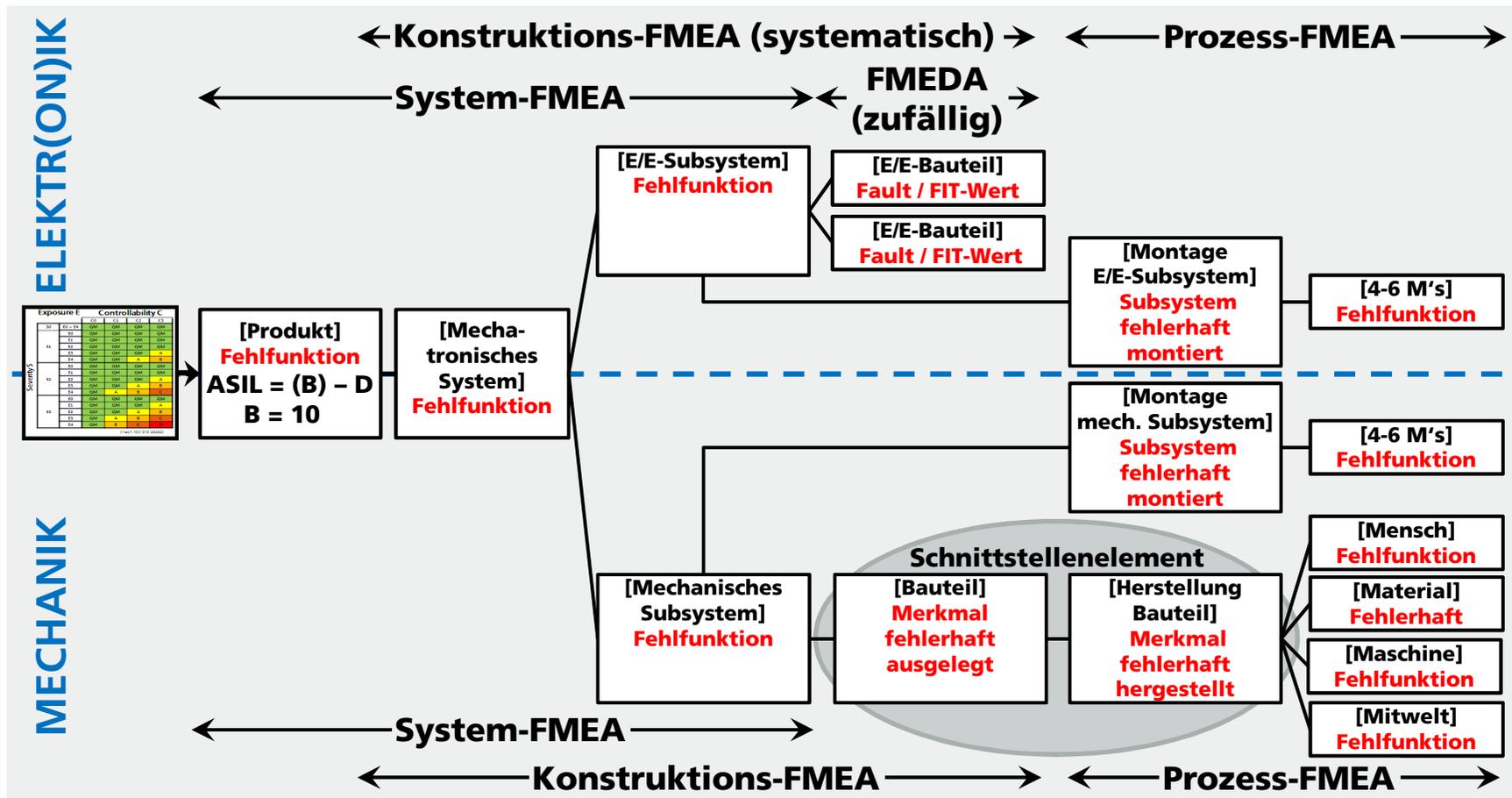
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



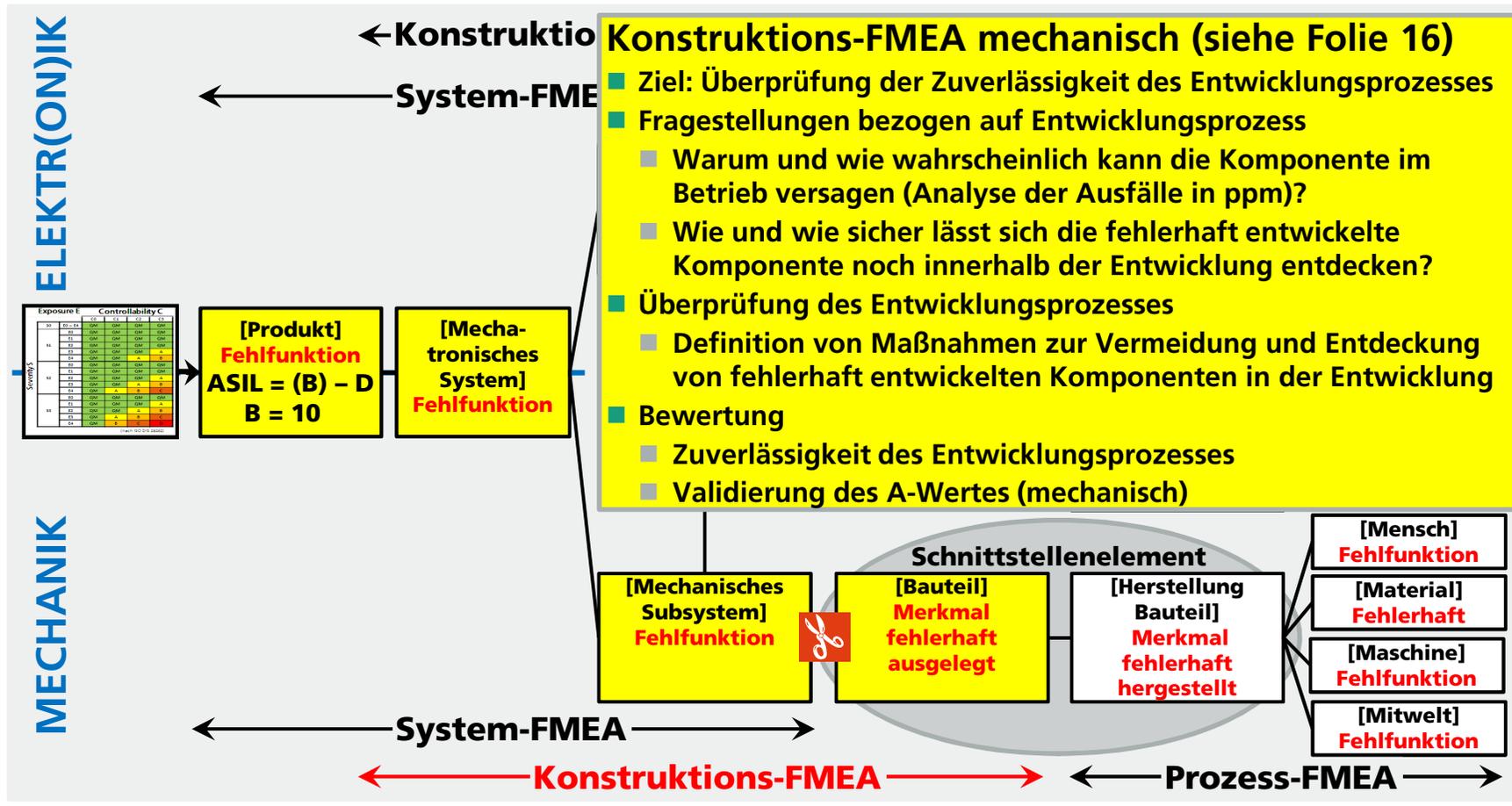
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



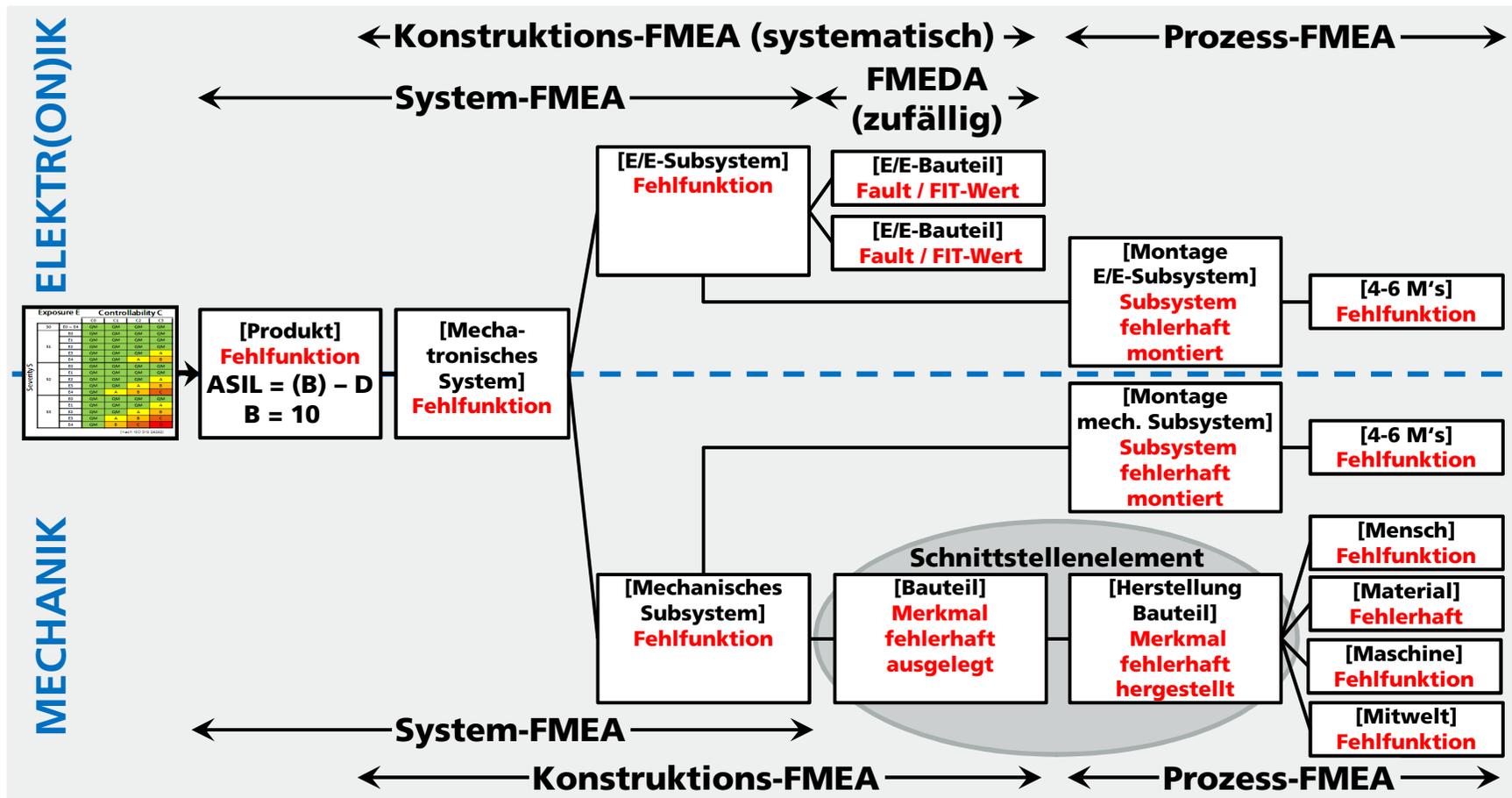
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



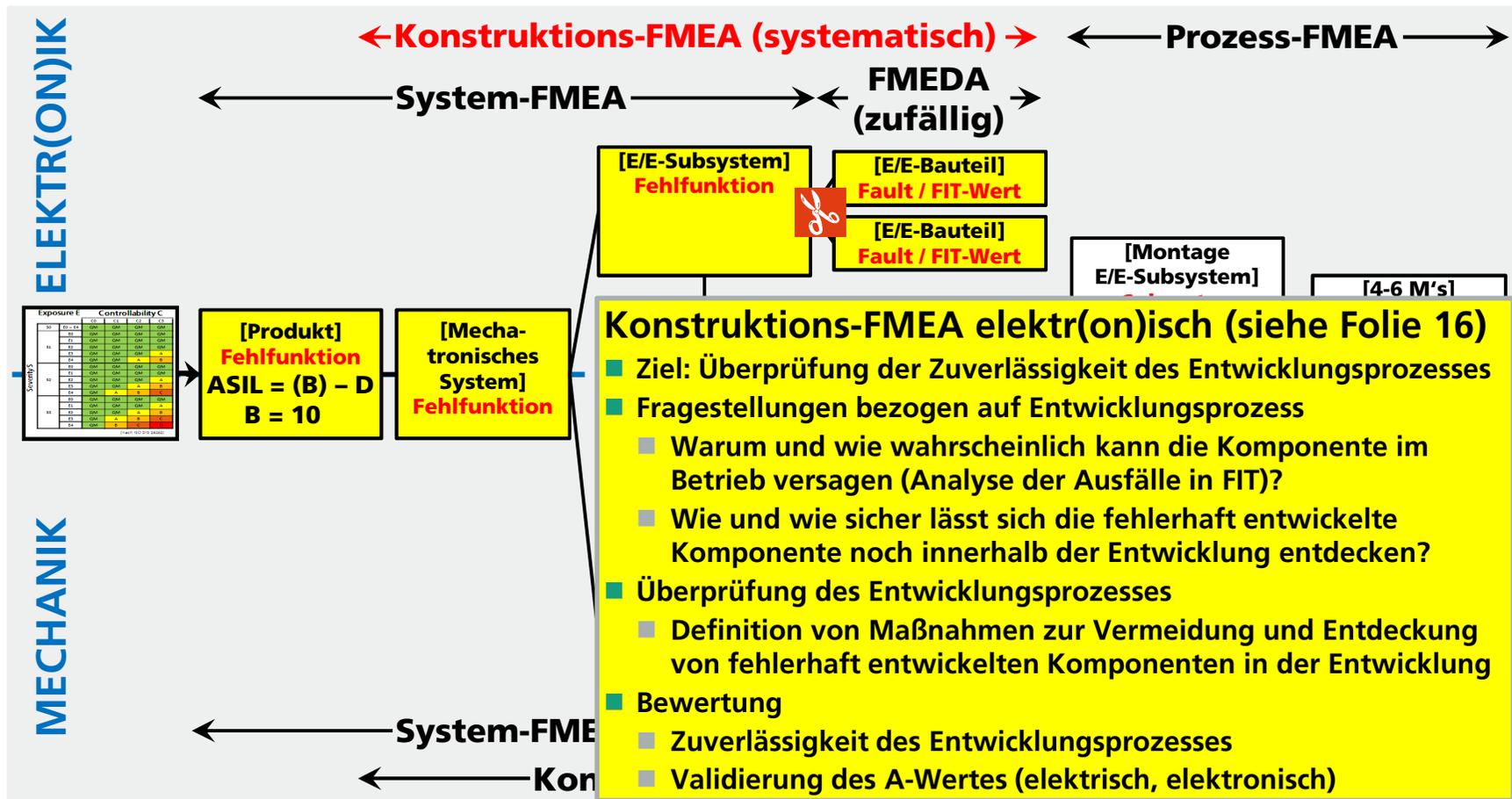
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



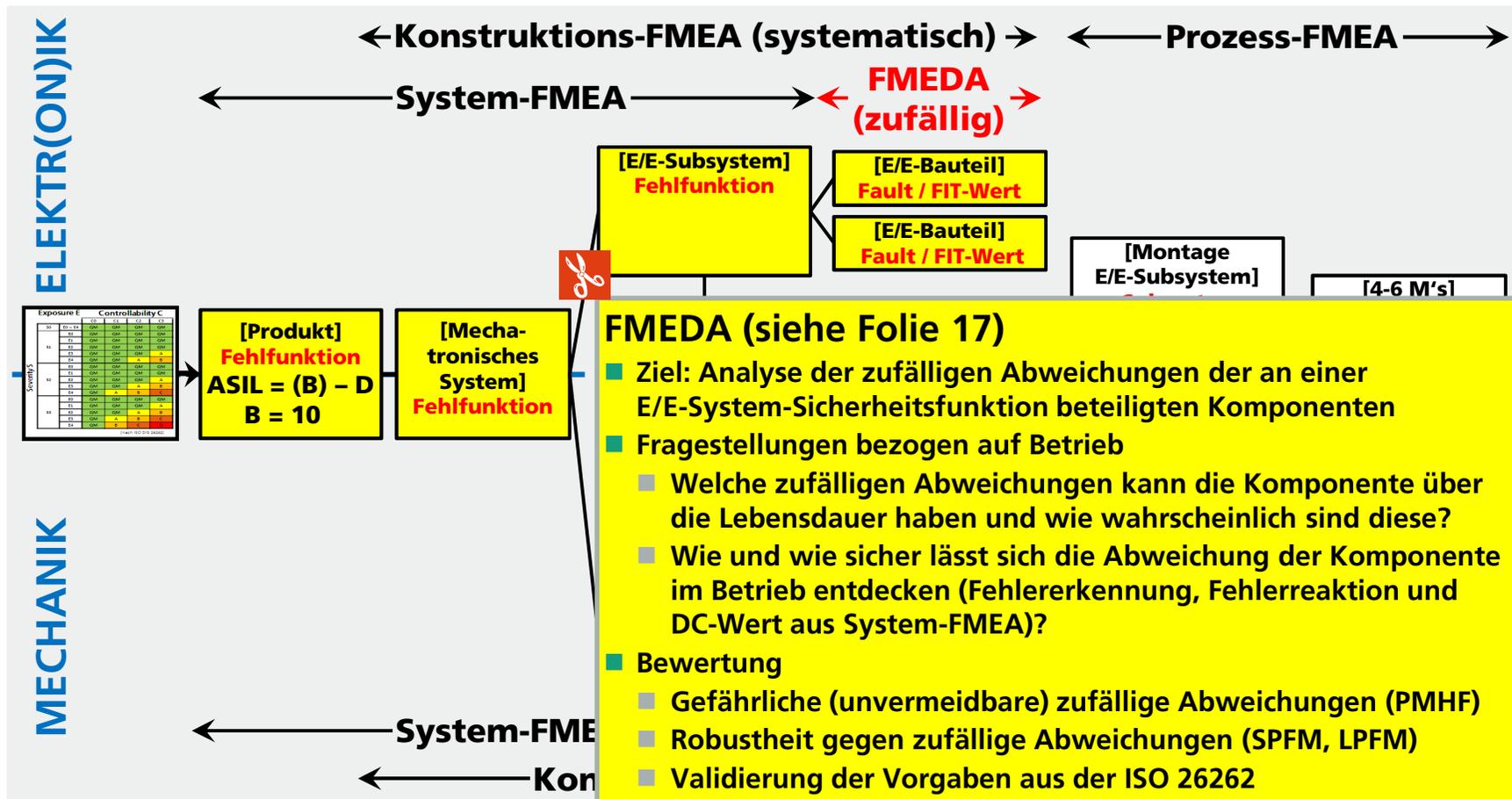
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



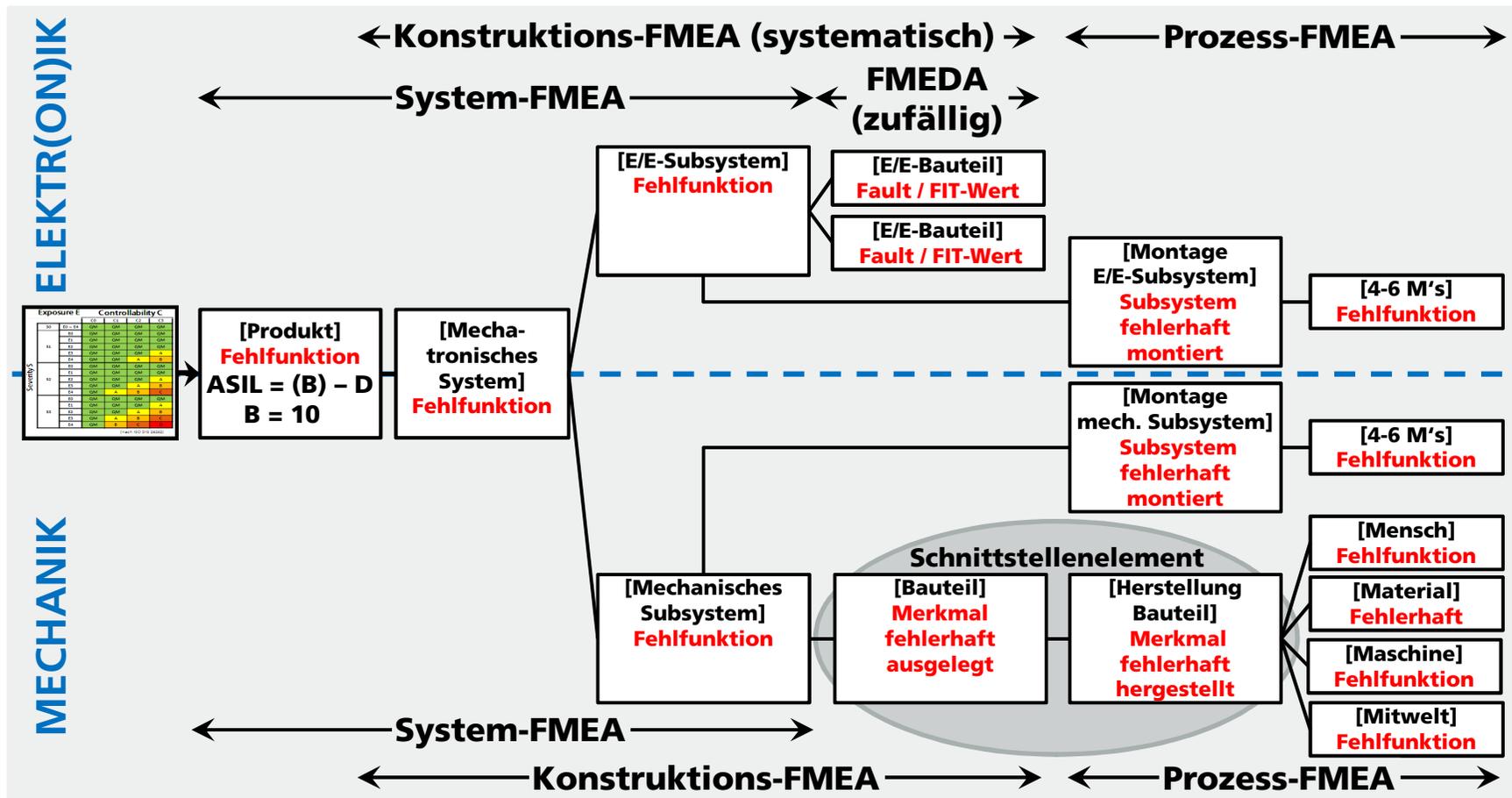
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



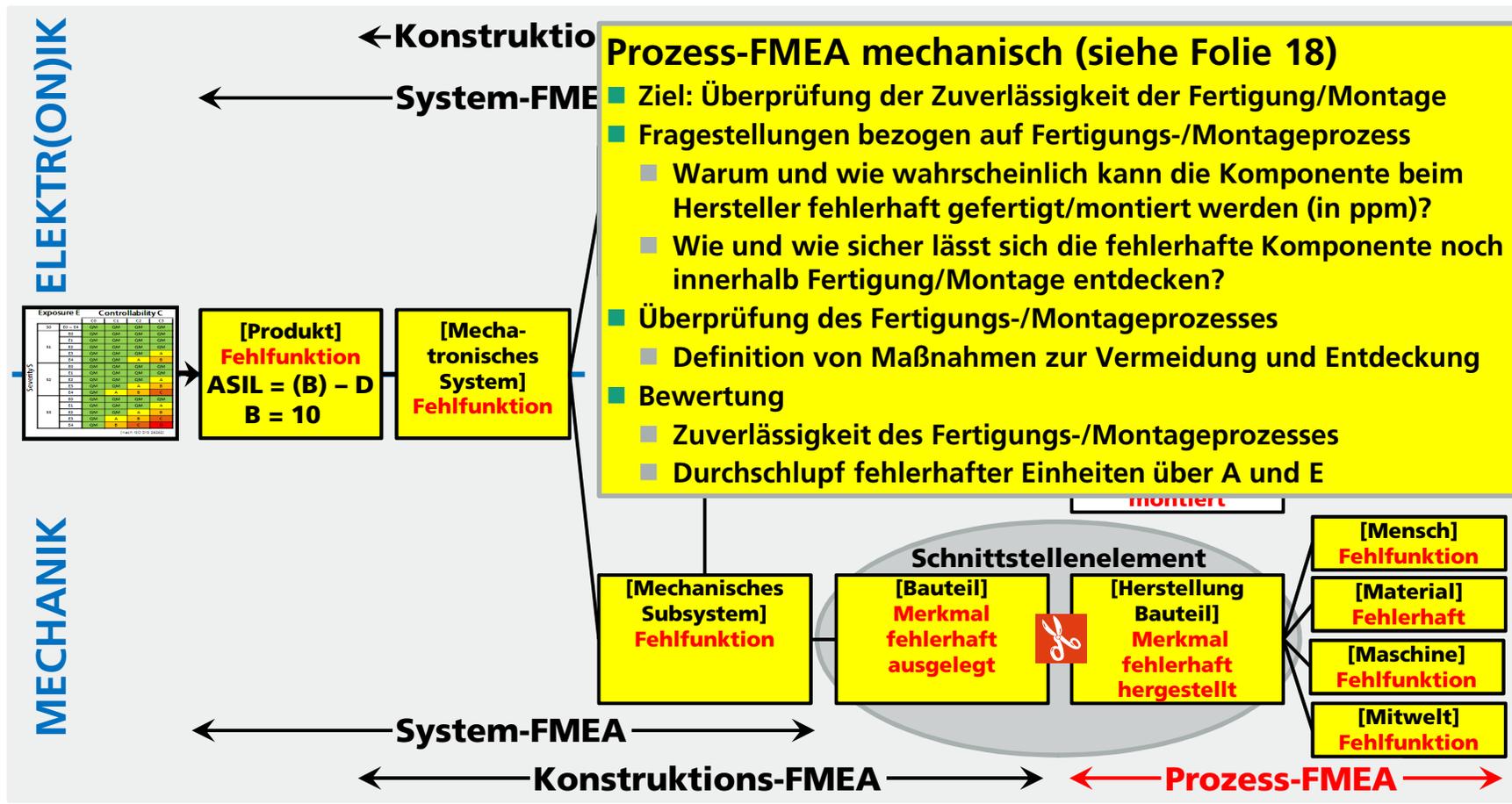
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



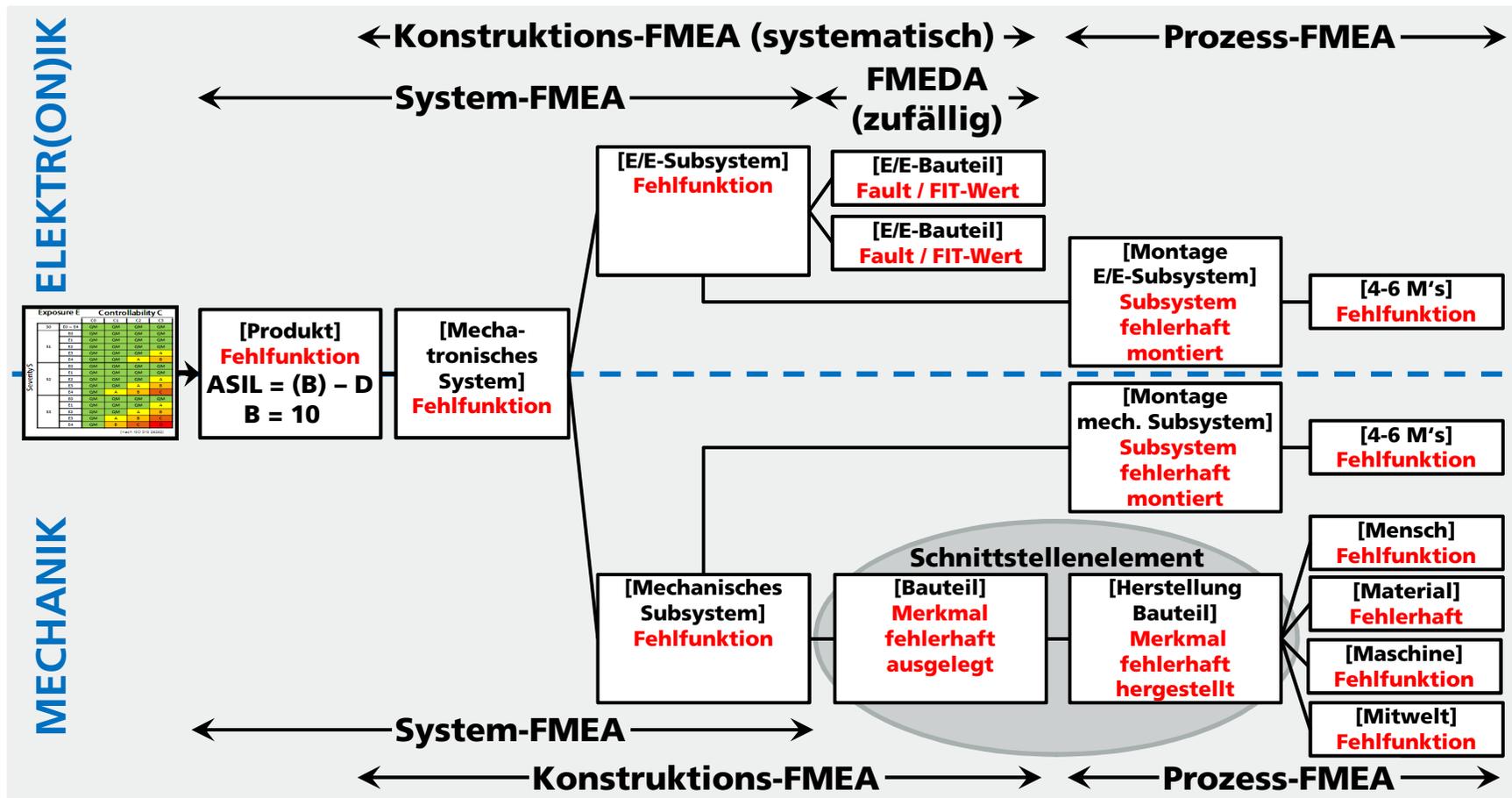
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



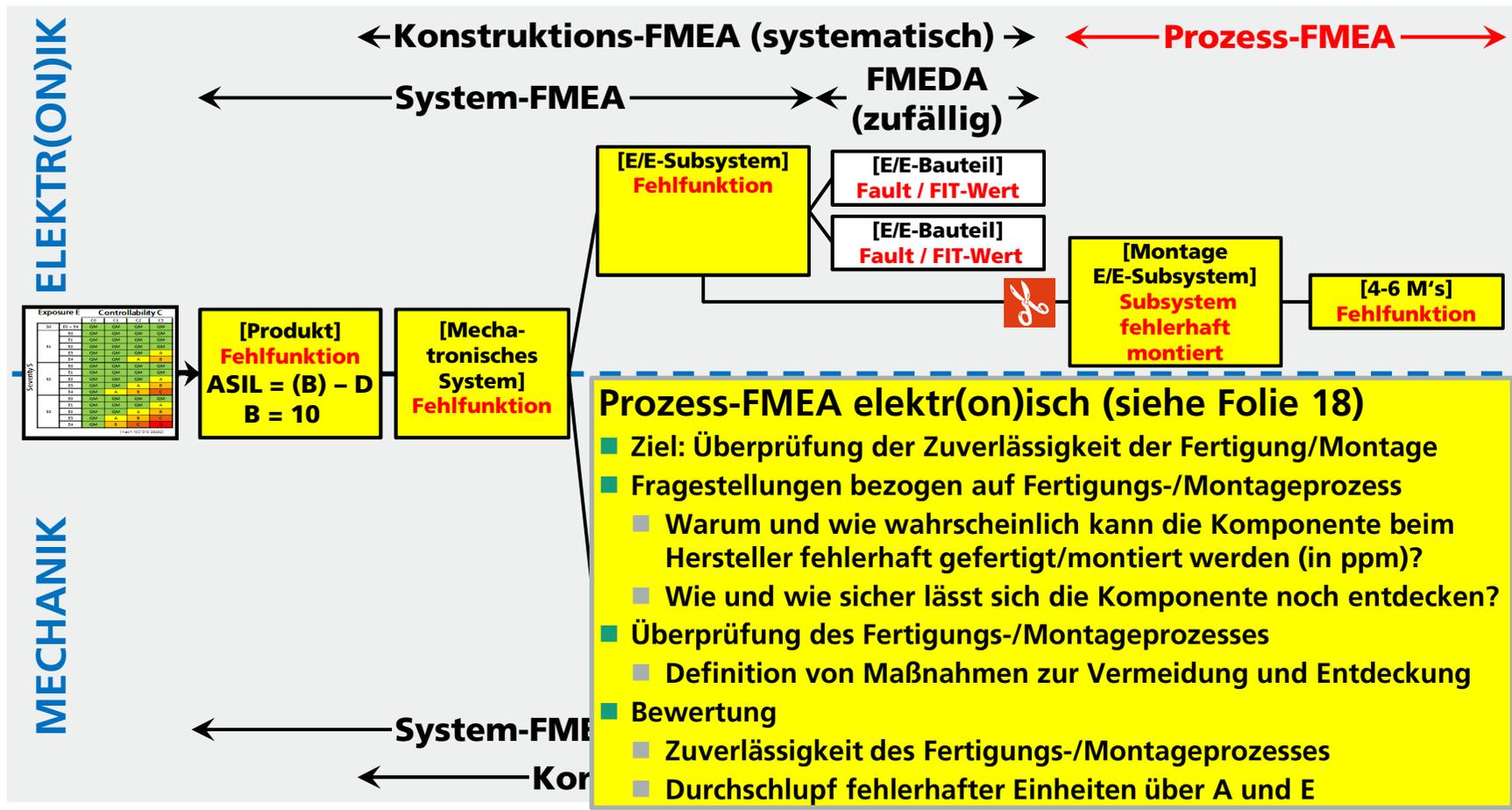
Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Denkmodell zur Analyse von Mechatronischen Systemen

Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



32

ABBILDUNG IM PROJEKT (E/E-KOMPONENTEN)

Beispiel: Einfacher Fehlerfall „Bit-Kipper im RAM“

Fehlererkennung und Fehlerreaktion (Sicherheitskonzept) im Betrieb (Beispiel nach DIN EN 61508)

Struktur-Editor: LKW [System]

- Hall-Sensoren-System
 - Software
 - Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt.
 - Bei Auftreten eines Fehlers im RAM erfolgt ein time-out.
 - RAM
 - Korrekte Datenhaltung (der sicherheitsrelevanten Daten) während der Laufzeit ermöglichen
 - (DCSPF=99,0%) (FR-Ist=1,6100 FIT) & Bit-Kipper (der sicherheitsrelevanten Daten) im RAM
 - (DCSPF=99,0%) (FR-Ist=1,6100 FIT) & Zeitdefekt (der sicherheitsrelevanten Daten) im RAM
 - (FR-Ist=1,6100 FIT) & QM: Korrekte Datenhaltung wird während der Laufzeit durchgeführt
 - EEPROM
 - Flash

Fehlernetz-Editor: LKW [System]

- LKW
 - & SIL2- (SFF-Soll=90%) (PFH-Soll=20,000 FIT)
 - 1% = 0,0161 FIT
 - 99% = 1,5939 FIT
 - Drehschalter
 - & SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt
 - Software
 - Bei Auftreten eines Fehlers im RAM erfolgt ein time-out.
 - µC
 - & Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)
 - Software
 - Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen und Zugriff erfolgt ein Vergleich.
 - RAM
 - & Bit-Kipper (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)

Reaktion im Betrieb

Erkennung im Betrieb

Erkennung / Reaktion im Betrieb (DC = High = 99%)

Beispiel: Zufällige Abweichung „Bit-Kipper im RAM“

FMEA-Formblattinhalte (Beispiel nach DIN EN 61508)

The screenshot shows the 'Formblatt-Editor VDA 96 / VDA 06: µC (LKW [System])' window. The table contains the following data:

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RP	Z	V/T
Funktion: [µC] Signale aller Hall-Sensor korrekt einlesen (Hall-Sensor) und auslesen (RAM)										
[Drehgeber] SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt	10	[µC] Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)	[RAM] (DCSPF=99,0%) (FR-Ist=1,6100 FIT) Bit-Kipper (der sicherheitsrelevanten Daten) im RAM	Maßnahmenstand - Anfang: Software-Requirement S-FMEA-V000830: Check des RAM (Test jeder Zelle mit den Bitmustern 0X55 und 0XAA) bei der Initialisierung Diagnose in der Initialisierungsphase	1		10	100		Schloske, Alexander 31.03.2011 SW-Freeze - C1-Muster abgeschlossen
>> (SIL=2) (SFF-Soll=90%) (PFH-Soll=20.000 FIT) [LKW] SIL2-Fehlfunktion				S-FMEA-V000720: Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen und Zugriff erfolgt ein Vergleich. Diagnose im Betrieb, IEC 61508-7: Verfahren A.4.5						
				S-FMEA-V000730: Zyklischer CPU-Test des XOR-Befehls vor RAM-Check. IEC 61508-7: Verfahren A.3						
				S-FMEA-V000740: Bei Auftreten eines Fehlers im RAM erfolgt ein time-out. Diagnose im Betrieb						
				Maßnahmenstand: Software Test						
				S-FMEA-E000290: Test des CPU-Tests für den XOR-Befehl.	1		1	10		Maier, Christoph 22.04.2011 Modultest - C1 abgeschlossen
				S-FMEA-E000050: Modultest der RAM-Check-Routine sowie der Sicherstellung der Einnahme des sicheren Zustandes (time-out).						

Annotations and Labels:

- Komp./ Funktion Software-Requirements**: Points to the function description.
- Requirement ID**: Points to the ID 'S-FMEA-V000830'.
- Verfahren**: Points to the procedure 'IEC 61508-7: Verfahren A.4.5'.
- Maßnahmen zum Test der Software**: Points to the test status 'Maßnahmenstand: Software Test'.
- Test-ID**: Points to the test ID 'S-FMEA-E000050'.
- Verifizierung im Rahmen der Entwicklung**: A central label with arrows pointing to the development phase measures.
- Erkennung / Reaktion Beherrschung im Betrieb (DC = High = 99%)**: A label with arrows pointing to the operational phase measures.
- SFF-Soll** and **PFH-Soll**: Labels pointing to the failure rate columns.
- DC-Ist** and **FIT-Ist**: Labels pointing to the current failure rate column.

System-FMEA

Vorgehensweise zur Analyse und Absicherung von E/E-Systemen gemäß Funktionaler Sicherheit

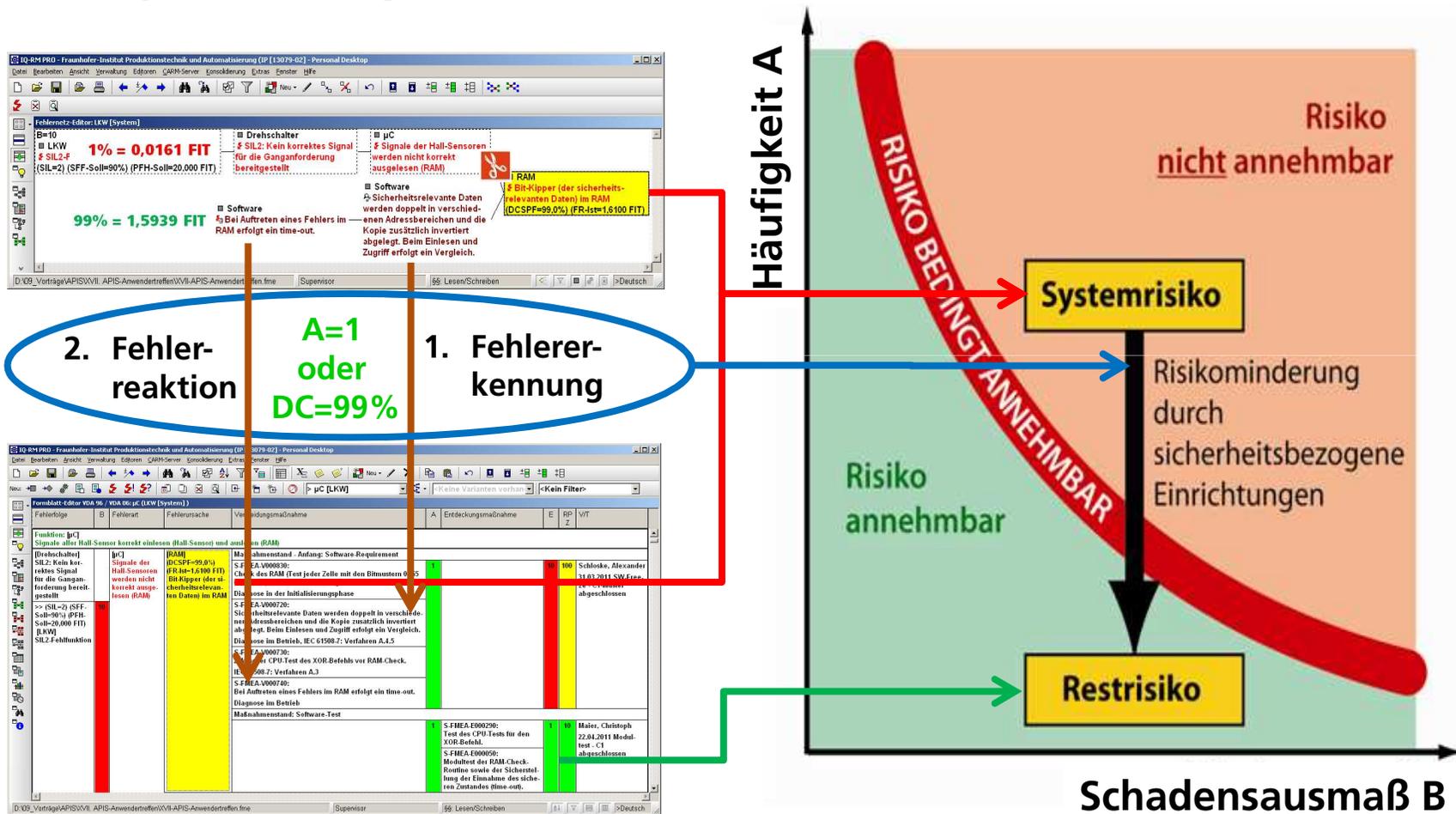


ABBILDUNG IM PROJEKT (MECHANIK-KOMPONENTEN)

Beispiel: Besondere Merkmale „Anker-Durchmesser“

Durchgängige Betrachtung Besonderer Merkmale durch Verknüpfung von Fehlernetzen über die FMEA-Arten

The screenshot displays the IQ-RM PRO software interface for FMEA analysis. The main window is titled 'Struktur-Editor: P-FMEA [Prozess]' and shows a hierarchical process tree for 'Herstellung Magnetgestell'. The 'Anker drehen' process is expanded, showing sub-processes like 'Außen-Durchmesser herstellen', 'Oberflächengüte herstellen', etc. A list of failure modes is shown on the right, including 'Anker mit zu großem Außen-Durchmesser hergestellt' and 'Anker mit zu kleinem Außen-Durchmesser hergestellt'. Below this, the 'Fehlernetz-Editor: K-FMEA [Konstruktion]' window shows a failure network diagram with callouts for 'K-FMEA' and 'P-FMEA' elements. The callouts highlight specific failure modes and their relationships, such as 'Außen-Durchmesser zu groß' and 'Anker drehen'.

FAZIT

Absicherung mechatronischer Systeme über Funktionale Sicherheit und Besondere Merkmale

Fazit

- Ziel der Funktionalen Sicherheit und der Besonderen Merkmale ist die Sicherstellung technisch relevanter Sicherheitsfunktionen
 - Funktionale Sicherheit untersucht E/E-Systeme
 - Besondere Merkmale untersucht mechanische Systeme
- Es lassen sich sowohl die Anforderungen der Funktionalen Sicherheit als auch die Anforderungen der Besonderen Merkmale in einer integrierten Risikoanalyse (FMEA-Datei) analysieren und absichern
- Der gemeinsame Nenner der Analyse ist die Gefährdungs- und Risikoabschätzung mit dem Risikograph sowie das Fehlernetz
- Die Fragestellungen, Maßnahmen und Bewertungsmaßstäbe sind entsprechend dem Fokus der Betrachtung über die FME(D)A-Arten zu wählen
- **Funktionale Sicherheit und Besondere Merkmale ergänzen sich auf dem Weg zum funktional sicheren System!**