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

TÜV Functional Safety Engineer
Safety Instrumented Systems
ID: 1427/08
FS Engineer
TÜV Rheinland Group

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

© Fraunhofer

Fraunhofer IPA

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

© Fraunhofer

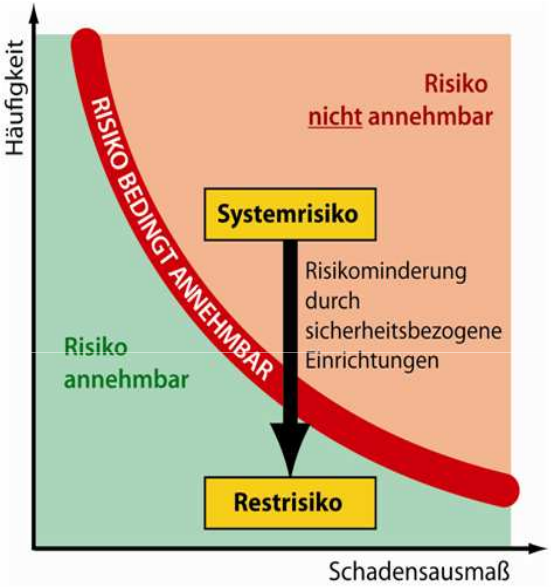
ZIELSETZUNG
FUNKTIONALE SICHERHEIT

© Fraunhofer

Fraunhofer IPA

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

© Fraunhofer

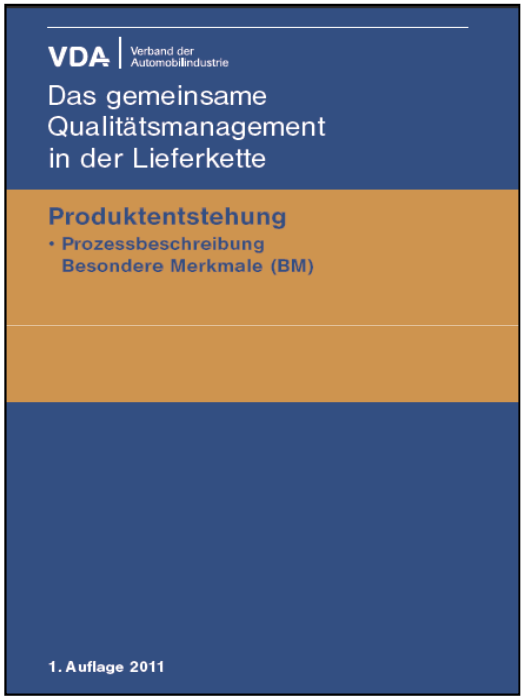
ZIELSETZUNG
BESONDERE MERKMALE

© Fraunhofer

Fraunhofer IPA

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)

© Fraunhofer

Fraunhofer IPA

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

© Fraunhofer

SORGFALTSPFLICHT IM PRODUKT-ENTSTEHUNGSPROZESS (PEP)

© Fraunhofer

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)

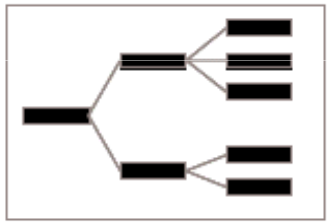
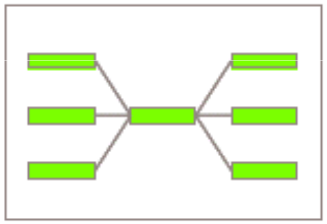
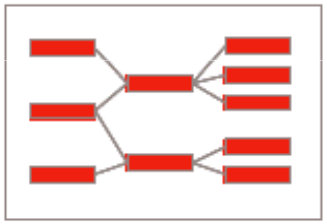
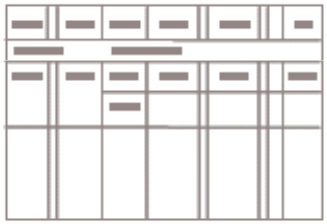
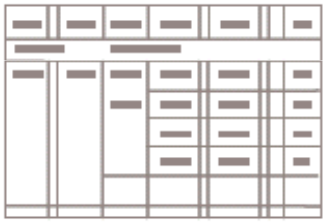
© Fraunhofer

RISIKOANALYSE NACH STAND DER TECHNIK (VDA 4 KAPITEL 3)

© Fraunhofer

Fehlermöglichkeits- und Einflussanalyse (FMEA)
Vorgehensweise nach VDA 4 Kapitel 3 (2006)

Systemanalyse | **Risikoanalyse und Maßnahmen**

1. Schritt	2. Schritt	3. Schritt	4. Schritt	5. Schritt
Strukturanalyse	**Funktionsanalyse**	**Fehleranalyse**	**Maßnahmenanalyse**	**Optimierung**
				
• Beteiligte Elemente erfassen u. strukturieren • Systemstruktur erstellen	• Funktionen den Strukturelementen zuordnen • Funktionen verknüpfen	• Fehlfunktionen den Funktionen zuordnen • Fehlfunktionen verknüpfen	• Aktuelle Vermeidungs-/ Entdeckungs-maßnahmen dokumentieren • Aktuellen Stand bewerten	• Risiko mit weiteren Maßnahmen mindern • Geänderten Stand bewerten

Quelle: VDA 4 Kapitel 3 (2006)

© Fraunhofer

Fraunhofer IPA

DEFINITIONEN

© Fraunhofer

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)

© Fraunhofer

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)

© Fraunhofer

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

© Fraunhofer

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

© Fraunhofer

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)
  - Eponentialverteilung (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

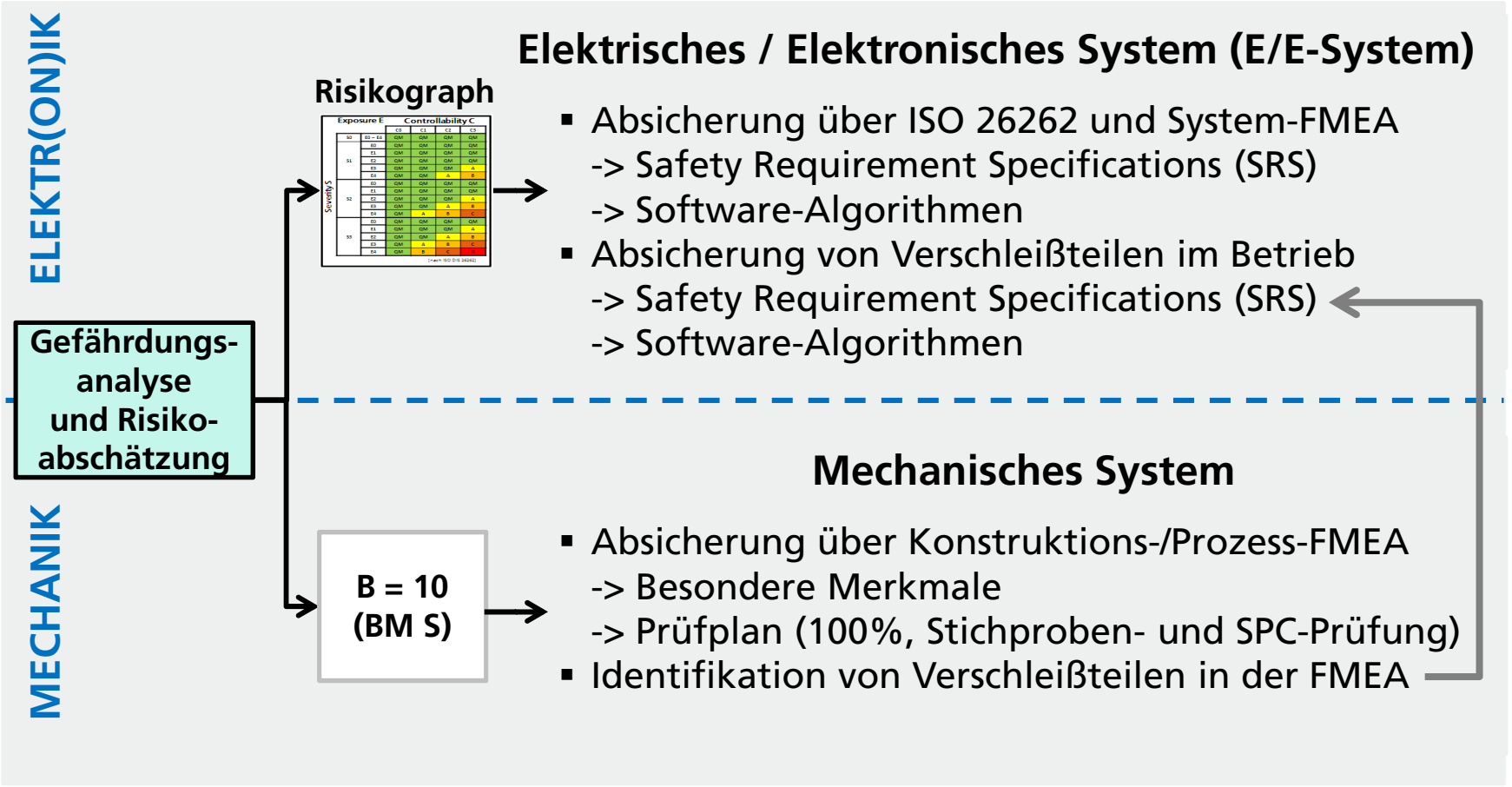
© Fraunhofer

DENKMODELL

© Fraunhofer

Denkmodell zur Analyse von Mechatronischen Systemen

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



© Fraunhofer

Fraunhofer IPA

Analyse von Mechatronischen Systemen

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

Exposure E Controllability C

Severity S	E	C0	C1	C2	C3
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
	E4	QM	QM	A	B
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	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

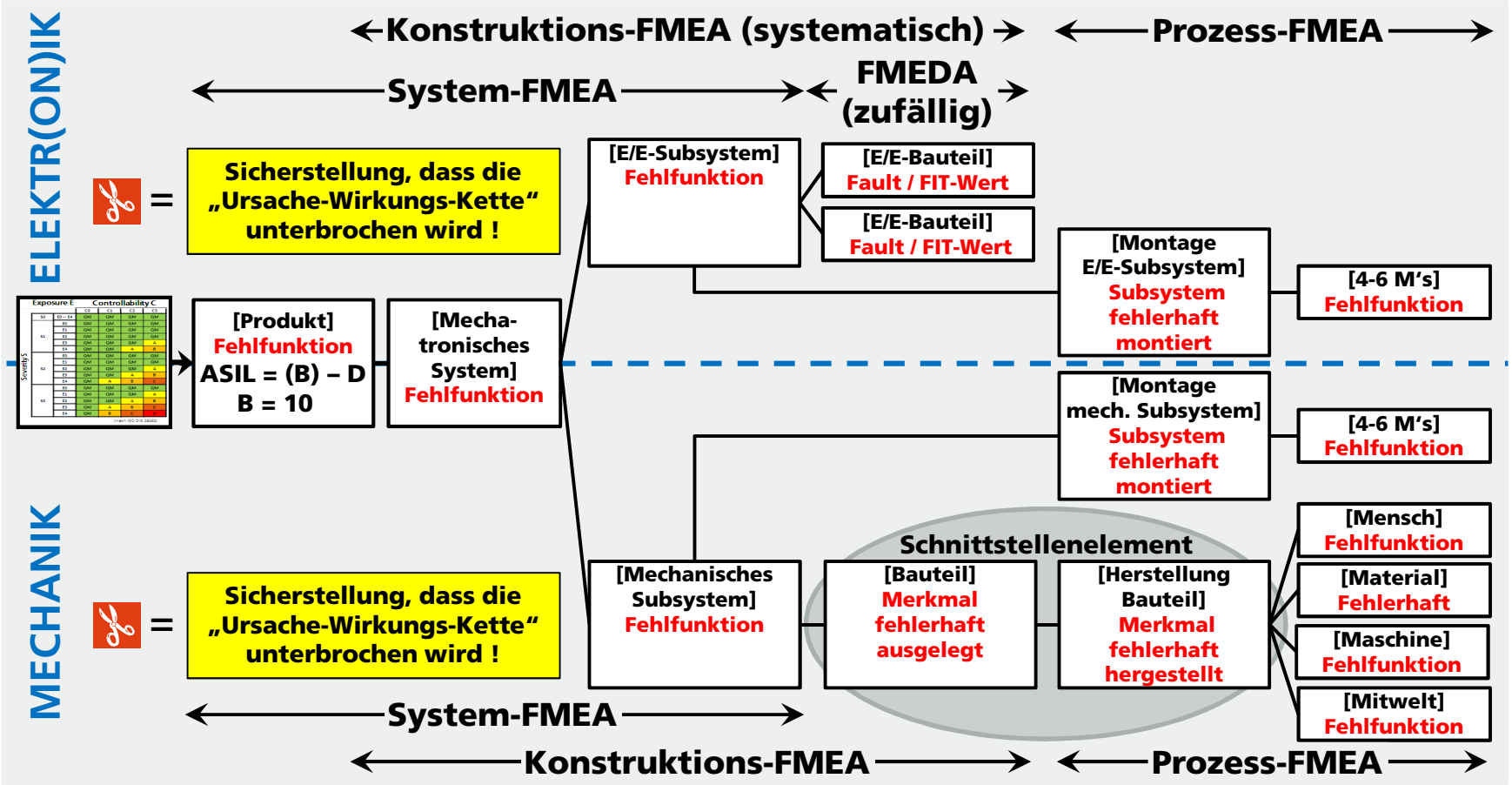
Beherrschbarkeit (Controllability)

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

© Fraunhofer

Denkmodell zur Analyse von Mechatronischen Systemen

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

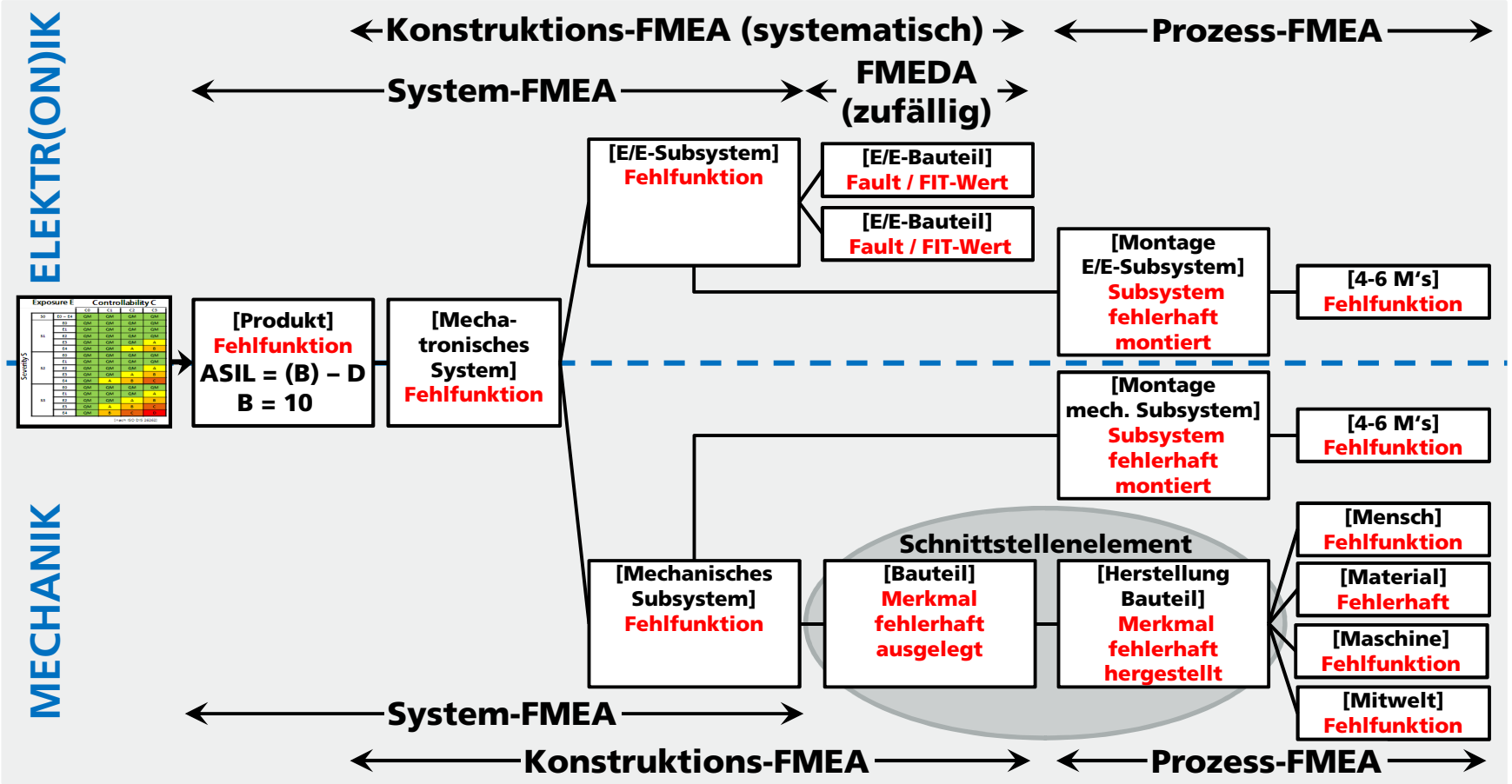


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

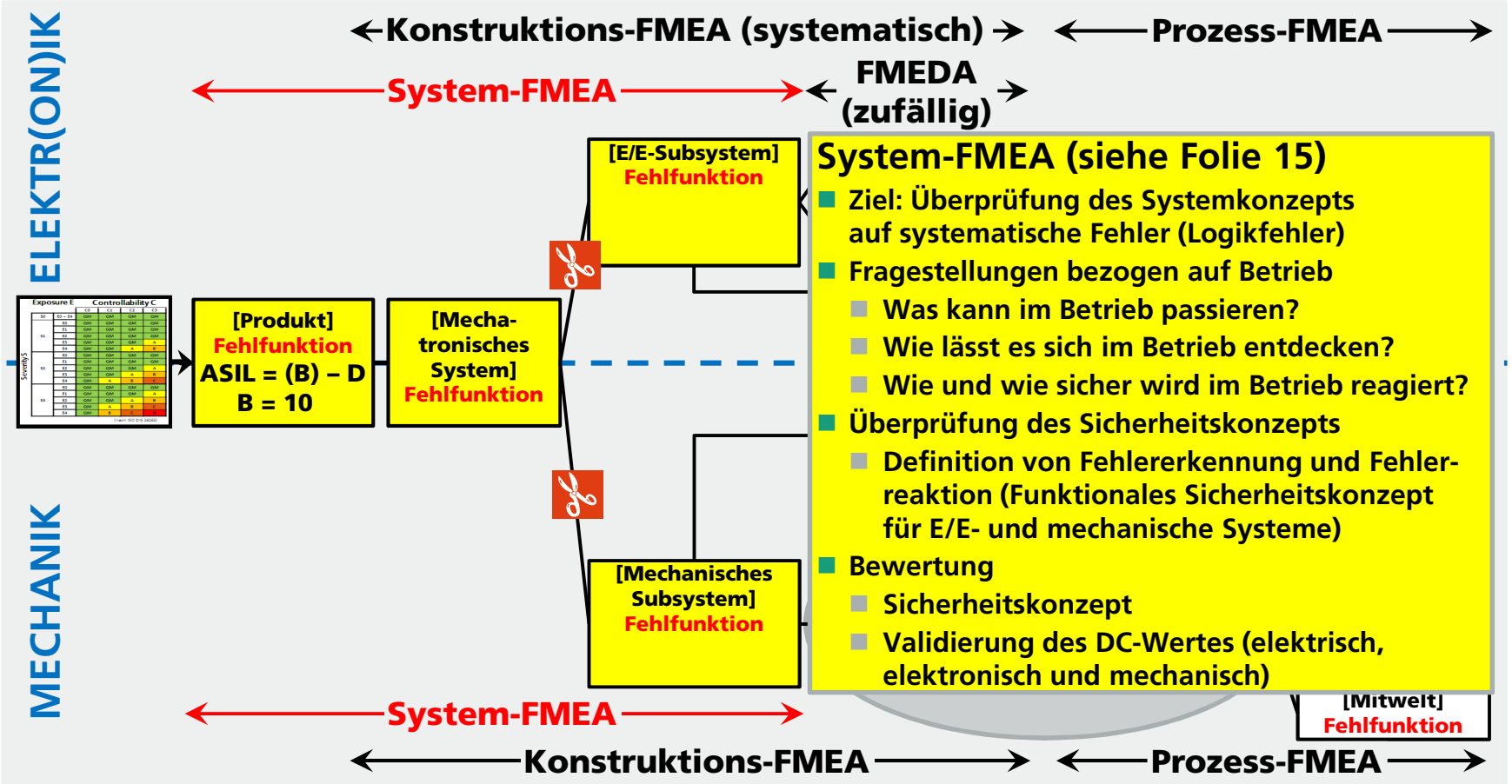


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

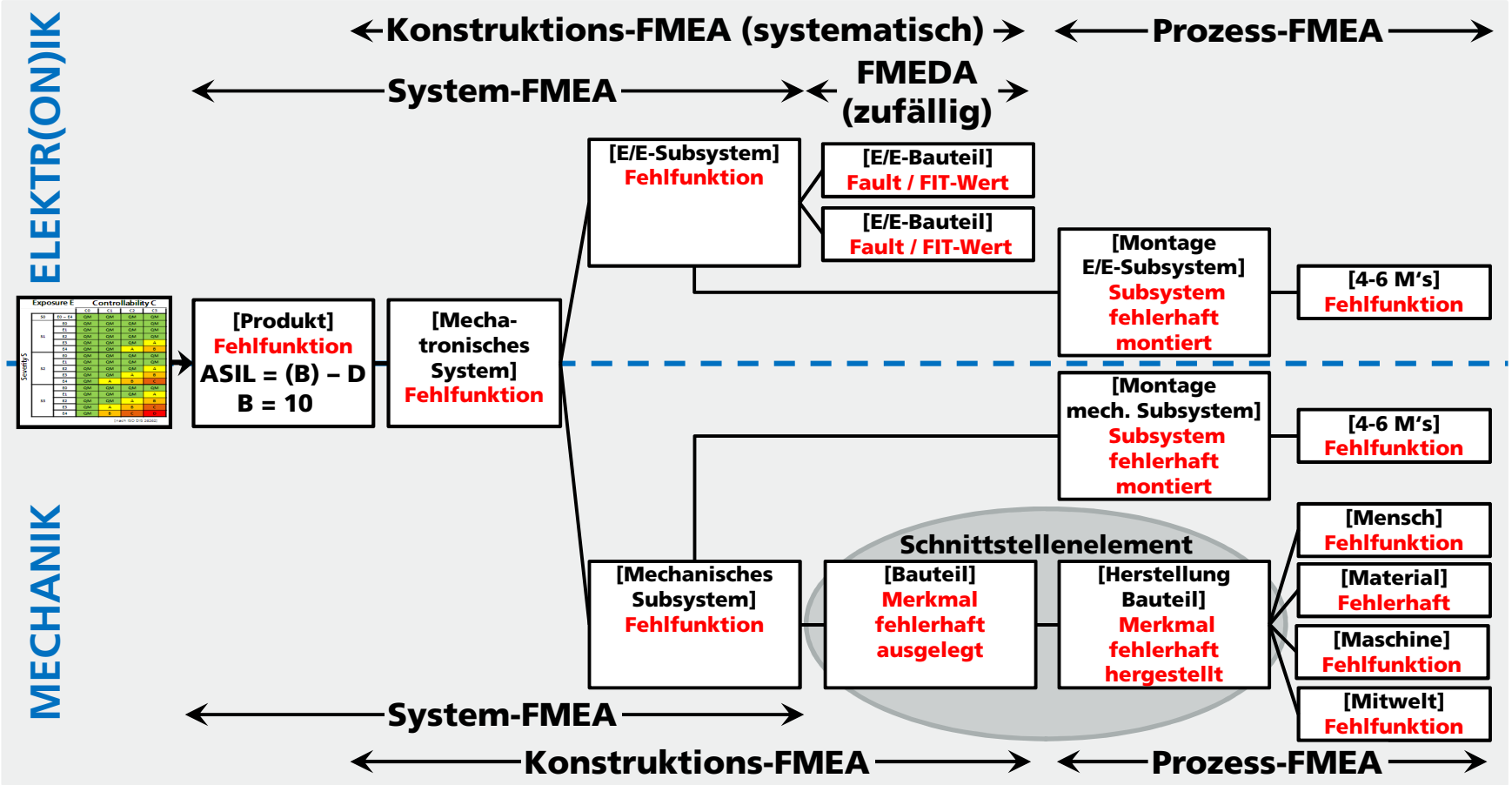


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

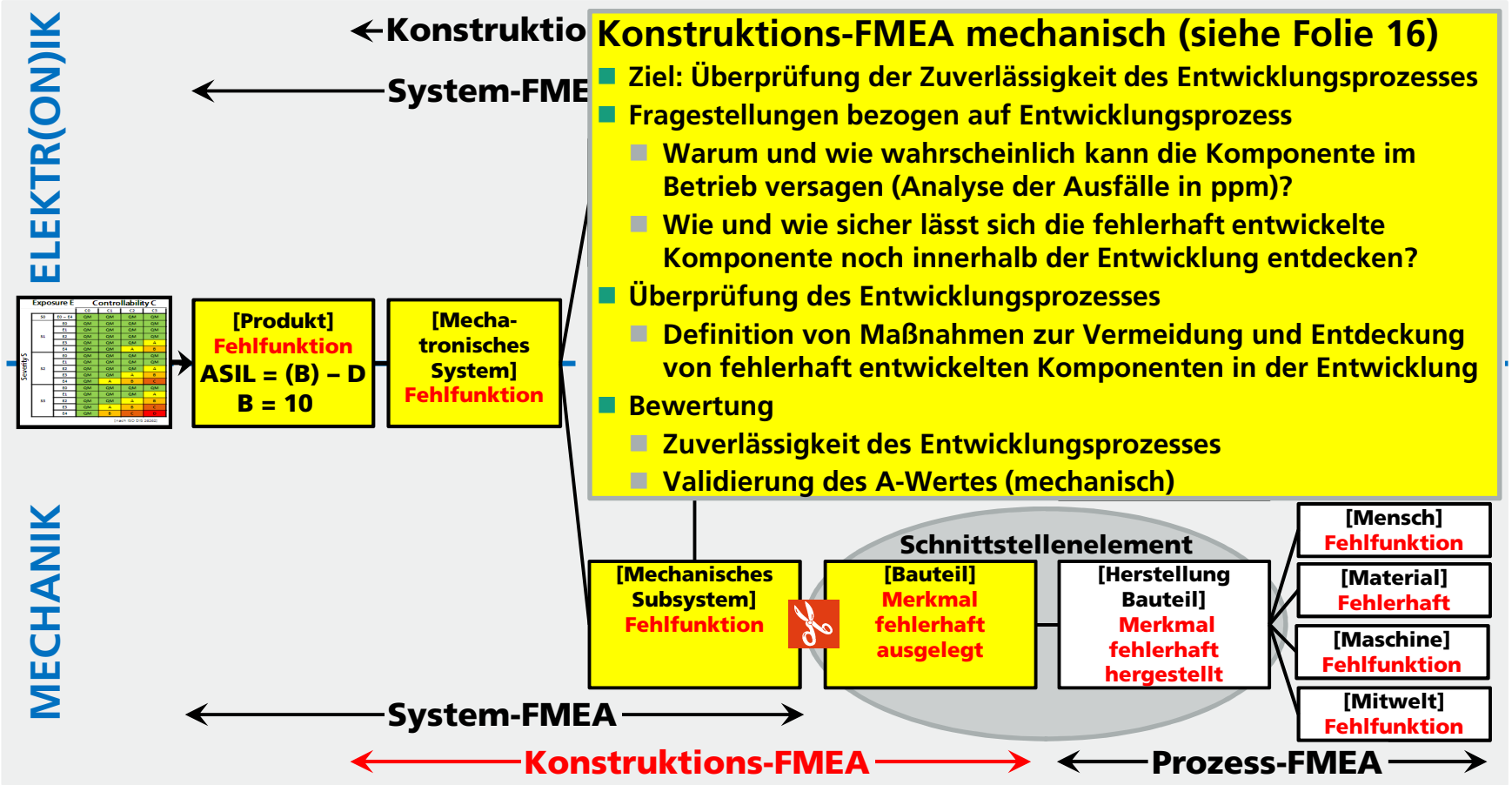


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

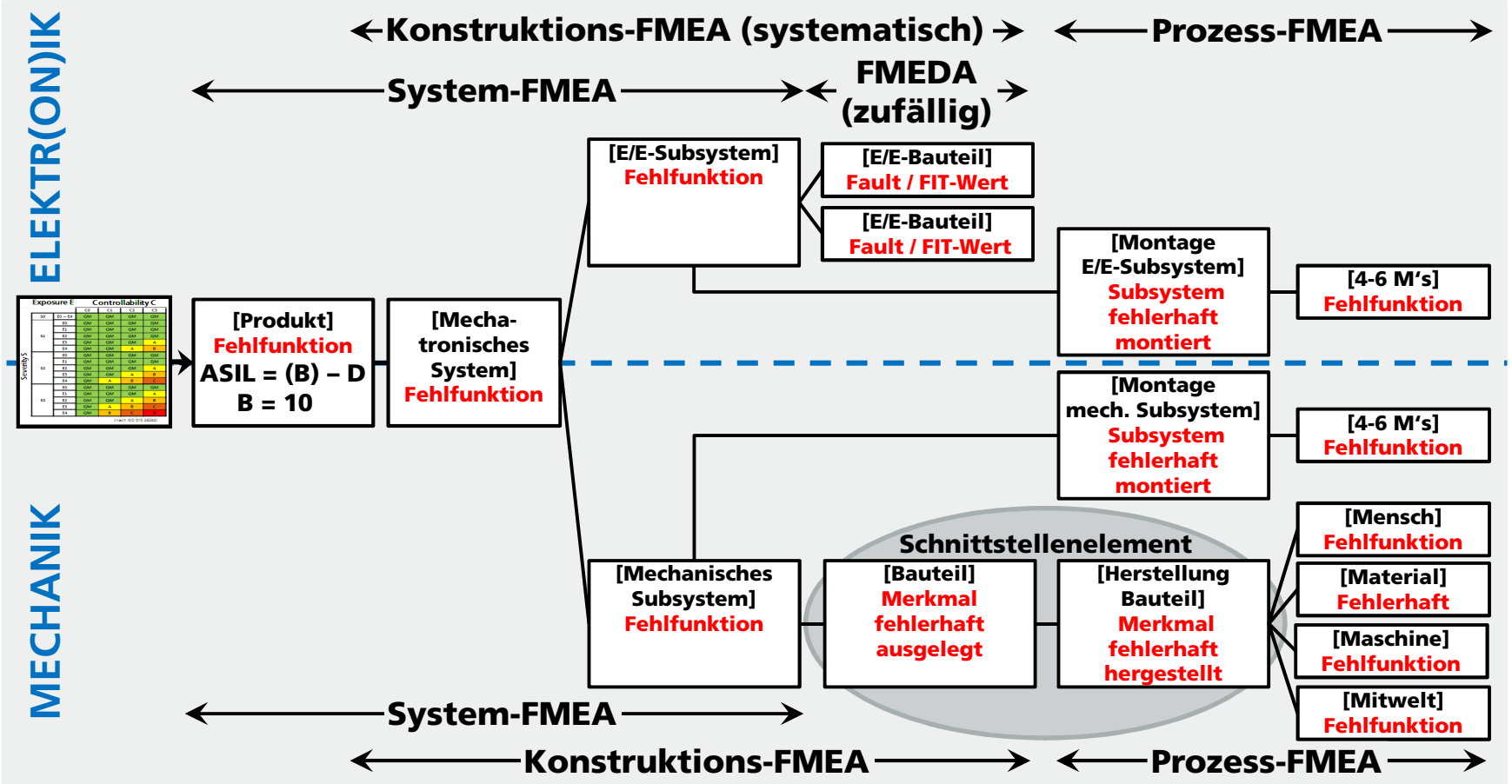


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

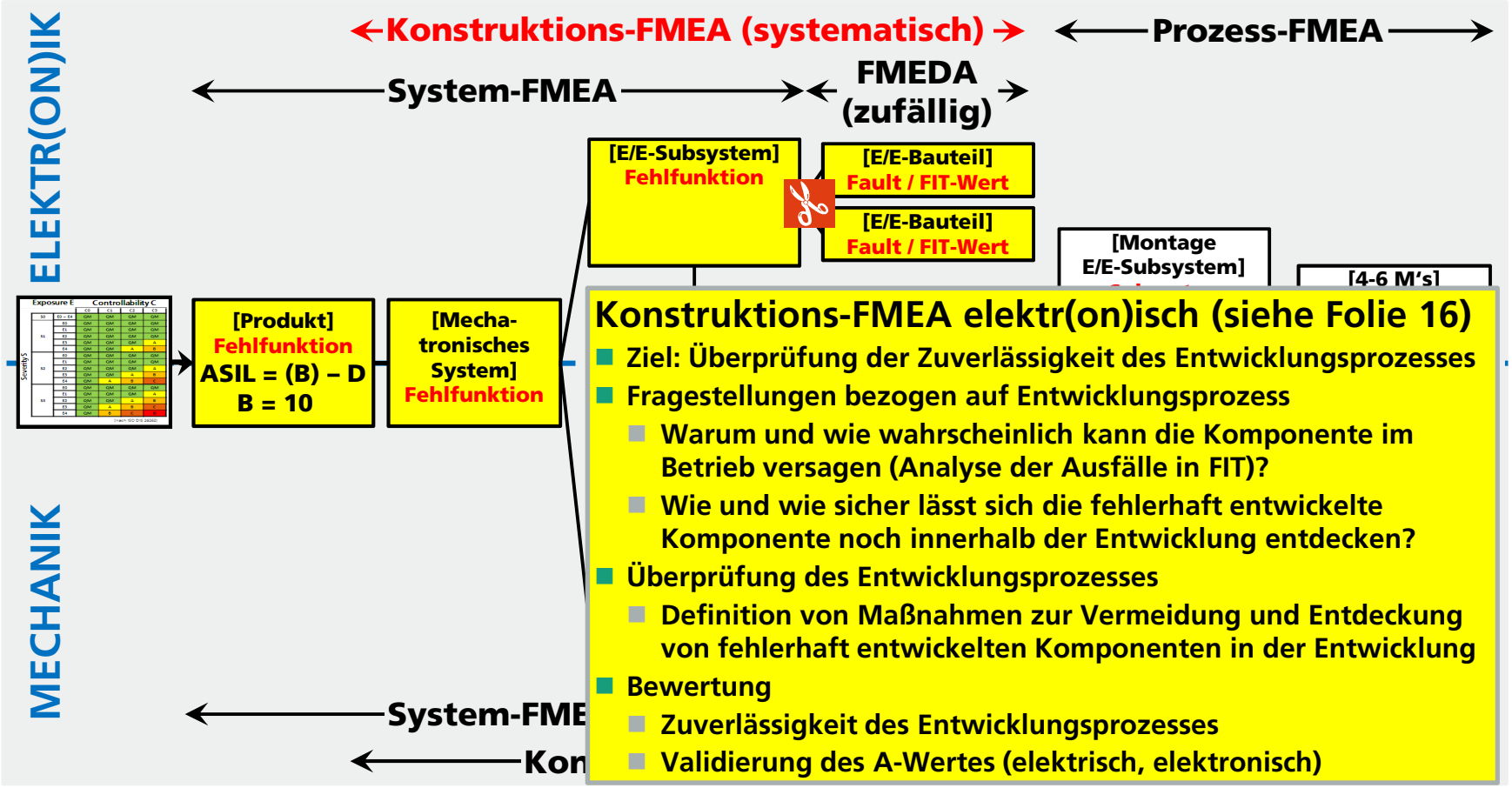


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

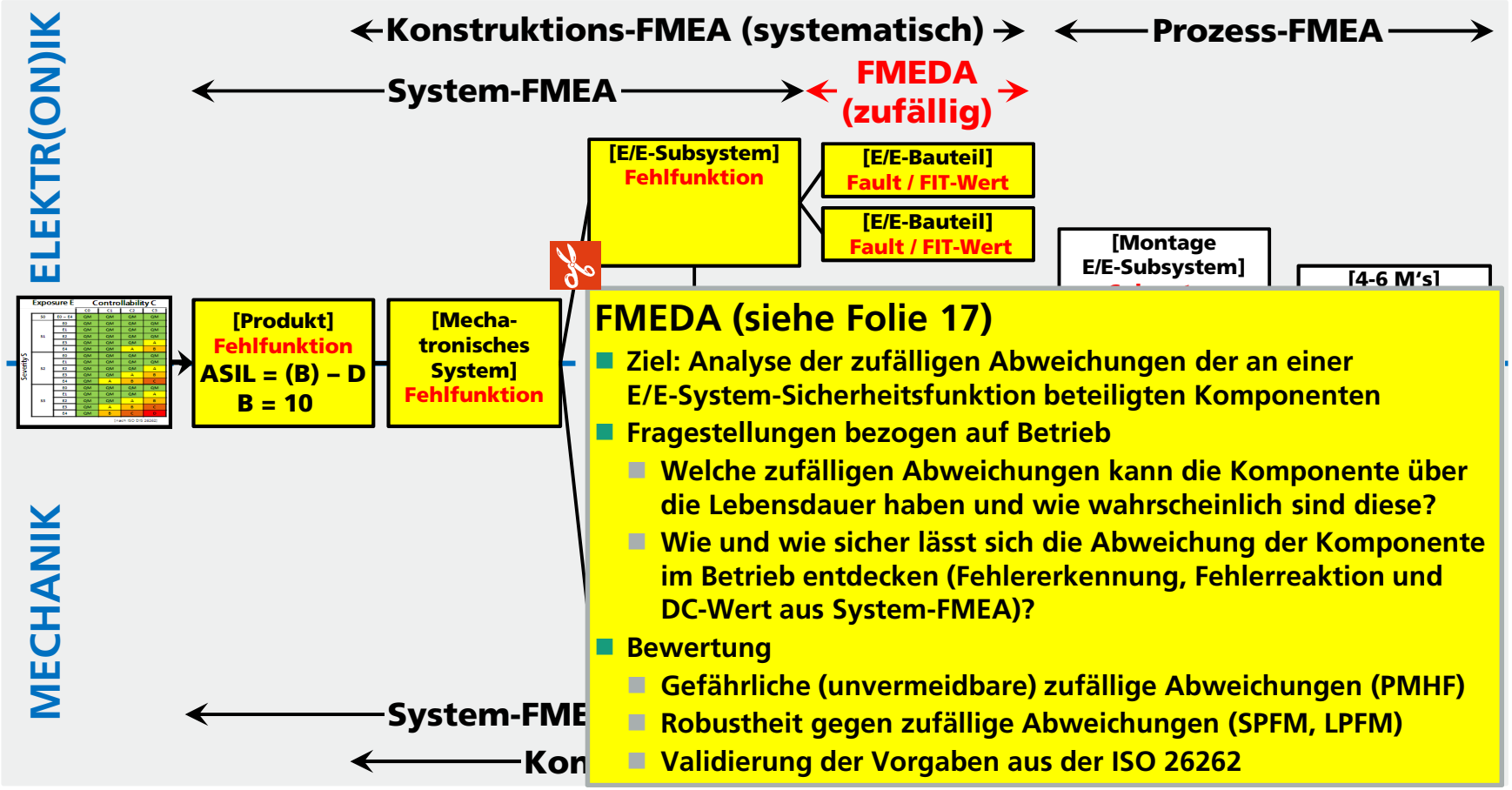


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

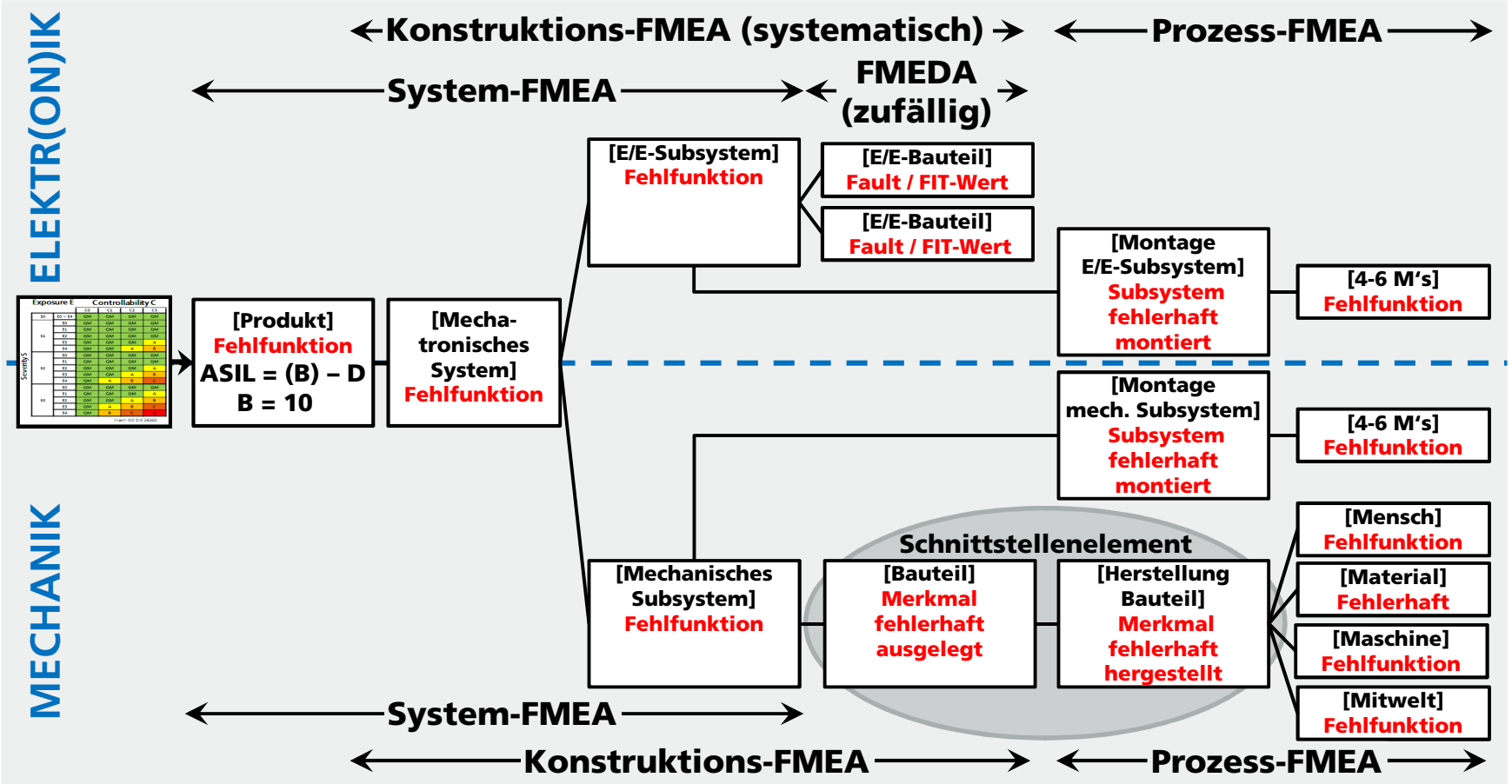


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

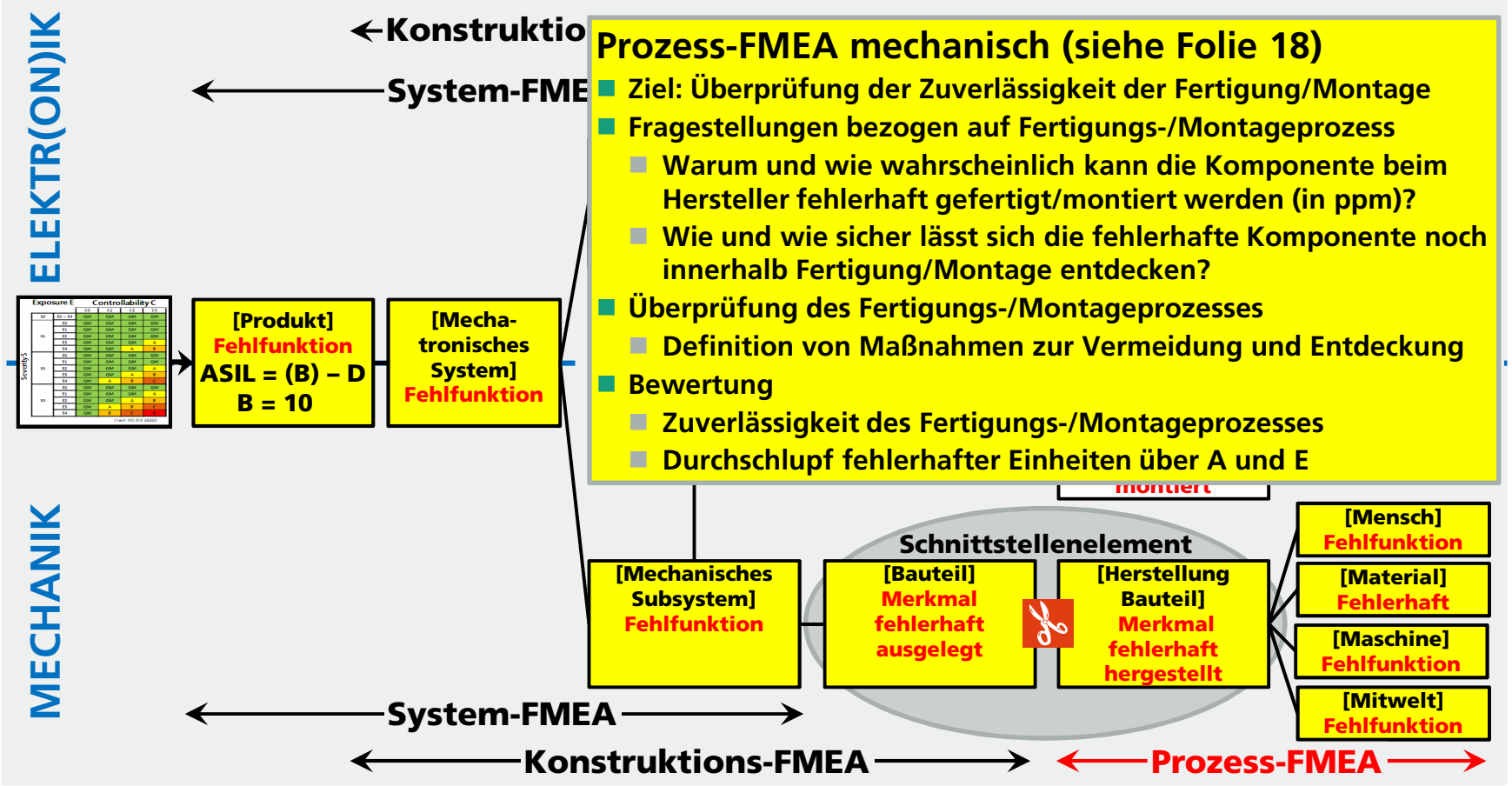


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

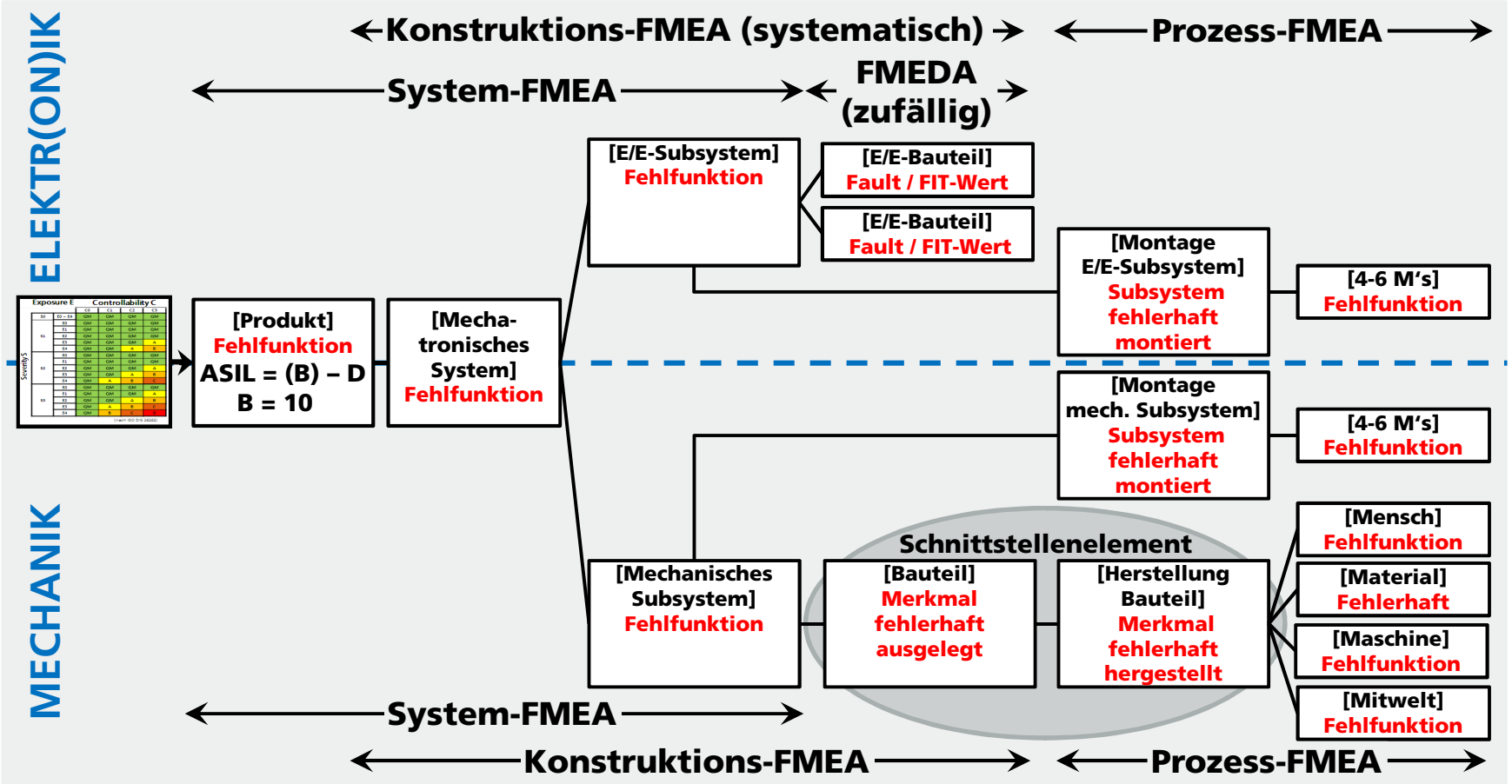


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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

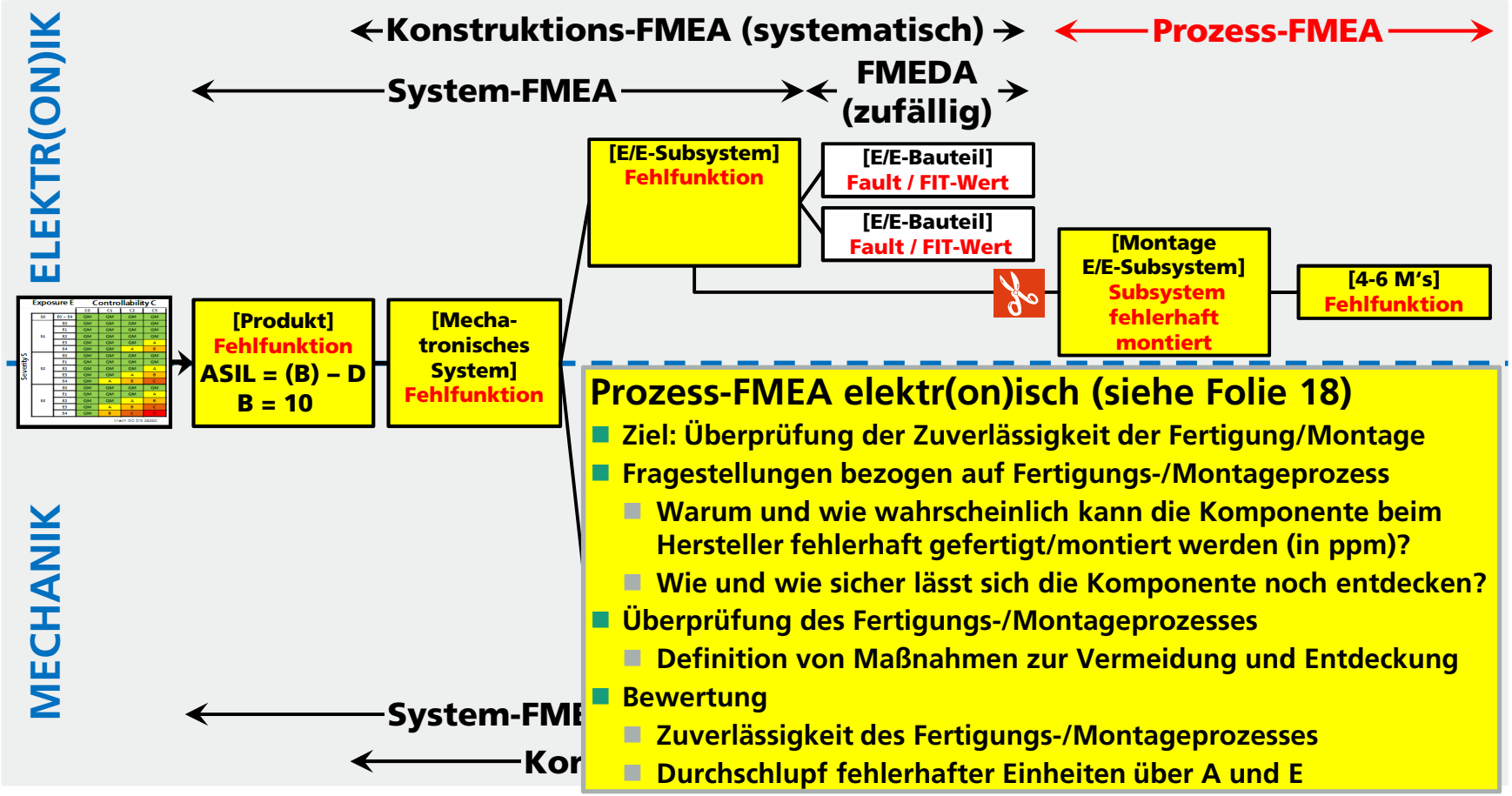


© Fraunhofer

Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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



© Fraunhofer

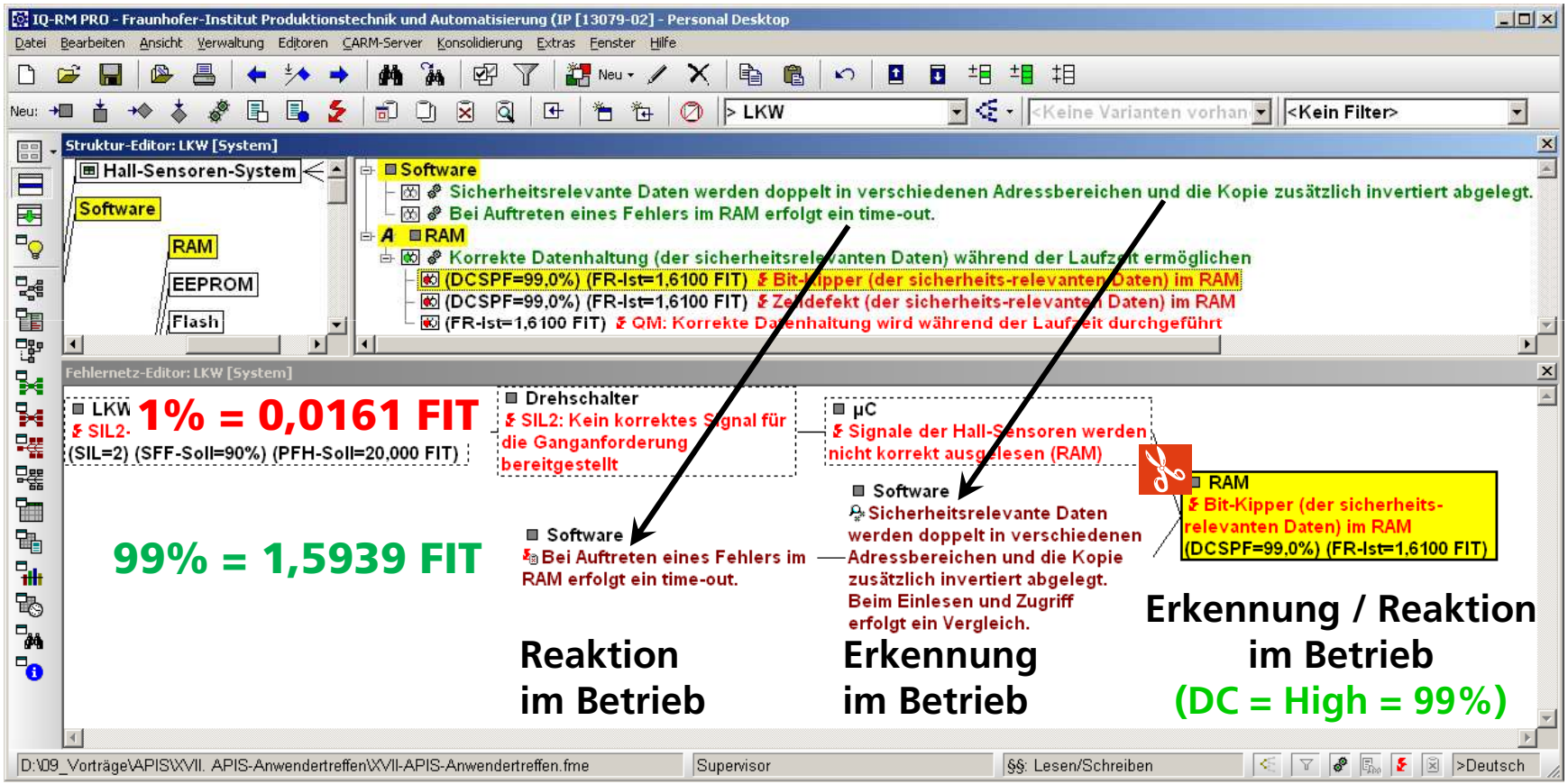
Fraunhofer IPA

ABBILDUNG IM PROJEKT (E/E-KOMPONENTEN)

© Fraunhofer

Beispiel: Einfacher Fehlerfall „Bit-Kipper im RAM“

Fehlererkennung und Fehlerreaktion (Sicherheits-konzept) im Betrieb (Beispiel nach DIN EN 61508)

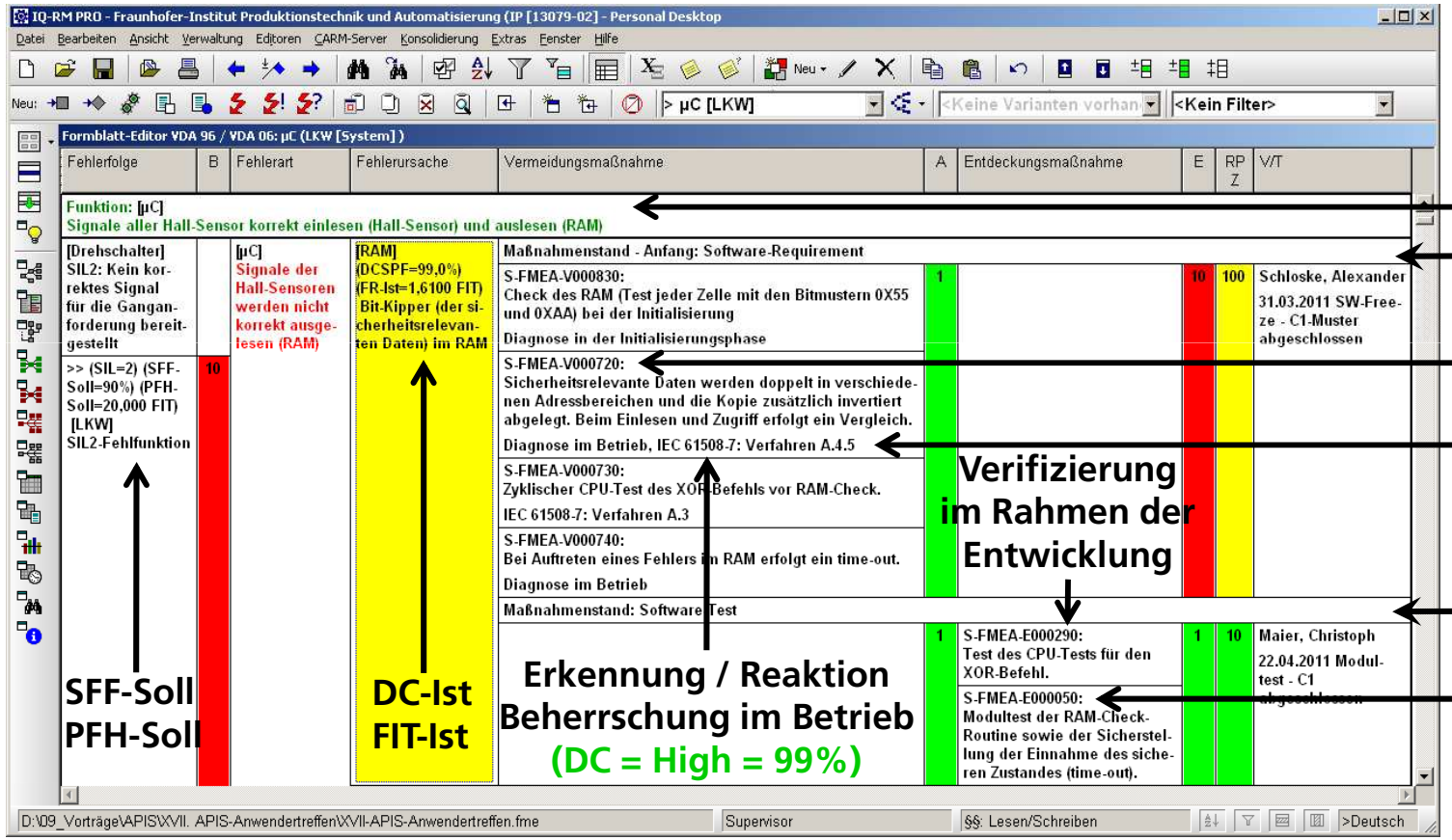


© Fraunhofer

Fraunhofer IPA

Beispiel: Zufällige Abweichung „Bit-Kipper im RAM“

FMEA-Formblattinhalte (Beispiel nach DIN EN 61508)

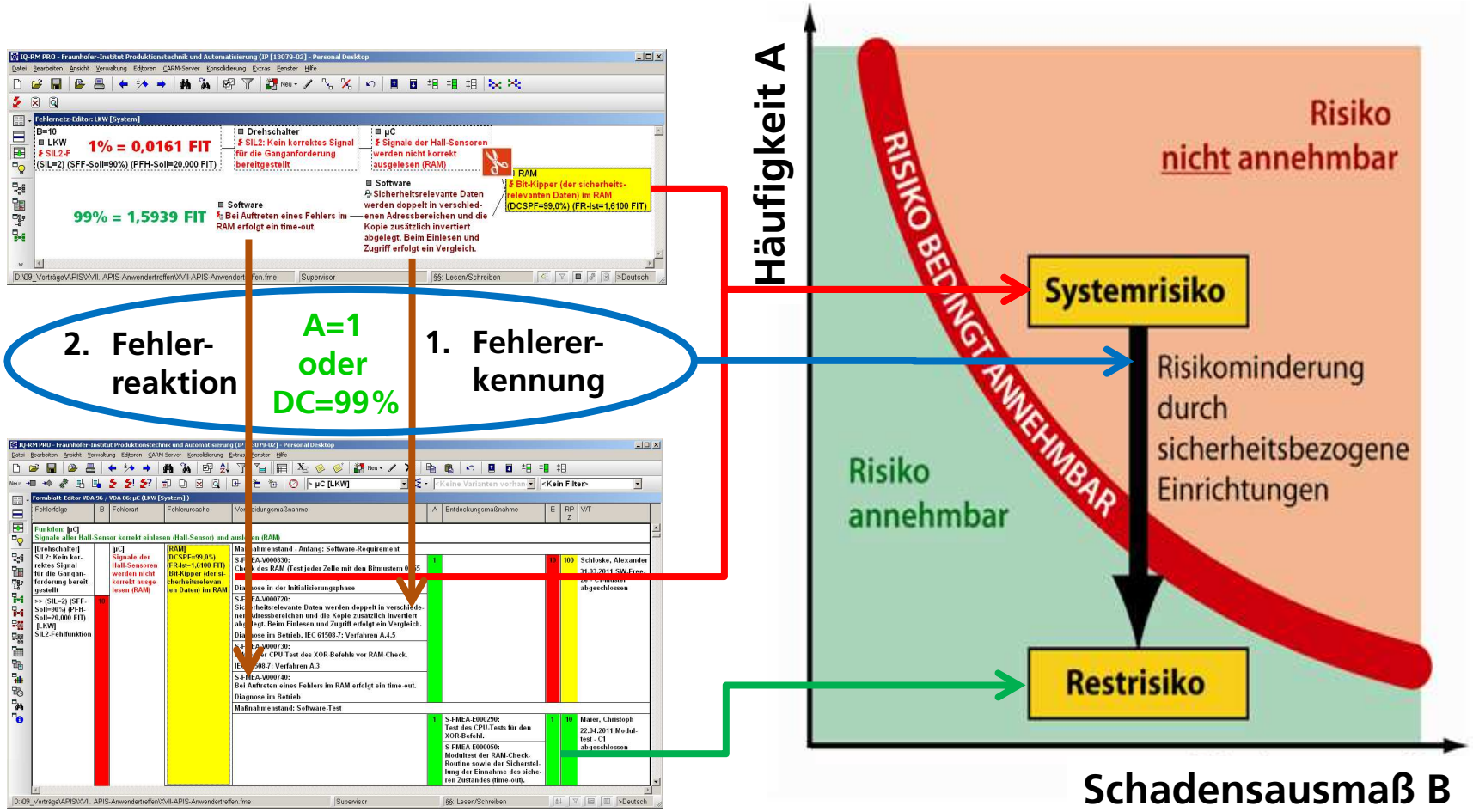


© Fraunhofer

Fraunhofer IPA

System-FMEA

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



© Fraunhofer

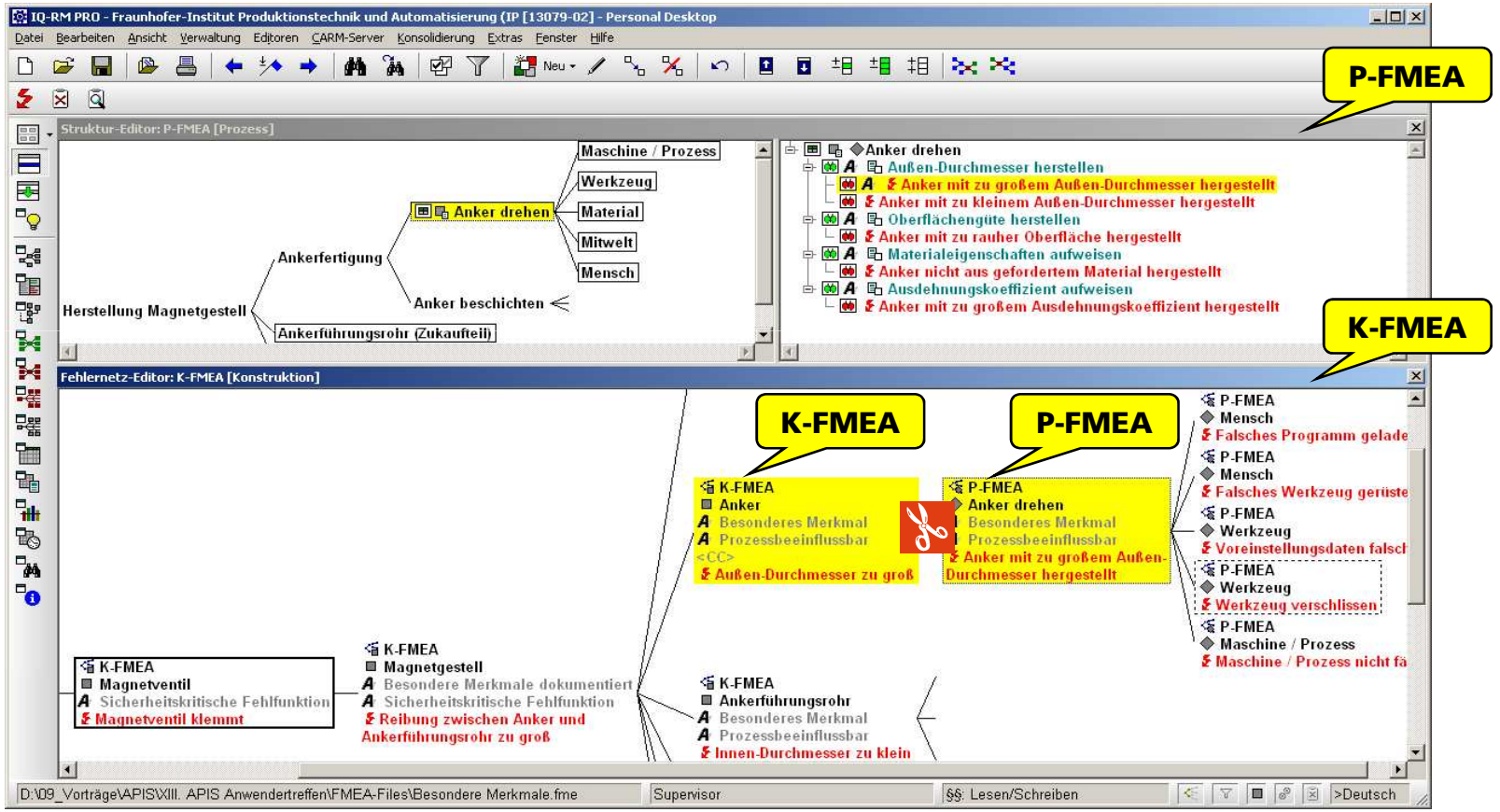
Fraunhofer IPA

ABBILDUNG IM PROJEKT (MECHANIK-KOMPONENTEN)

© Fraunhofer

Beispiel: Besondere Merkmale „Anker-Durchmesser“

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

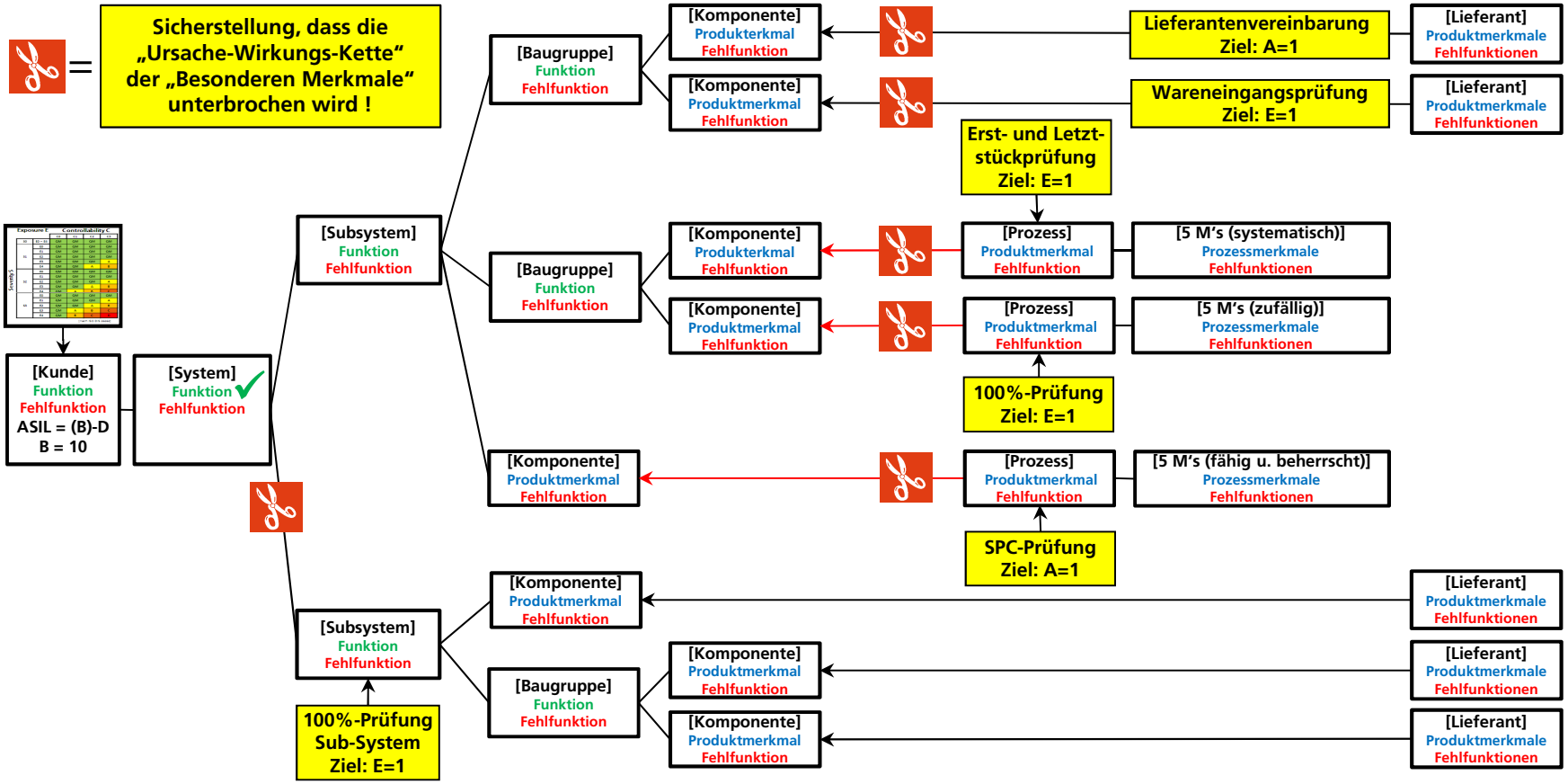


© Fraunhofer

Fraunhofer IPA

Besondere Merkmale

Vorgehensweise zur Analyse und Absicherung von mechanischen Systemen über Besondere Merkmale



© Fraunhofer

Fraunhofer IPA

FAZIT

© Fraunhofer

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!**

© Fraunhofer