ABSICHERUNG MECHATRONISCHER SYSTEME ÜBER FUNKTIONALE SICHERHEIT UND BESONDERE MERKMALE

XVIII. APIS-Anwendertreffen, 18.-19. September 2012, Würzburg

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 IPA

Vorstellung
Die Fraunhofer-Gesellschaft

60 Institute an rund 40 Standorten

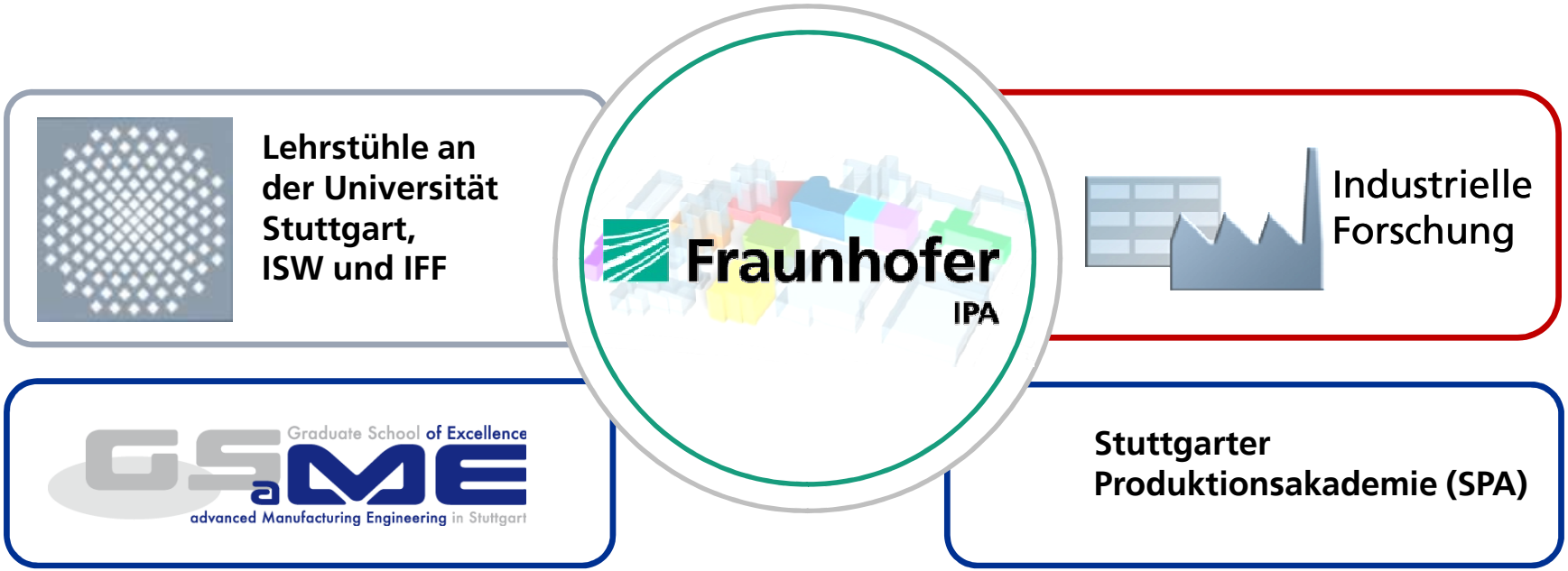
20.000 Mitarbeiter

1,9 Mrd. € Budget

Fraunhofer IPA

Vernetzung von Wissenschaft und Praxis

Fraunhofer IPA als Basis für den Wissenstransfer



Lehre → Forschung → Entwicklung → Realisierung → Anwendung

Erfahrungen aus der Industrie

Fraunhofer IPA

FRAGESTELLUNGEN

Fragestellungen

- Wie gehe ich mit elektr(on)ischen Komponenten bei ASIL-Systemen um?
- Wie gehe ich mit mechanischen Komponenten bei ASIL-Systemen um?
- Wo nehme ich die A-Bewertung und wo nehme ich die FIT-Werte?
- Wo nehme ich die E-Bewertung und wo nehme ich den DC-Wert?
- Muss ich FIT-Werte in A-Bewertungen umrechnen?
- Muss ich DC-Werte in E-Bewertungen umrechnen?
- Besondere Merkmale und Risikograph nach ISO 26262 – kann ich hier eine Verbindung aufbauen?

Vortragsgliederung

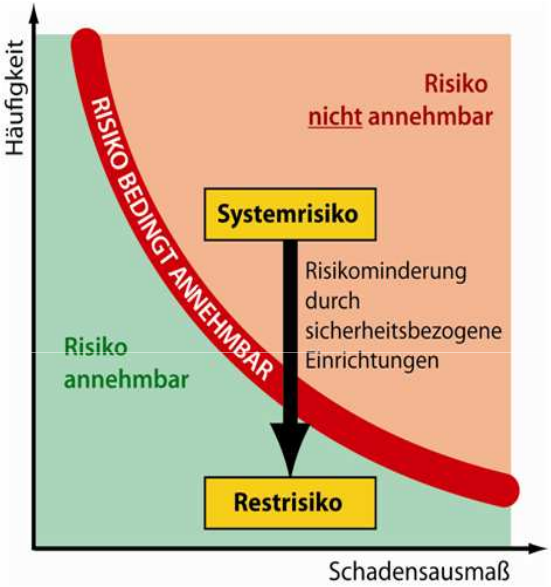
- Grundlagen Funktionale Sicherheit
- Grundlagen Besondere Merkmale
- Definitionen
- Denkmodell

GRUNDLAGEN
FUNKTIONALE SICHERHEIT

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)

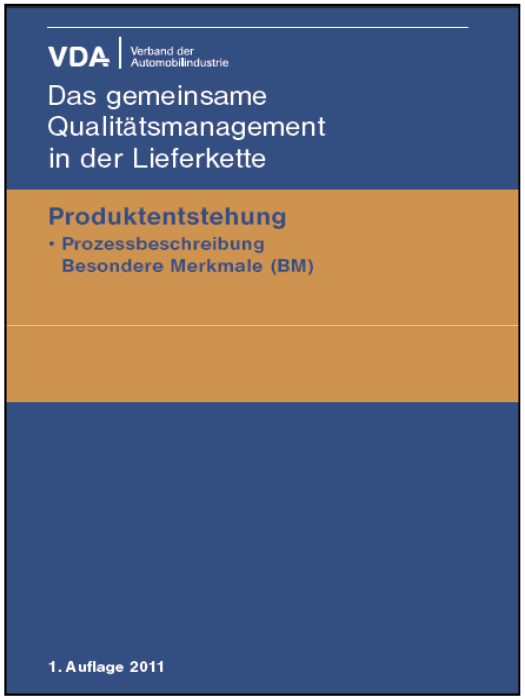
mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

Primärer Fokus: E/E-Systeme

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)

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

SORGFALTSPFLICHT IM PRODUKT-ENTSTEHUNGSPROZESS (PEP)

Fraunhofer IPA

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)

DEFINITIONEN

Definitionen
System-FMEA

- Zielsetzung: Überprüfung des Konzepts zur Funktionalen Sicherheit auf Logikfehler (systematische Fehler)
- Fragestellungen
  - Was kann im Betrieb passieren (und nicht warum passiert es)?
  - Wie lässt es sich im Betrieb entdecken und wie wird darauf reagiert?
  - Wie sicher sind die Entdeckungsmaßnahmen im Betrieb?
- Systemkonzept (Maßnahmen)
  - Definition von System-Fehlererkennung und System-Fehlerreaktion (Funktionales Sicherheitskonzept für E/E/PE- und mechanische Systeme)
- Bewertung
  - Bewertung der Sicherheit des Konzeptes zur Funktionalen Sicherheit
  - Validierung des DC-Wertes (mechanisch, elektrisch und elektronisch)

Definitionen
Konstruktions-FMEA

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

Definitionen
FMEDA (für elektrische/elektronische Komponenten)

- Zielsetzung: Analyse der zufälligen Abweichungen der an einer E/E-System-Sicherheitsfunktion beteiligten Komponenten
- Fragestellungen
  - 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
  - Bewertung der Robustheit gegen zufällige Fehler (PMHF, SPFM, LPFM)
  - Validierung der Vorgaben aus der ISO 26262

Definitionen
Prozess-FMEA

- Zielsetzung: Überprüfung der Zuverlässigkeit der Fertigung/Montage
- Fragestellungen
  - Warum und wie wahrscheinlich kann die Komponente beim Hersteller fehlerhaft gefertigt/montiert werden?
  - Wie und wie sicher lässt sich die fehlerhaft gefertigte/montierte Komponente noch innerhalb der Fertigung/Montage entdecken?
- Maßnahmen
  - Definition von Maßnahmen zur Vermeidung und Entdeckung von Fehlern in der Fertigung/Montage
- Bewertung
  - Bewertung der Zuverlässigkeit der Fertigung/Montage
  - Bewertung des Durchschlupfs 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)
  - 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

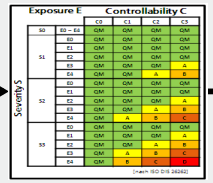
DENKMODELL

Denkmodell zur Analyse von Mechatronischen Systemen

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

ELEKTR(ON)IK

Risikograph



Elektrisches / Elektronisches System (E/E-System)

- Absicherung über ISO 26262 und System-FMEA
  -> Safety Requirement Specifications (SRS)
  -> Software-Algorithmen
- Absicherung von Verschleißteilen im Betrieb
  -> Safety Requirement Specifications (SRS)
  -> Software-Algorithmen

Gefährdungs-analyse und Risiko-abschätzung

MECHANIK

B = 10 (BM S)

Mechanisches System

- Absicherung über Konstruktions-/Prozess-FMEA
  -> Besondere Merkmale
  -> Prüfplan (100%, Stichproben- und SPC-Prüfung)
- Identifikation von Verschleißteilen in der FMEA

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		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)

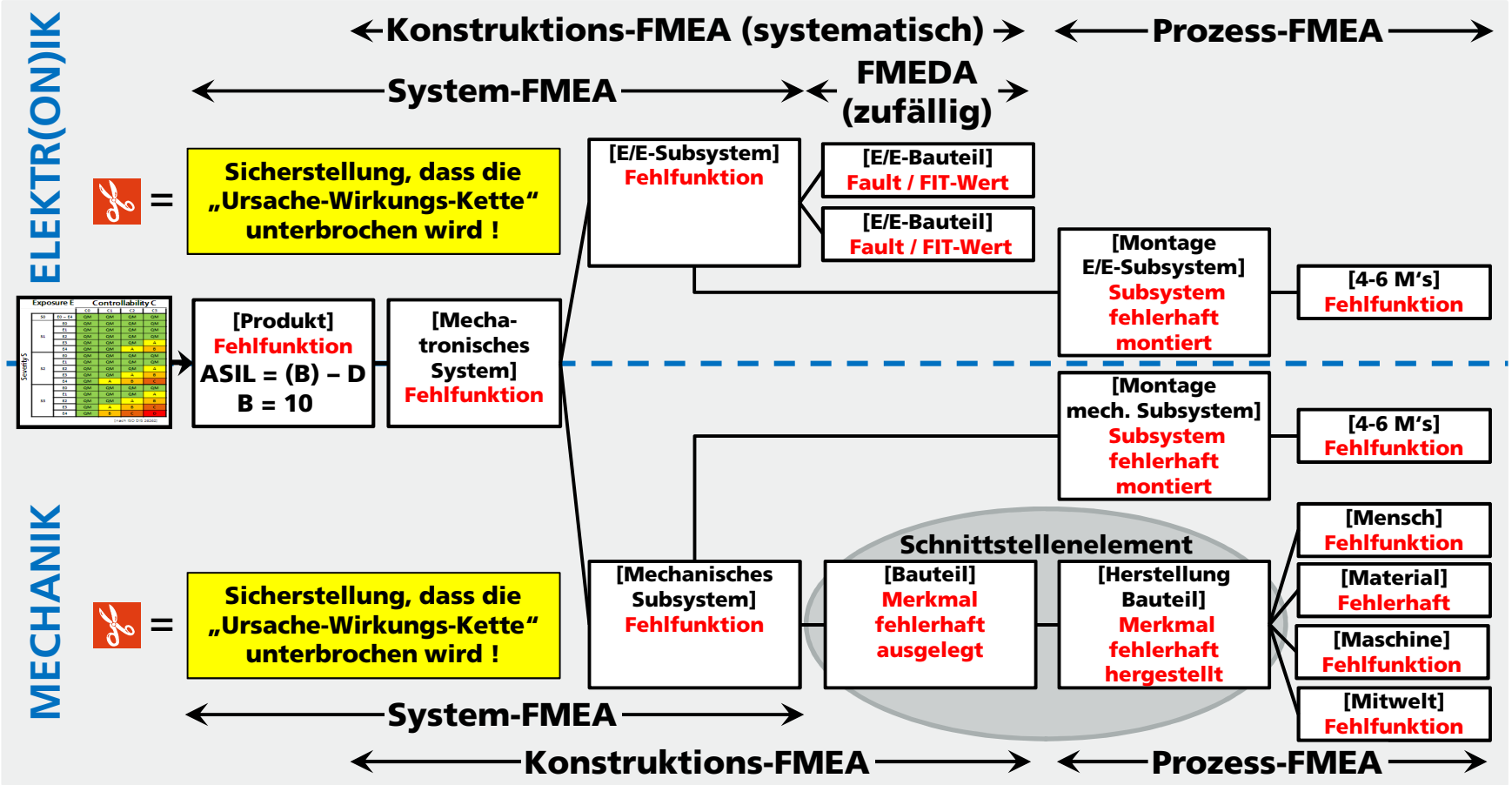
E1: **selten:** Situation tritt für die meisten Fahrer seltener als einmal pro Jahr auf
E2: **gelegentlich:** Situation tritt für die meisten Fahrer wenige Male pro Jahr auf
E3: **ziemlich oft:** Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf
E4: **oft:** Situation die bei nahezu 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

Denkmodell zur Analyse von Mechatronischen Systemen

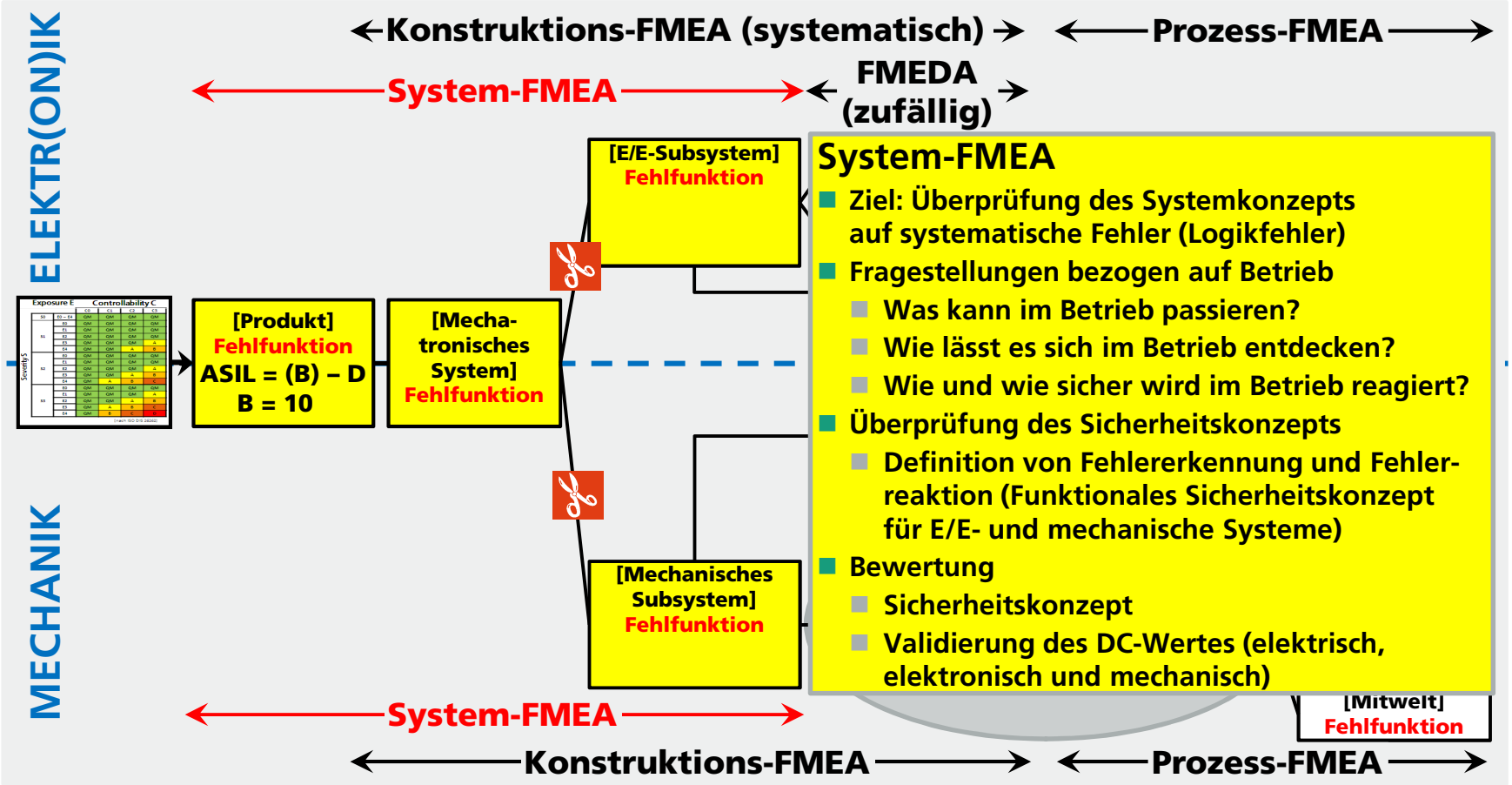
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

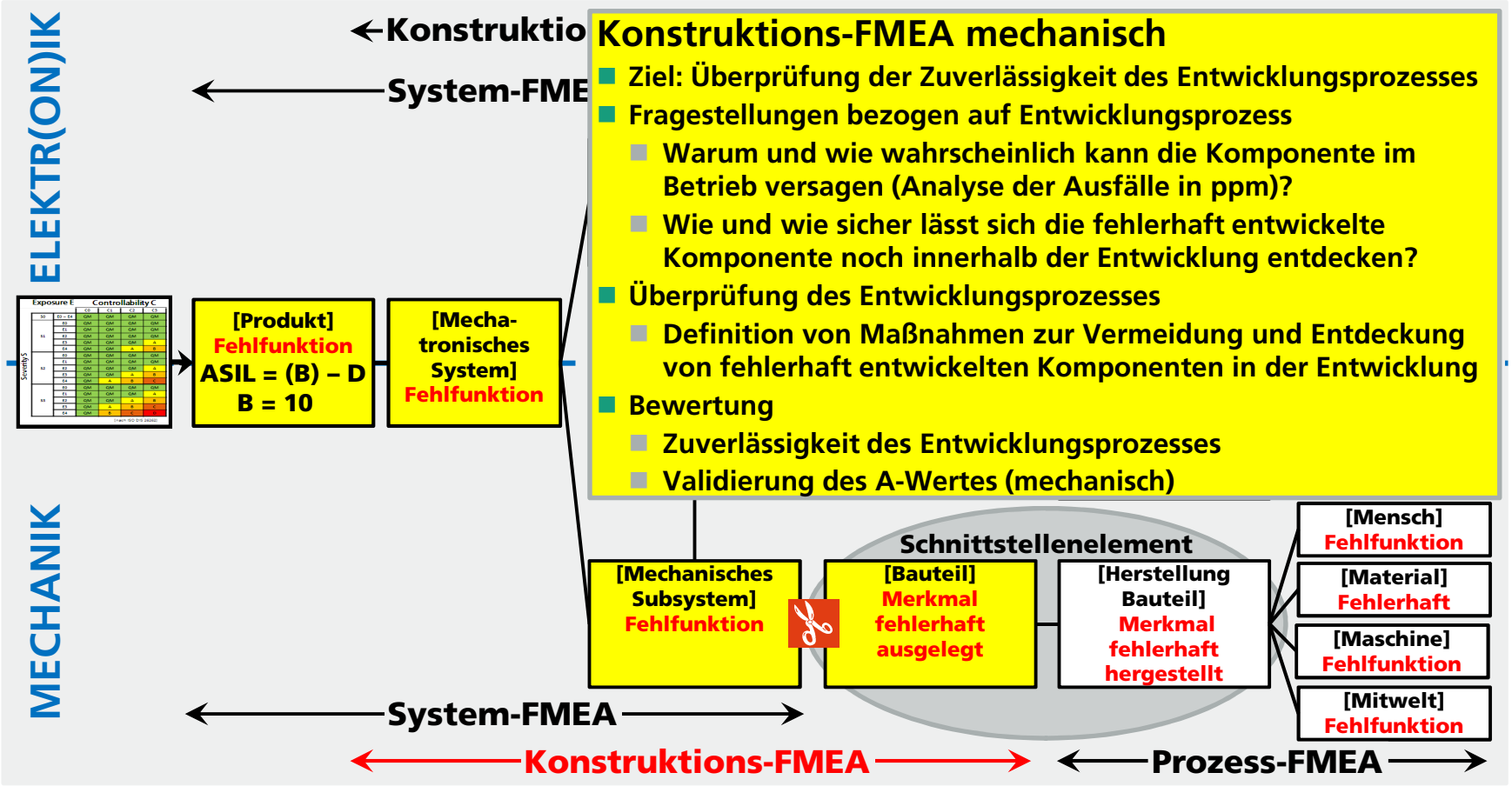
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

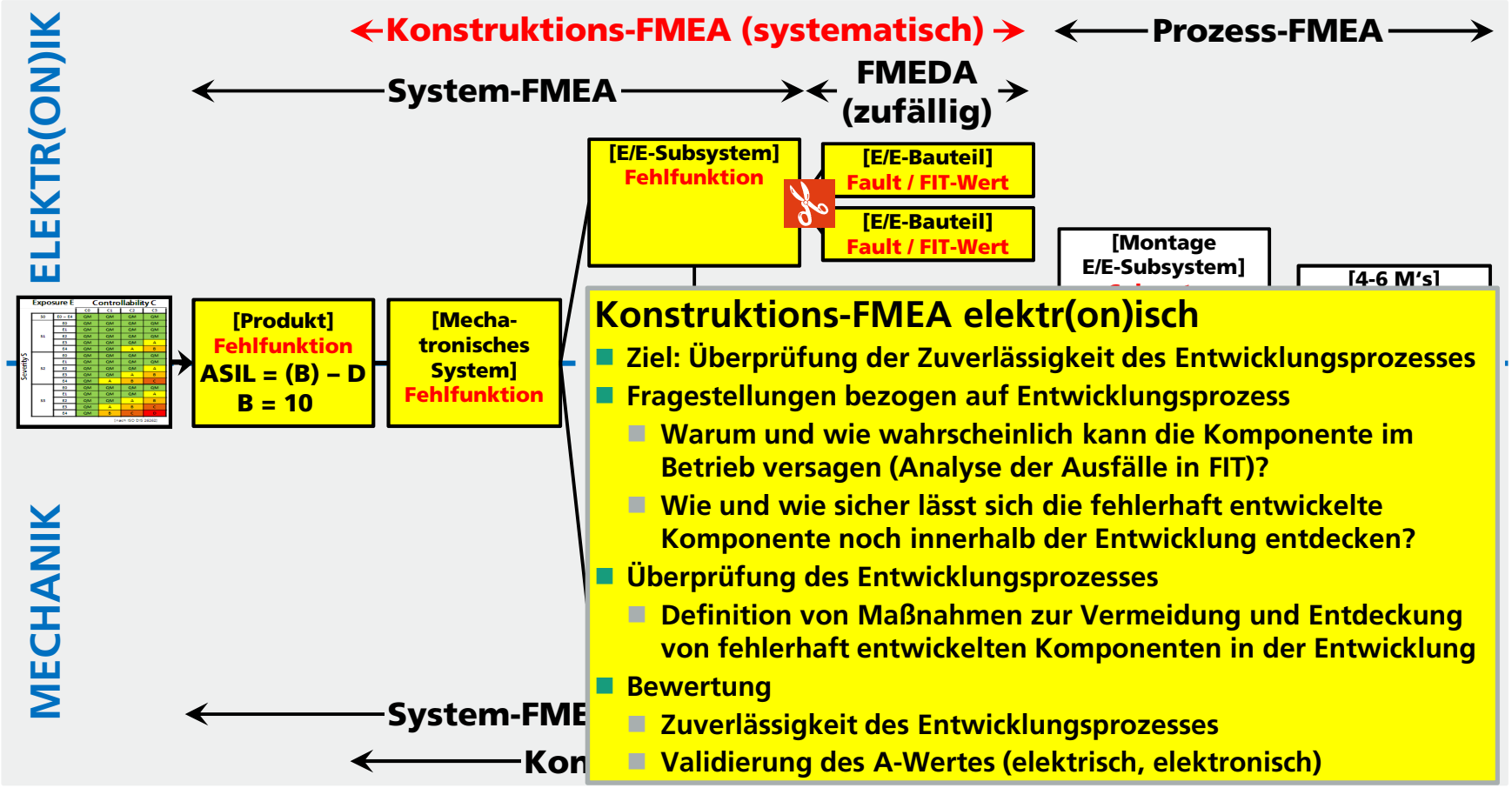
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

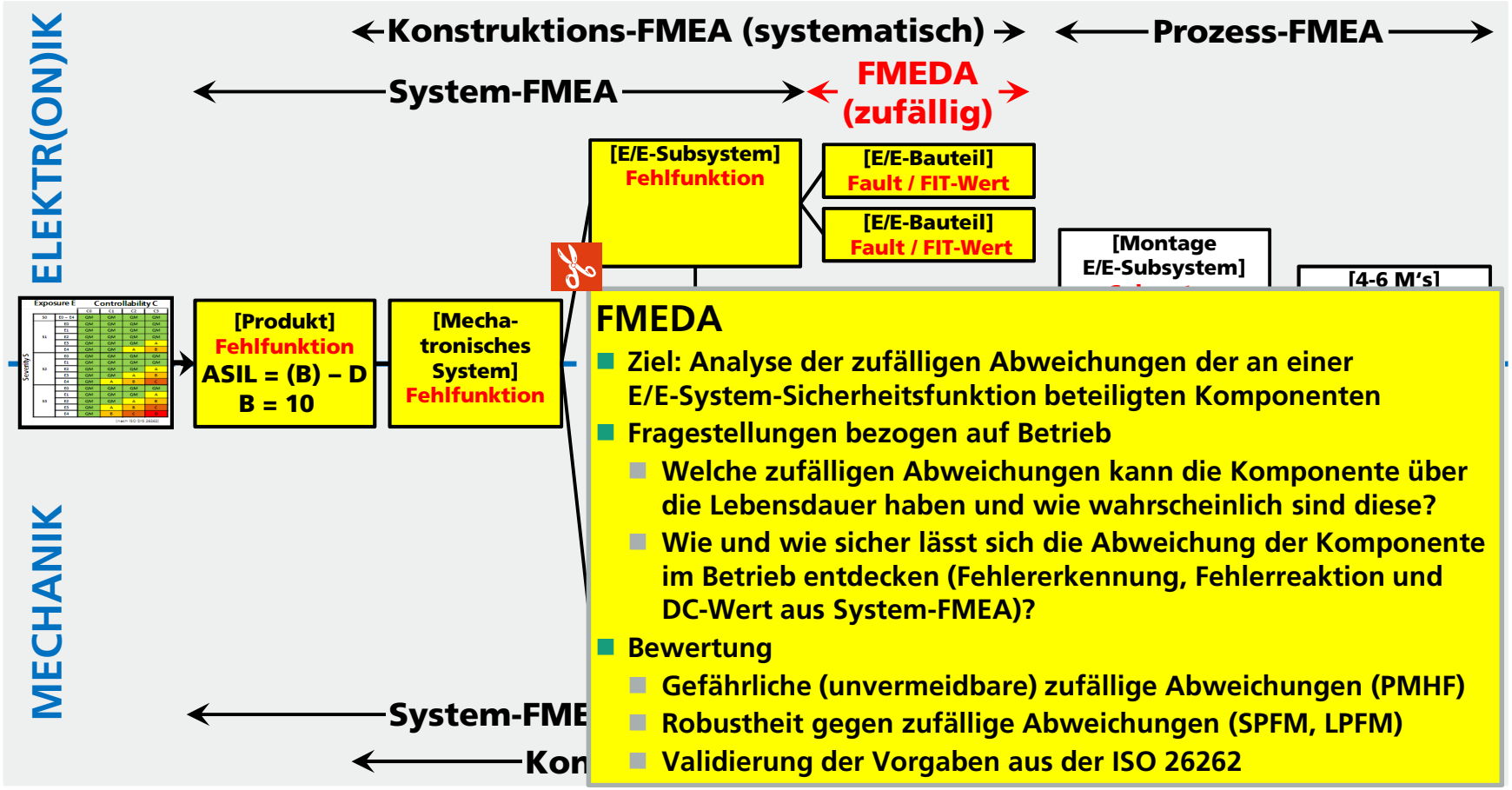
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

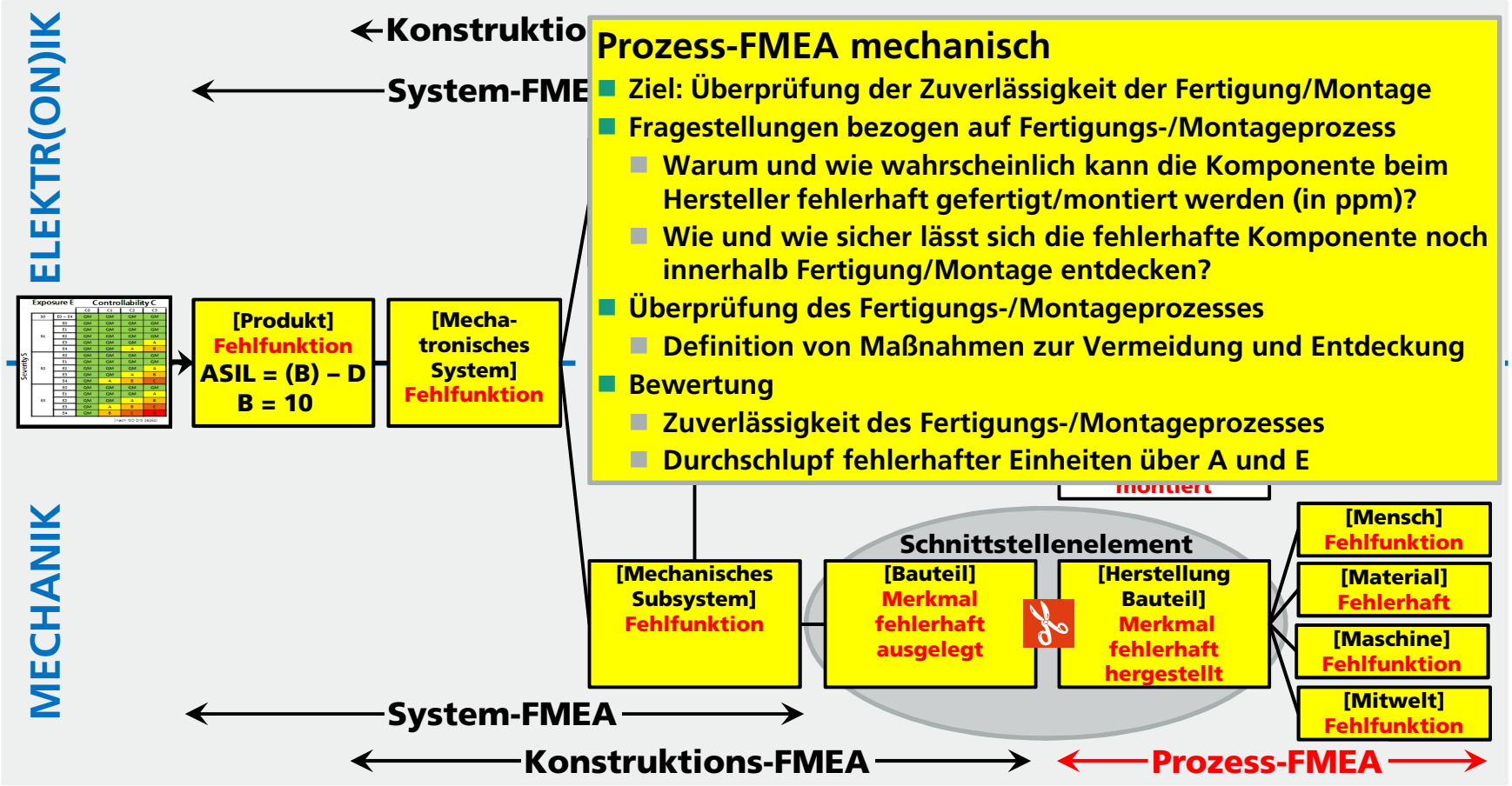
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

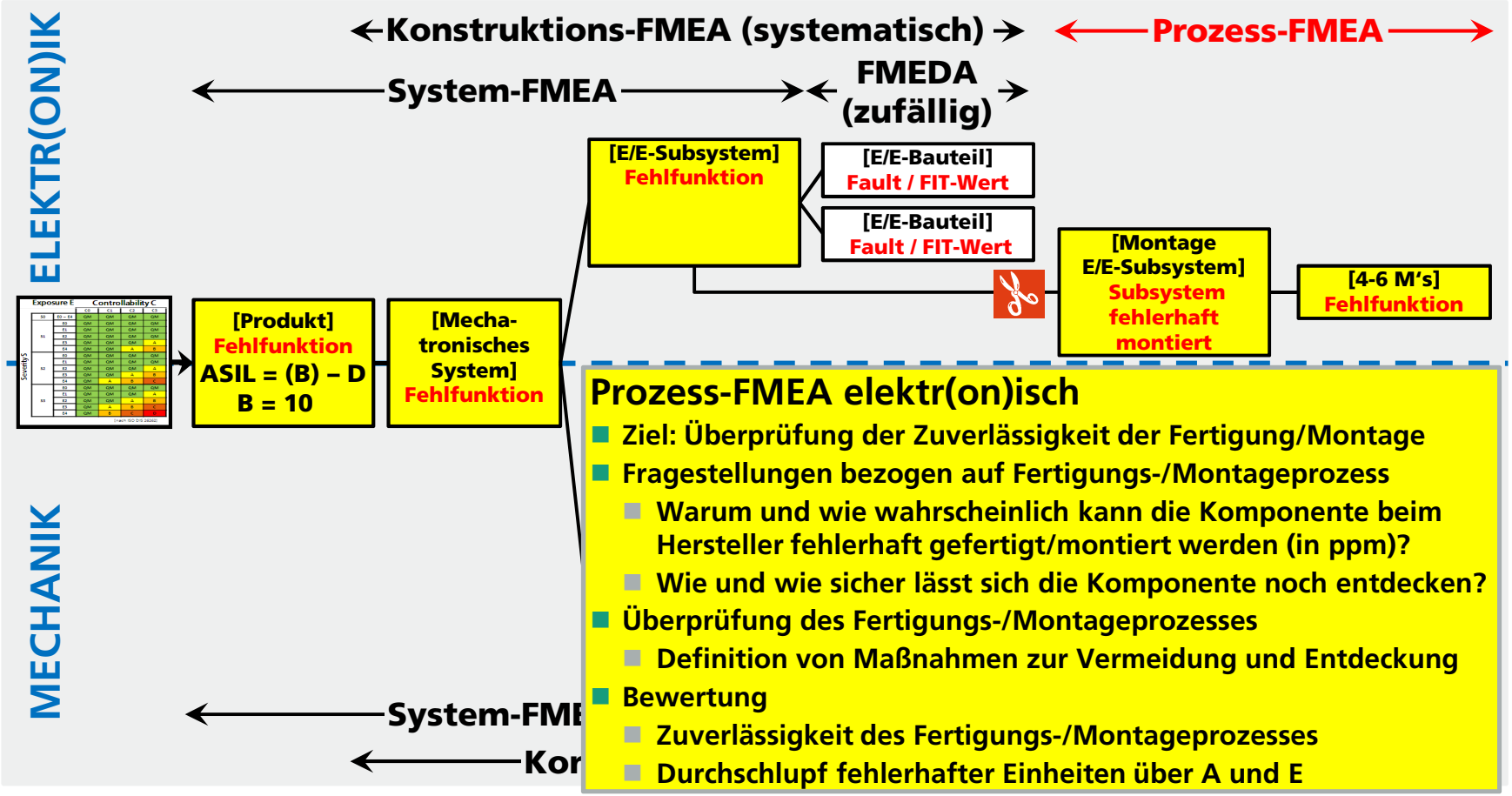
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

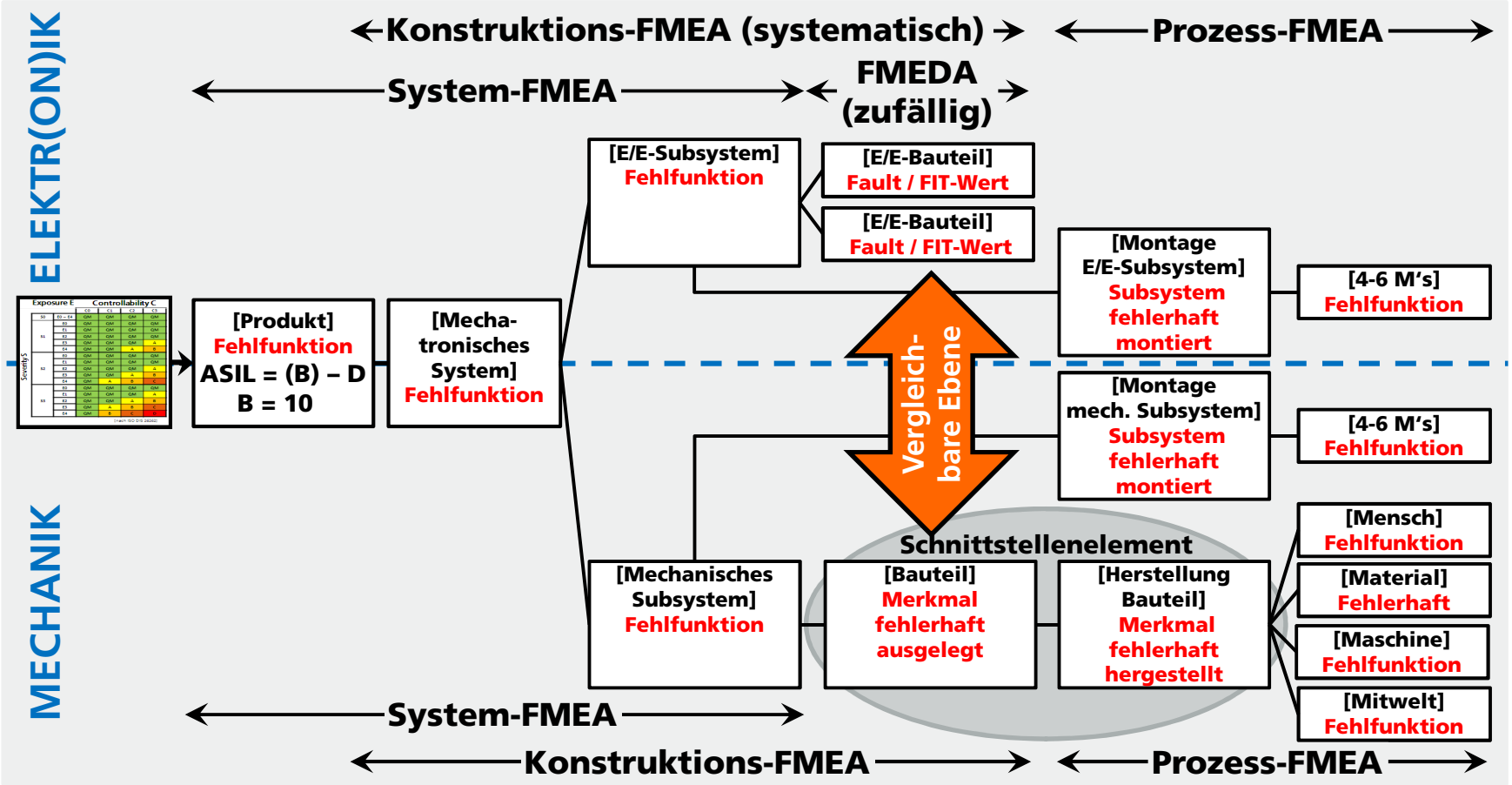
Einordnung der verschiedenen FME(D)A-Arten und deren Zusammenhang über Risikograph und Fehlernetz



Fraunhofer IPA

Denkmodell zur Analyse von Mechatronischen Systemen

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



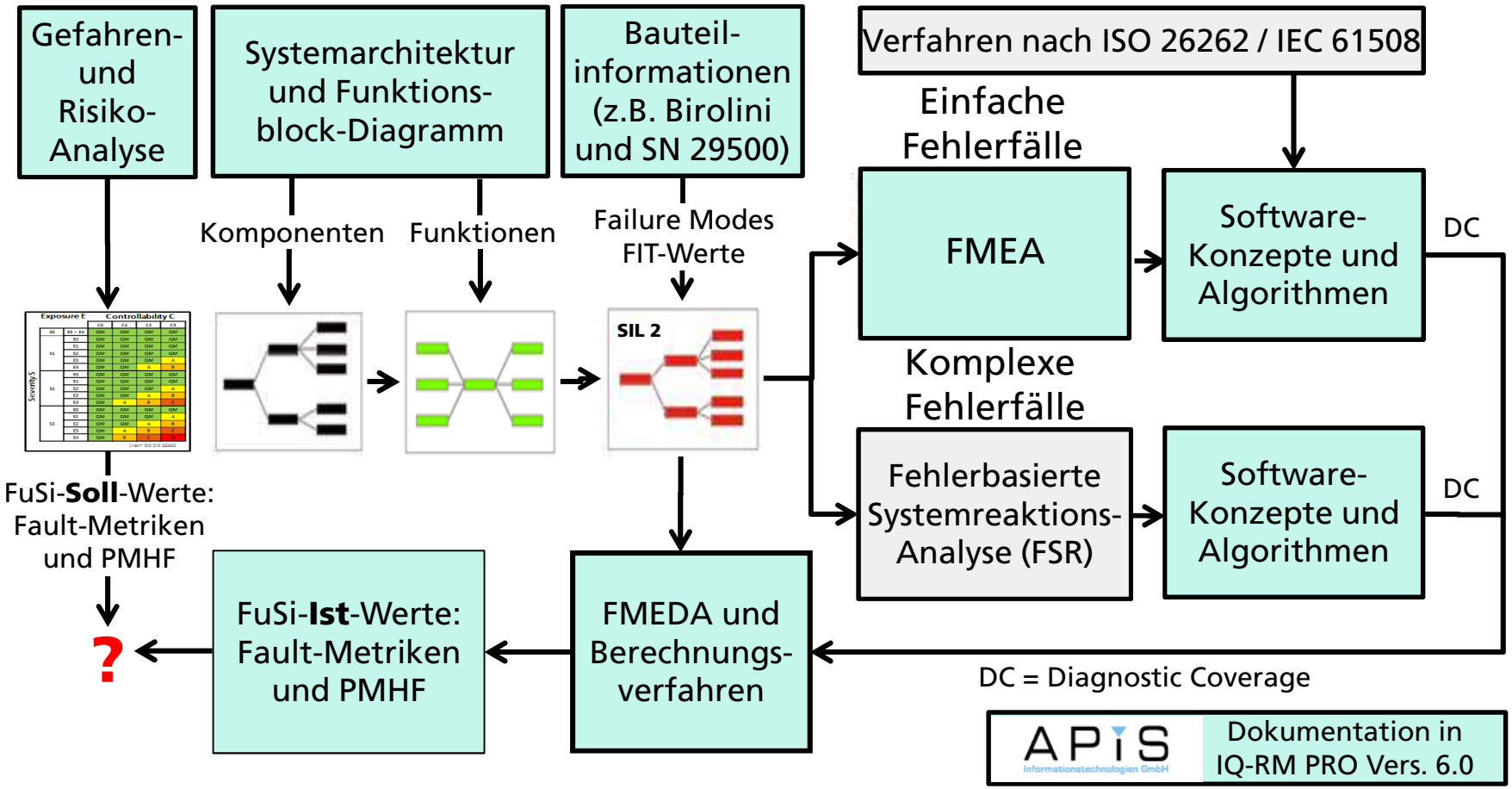
Fraunhofer IPA

VORGEHENSWEISE ZUR ANALYSE MECHATRONISCHER SYSTEME

Fraunhofer IPA

Funktionale Sicherheit

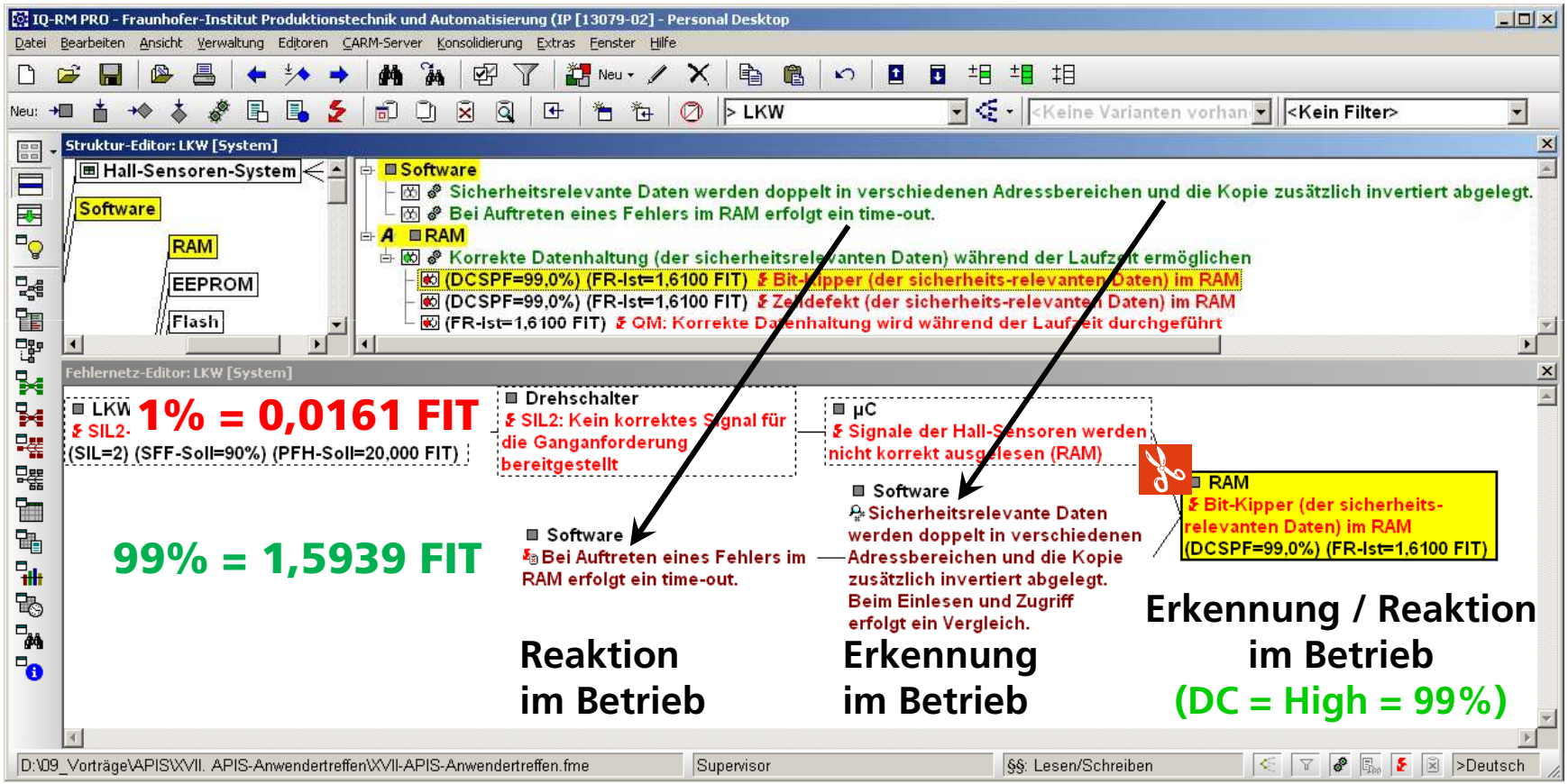
Vorgehensweise zur Analyse und Absicherung funktional sicherer mechatronischer Systeme



Fraunhofer IPA

Beispiel: Einfacher Fehlerfall „Bit-Kipper im RAM“

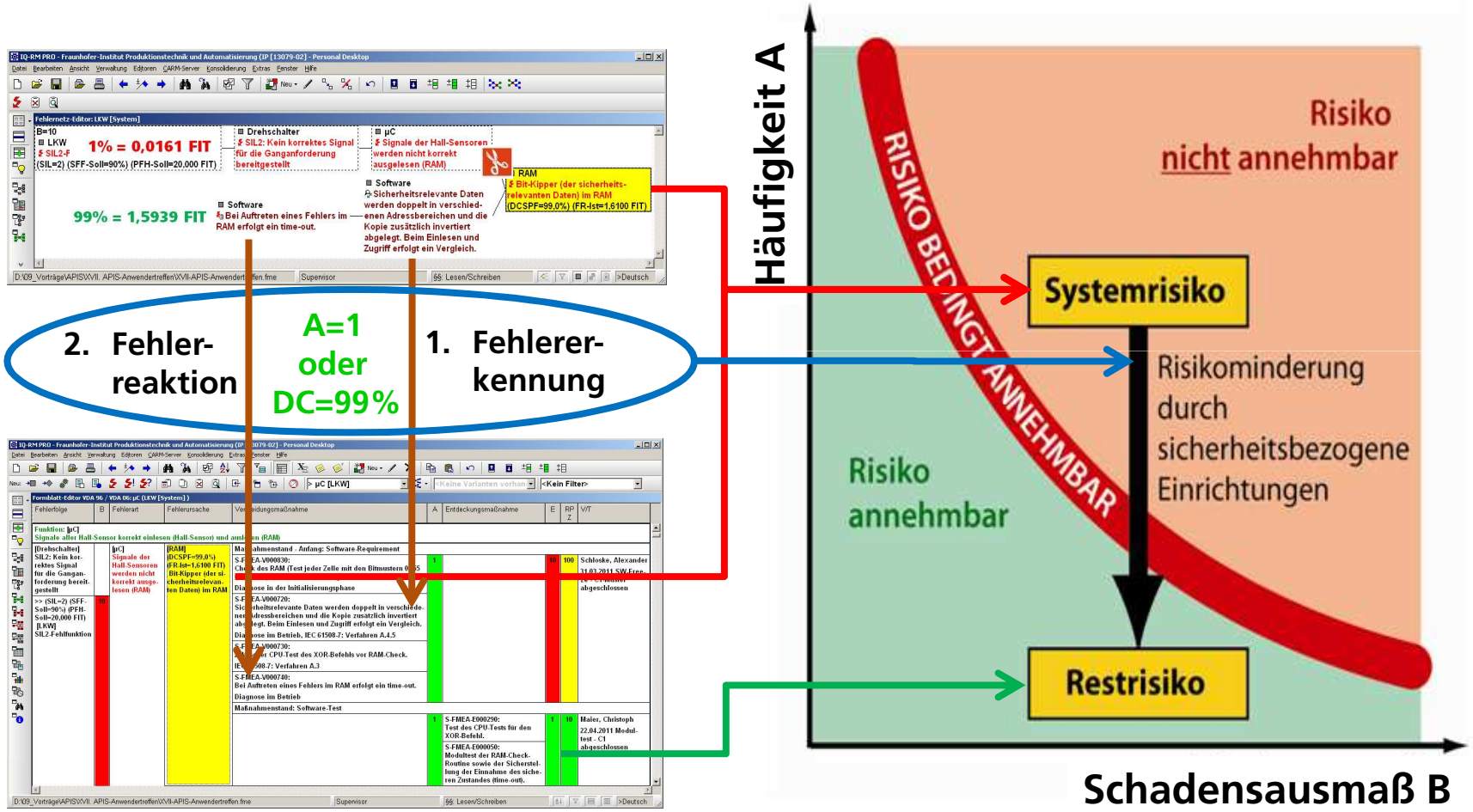
Fehlererkennung und Fehlerreaktion im Betrieb durch die Software



Fraunhofer IPA

System-FMEA

Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb

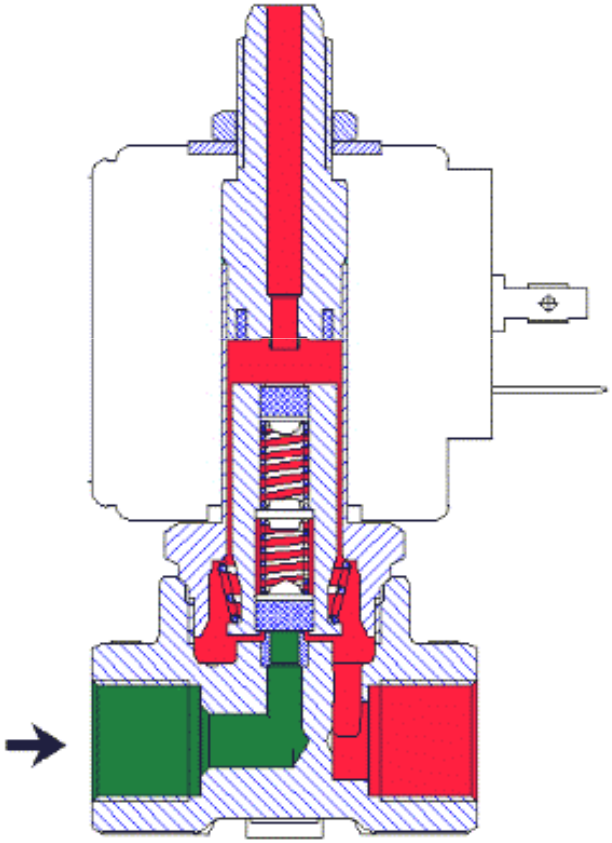


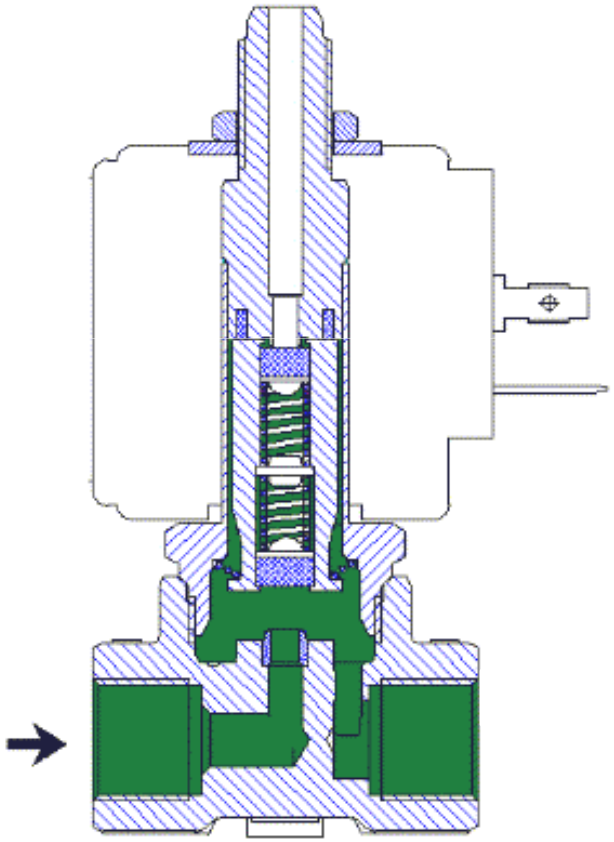
Fraunhofer IPA

VORGEHENSWEISE ZUR ANALYSE BESONDERER MERKMALE

Fraunhofer IPA

Beispielsystem Magnetventil
Funktionsprinzip

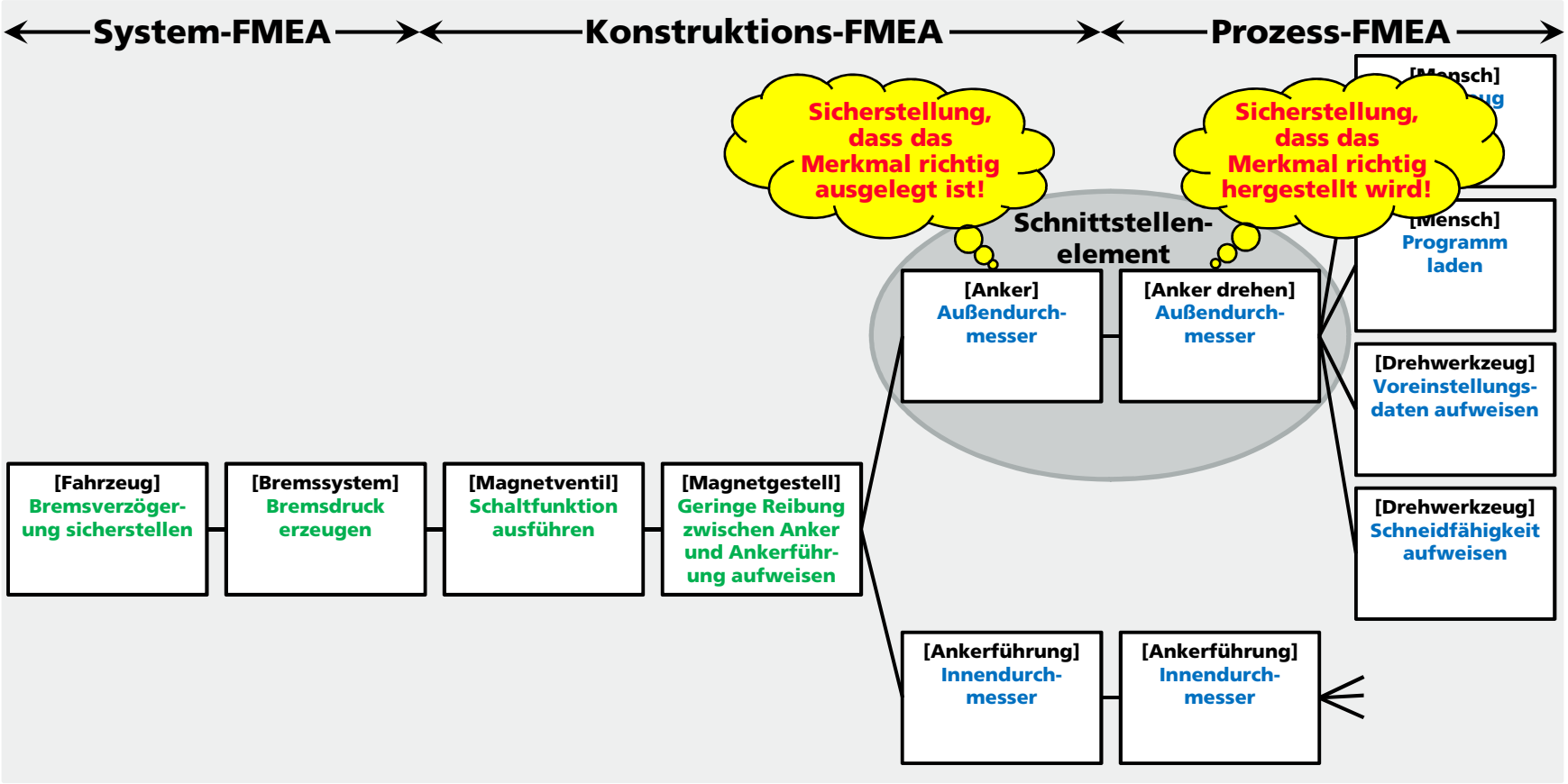




Bildquelle: http://www.magnetventile-shop.de

Koppelung von Konstruktions-FMEA und Prozess-FMEA

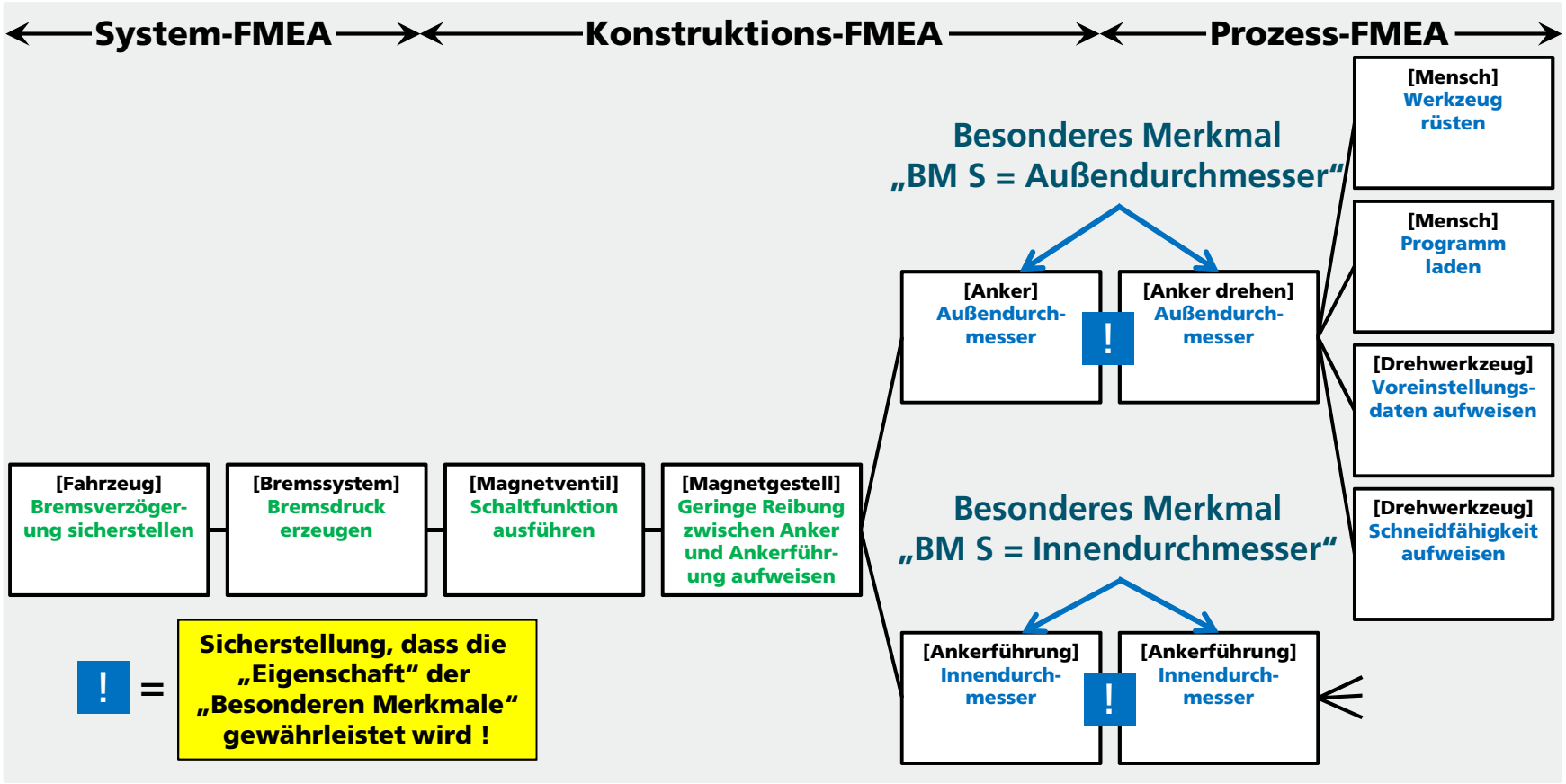
Systematische Ermittlung und durchgängige Betrachtung mittels Funktionsnetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

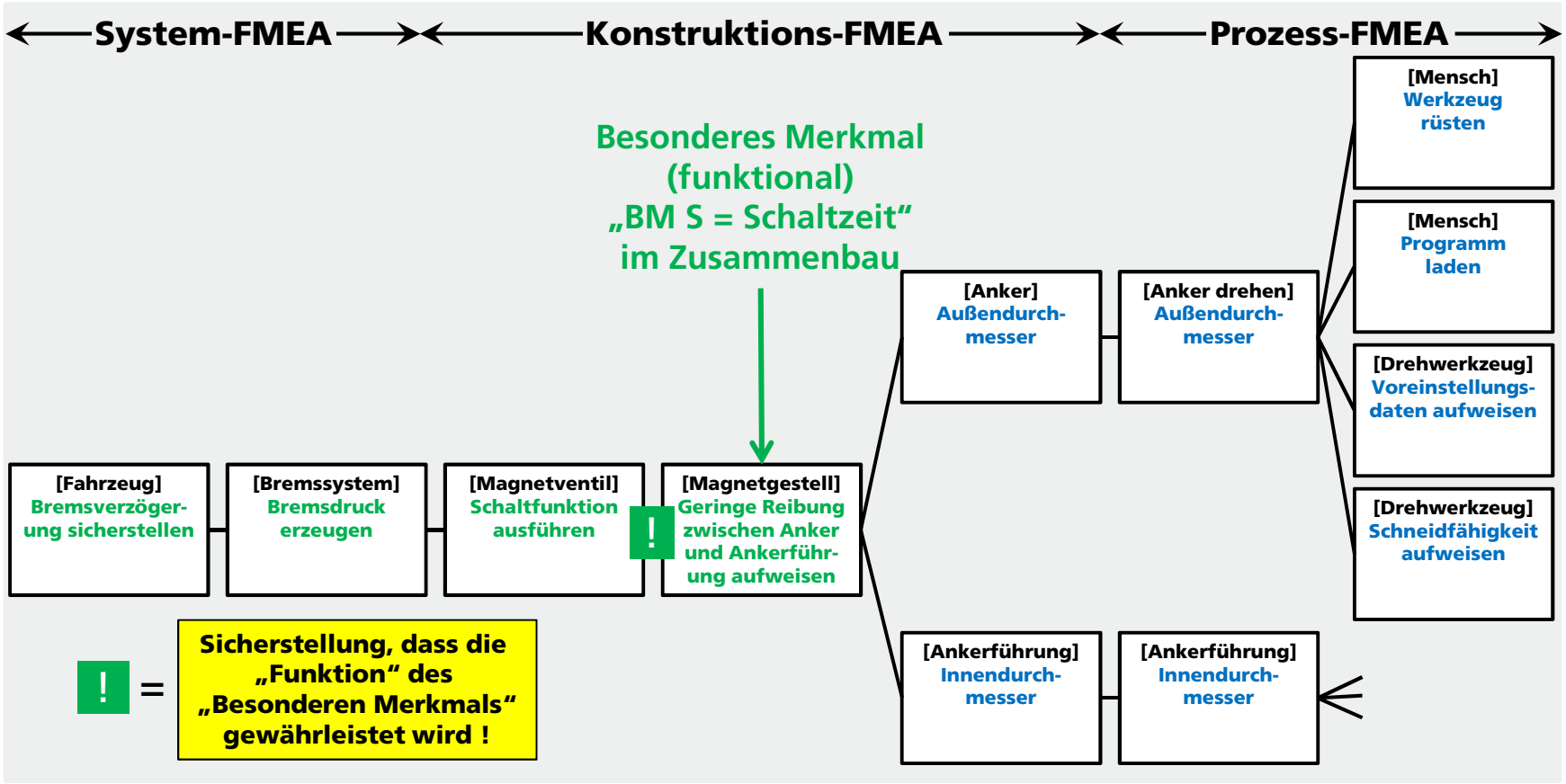
Systematische Ermittlung und durchgängige Betrachtung mittels Funktionsnetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

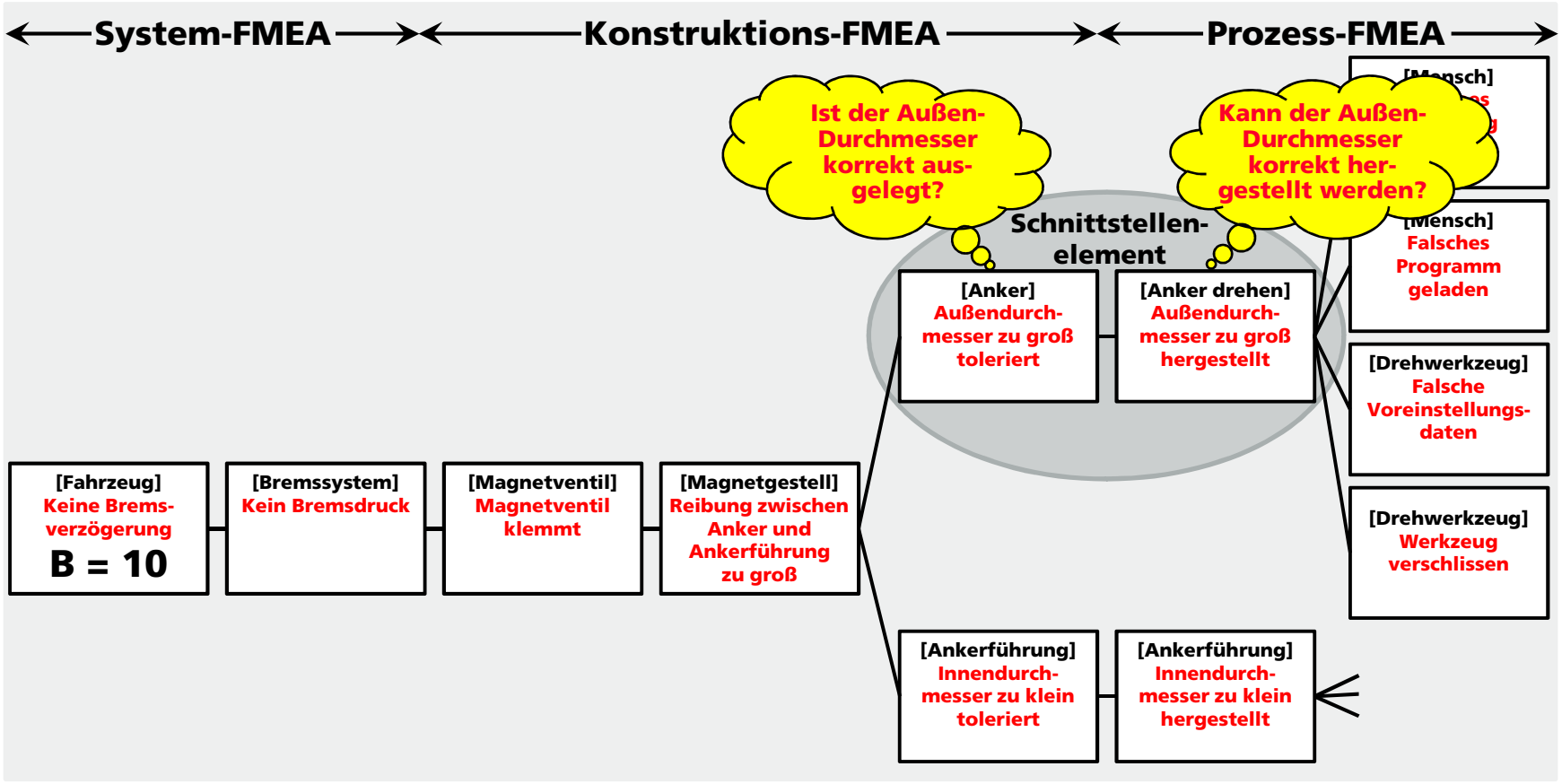
Systematische Ermittlung und durchgängige Betrachtung mittels Funktionsnetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

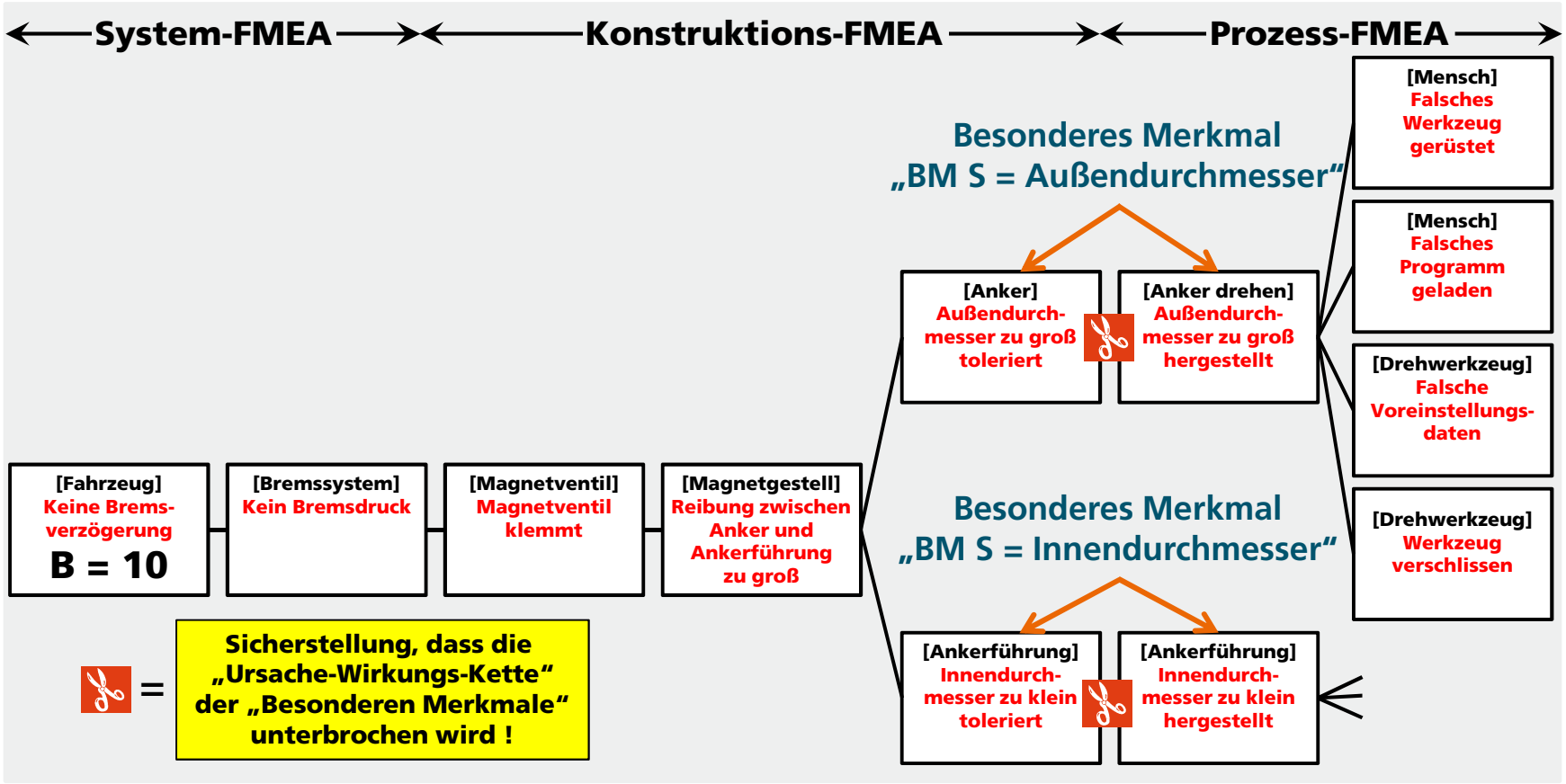
Systematische Ermittlung und durchgängige Betrachtung mittels Fehlernetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

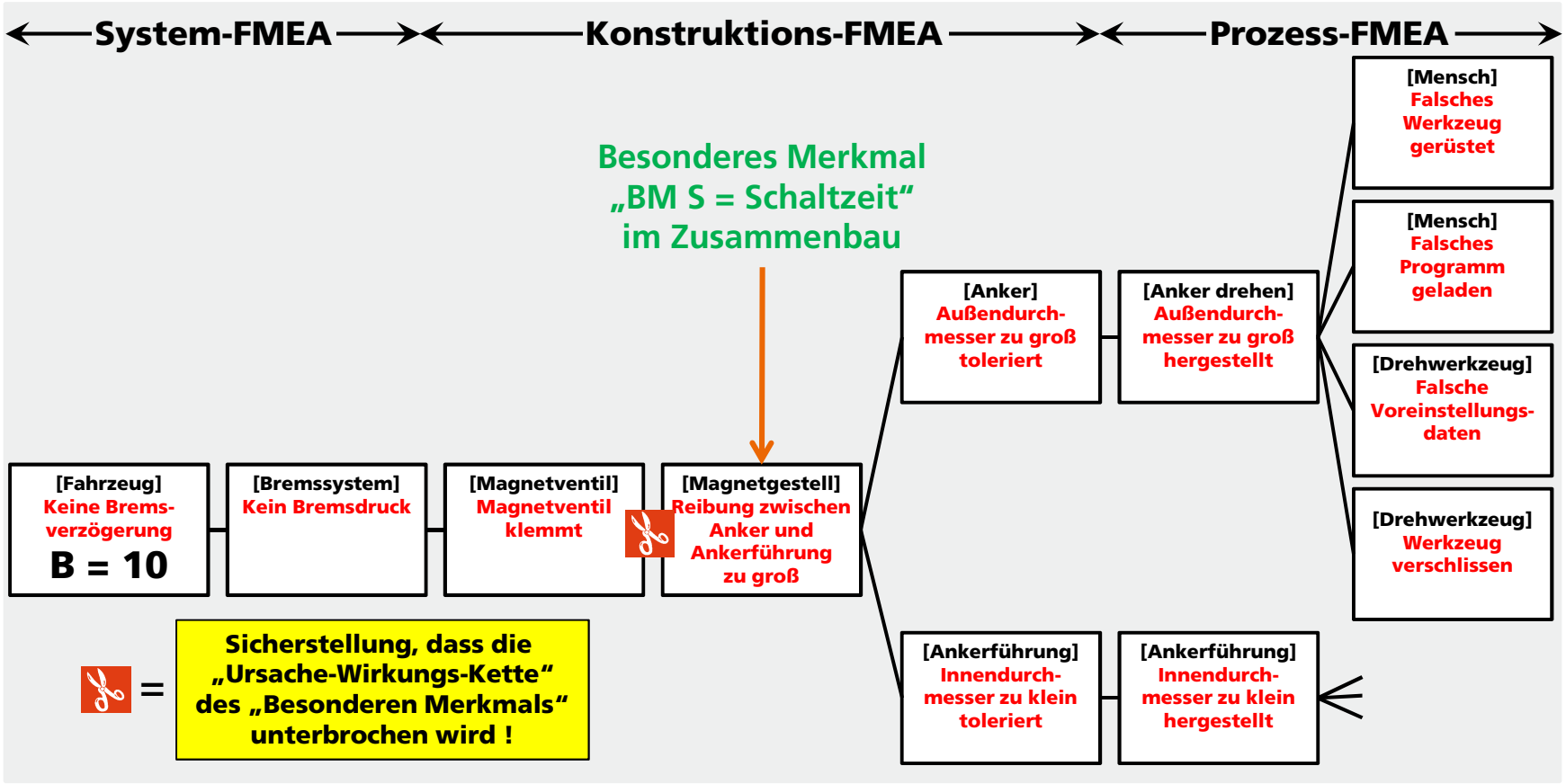
Systematische Ermittlung und durchgängige Betrachtung mittels Fehlernetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

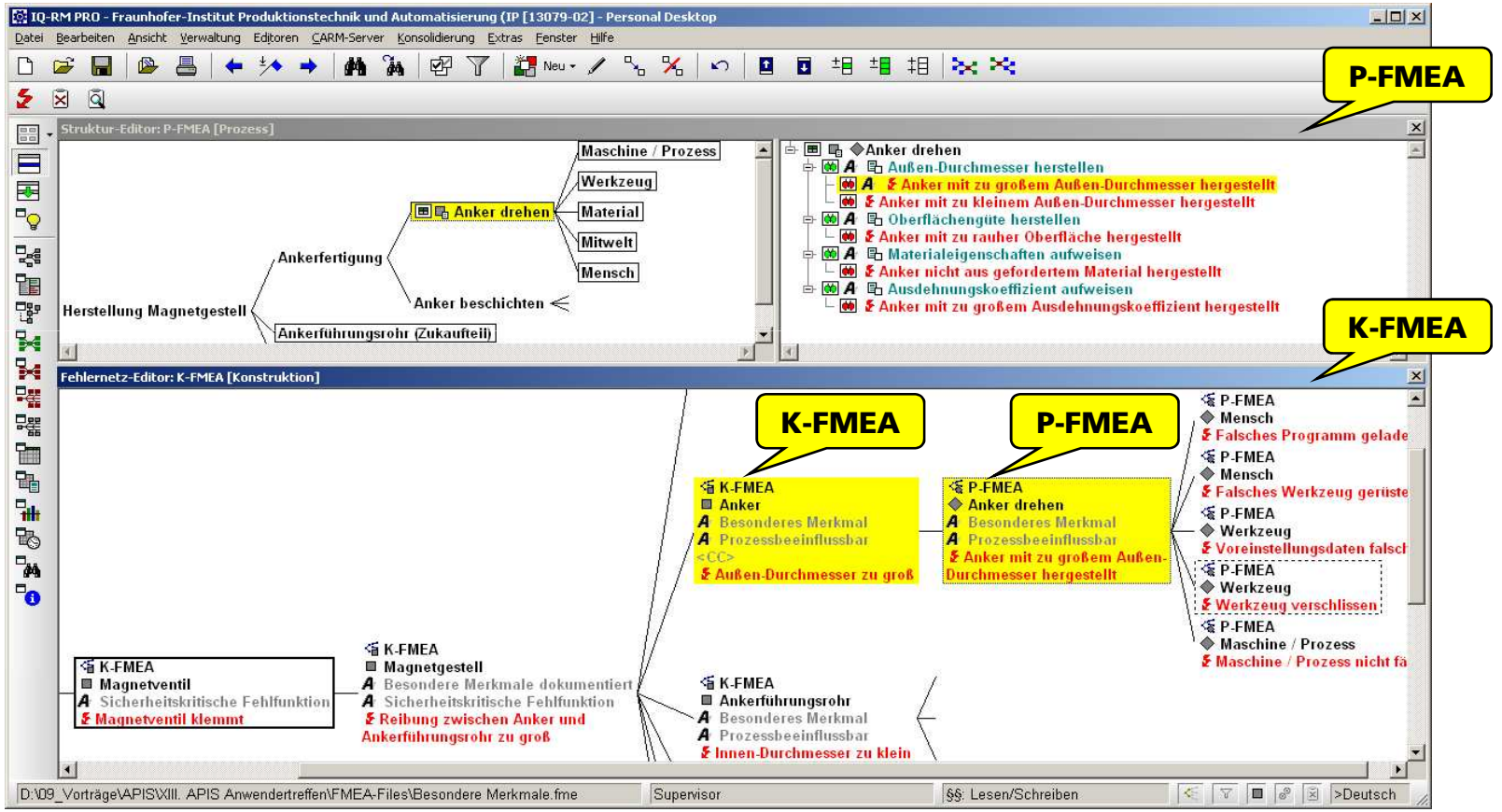
Systematische Ermittlung und durchgängige Betrachtung mittels Fehlernetz über die FMEA-Arten hinweg



Fraunhofer IPA

Koppelung von Konstruktions-FMEA und Prozess-FMEA

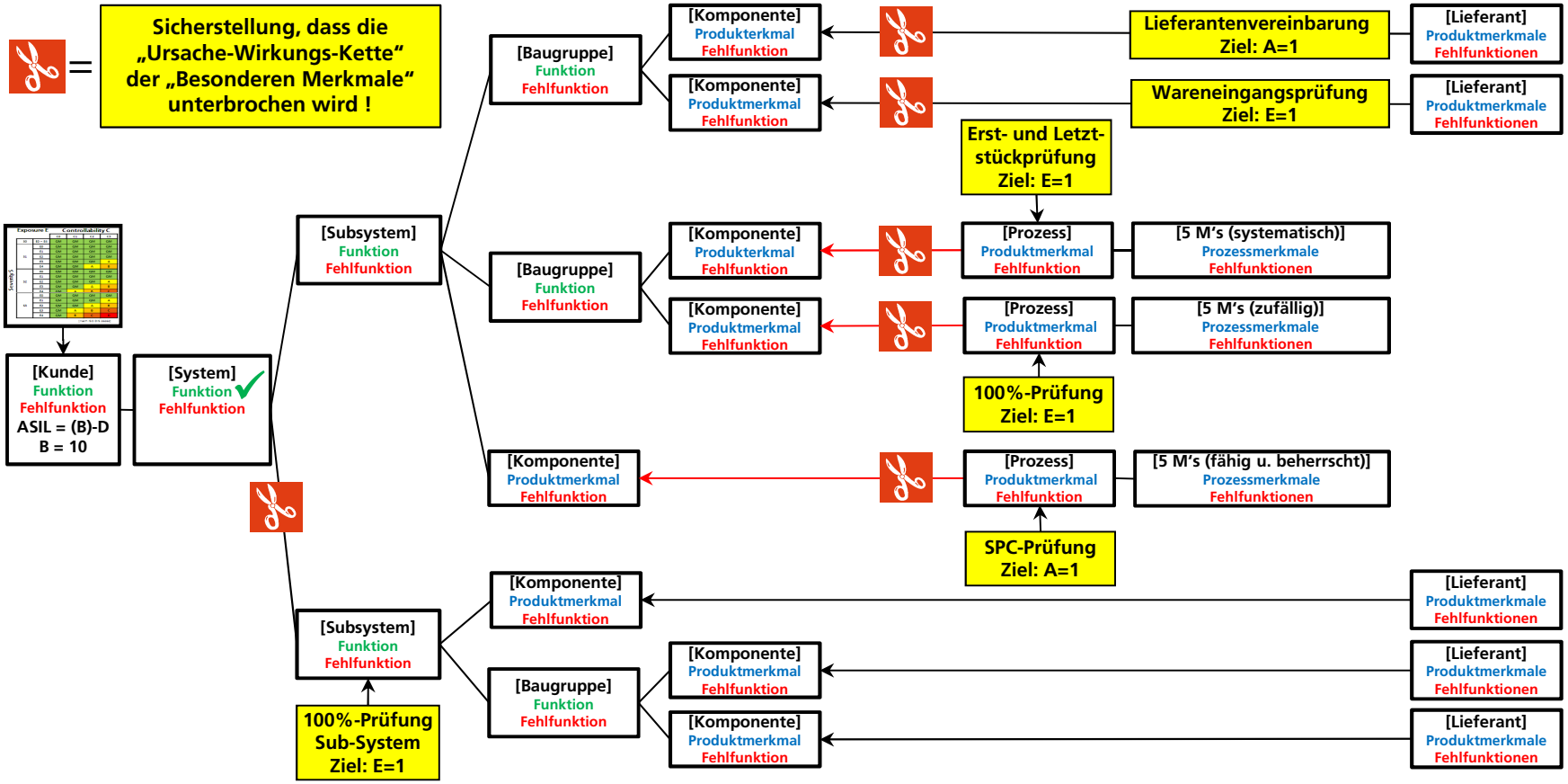
Durchgängige Betrachtung Besonderer Merkmale durch Verknüpfung von Fehlernetzen über die FMEA-Arten



Fraunhofer IPA

Besondere Merkmale

Vorgehensweise zur Analyse und Absicherung Besonderer Merkmale



Fraunhofer IPA

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/PE-Systeme
  - Besondere Merkmale untersucht mechanische Systeme
- Es lassen sich sowohl die Anforderungen der Funktionalen Sicherheit als auch die Anforderungen der Besonderen Merkmale in einer FMEA-Datei analysieren und absichern
- Der gemeinsame Nenner der Analysen ist die Gefährdungsanalyse und Risikoabschätzung sowie das Fehlernetz über die FMEA-Arten hinweg
- Die Bewertungsmaßstäbe und Maßnahmen sind entsprechend dem Fokus der Betrachtung zu wählen
- **Funktionale Sicherheit und Besondere Merkmale ergänzen sich auf dem Weg zum funktional sicheren System!**