DIA und die Schnittstelle zwischen OEM und Lieferant

1. Österreichische Fachkonferenz: ISO 26262 Funktionale Sicherheit
20. und 21 . Mai 2014, Wien

Dipl.-Ing. Stefan Gerstmayr

Functional Safety Engineer (TÜV Rheinland, Automotive)

Wissenschaftl. Mitarbeiter

Abteilung Nachhaltige Produktion und Qualität

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA

Telefon:	+49(0)711/9 70-1337
Fax:	+49(0)711/9 70-1002
E-Mail:	stefan.gerstmayr@ipa.fraunhofer.de
Internet:	www.ipa.fraunhofer.de

Fraunhofer IPA

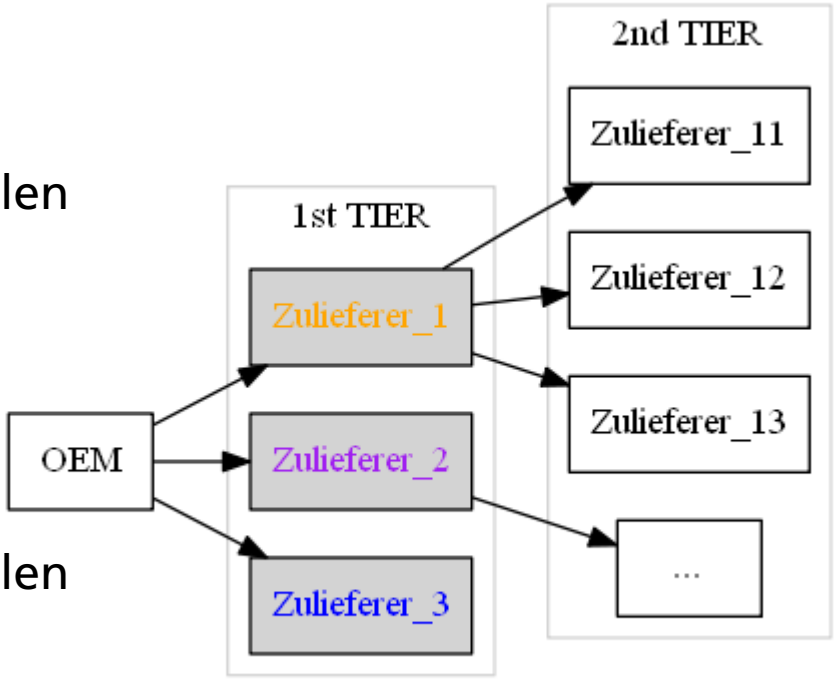
Verteilte Entwicklung nach ISO 26262
Vortragsinhalte

- Voraussetzungen für verteilte Entwicklung sicherheits-relevanter E/E-Systeme
- Management der Funktionalen Sicherheit bei verteilter Entwicklung
- Rolle der DIA in der verteilten Entwicklung
- Inhalte und Umfang der DIA
- Sinnvolle Teilung der Verantwortlichkeiten
- Umgang mit Safety Assessments

VORAUSSETZUNGEN VERTEILTER ENTWICKLUNG NACH ISO 26262

Verteilte Entwicklung nach ISO 26262
Kunde und Lieferanten-Strukturen

- Projekt A
  - 2 große TIER 1 beteiligt
  - OEM mit Eigenentwicklungsanteilen in mechanische HW
- Projekt B
  - Systemhersteller (Kein TIER 1)
  - OEM mit Eigenentwicklungsanteilen in SW an der Fzg-Schnittstelle
  - Elektronik-Lieferant
  - SW-Dienstleister



Lieferanten Verhältnisse Automobilindustrie

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

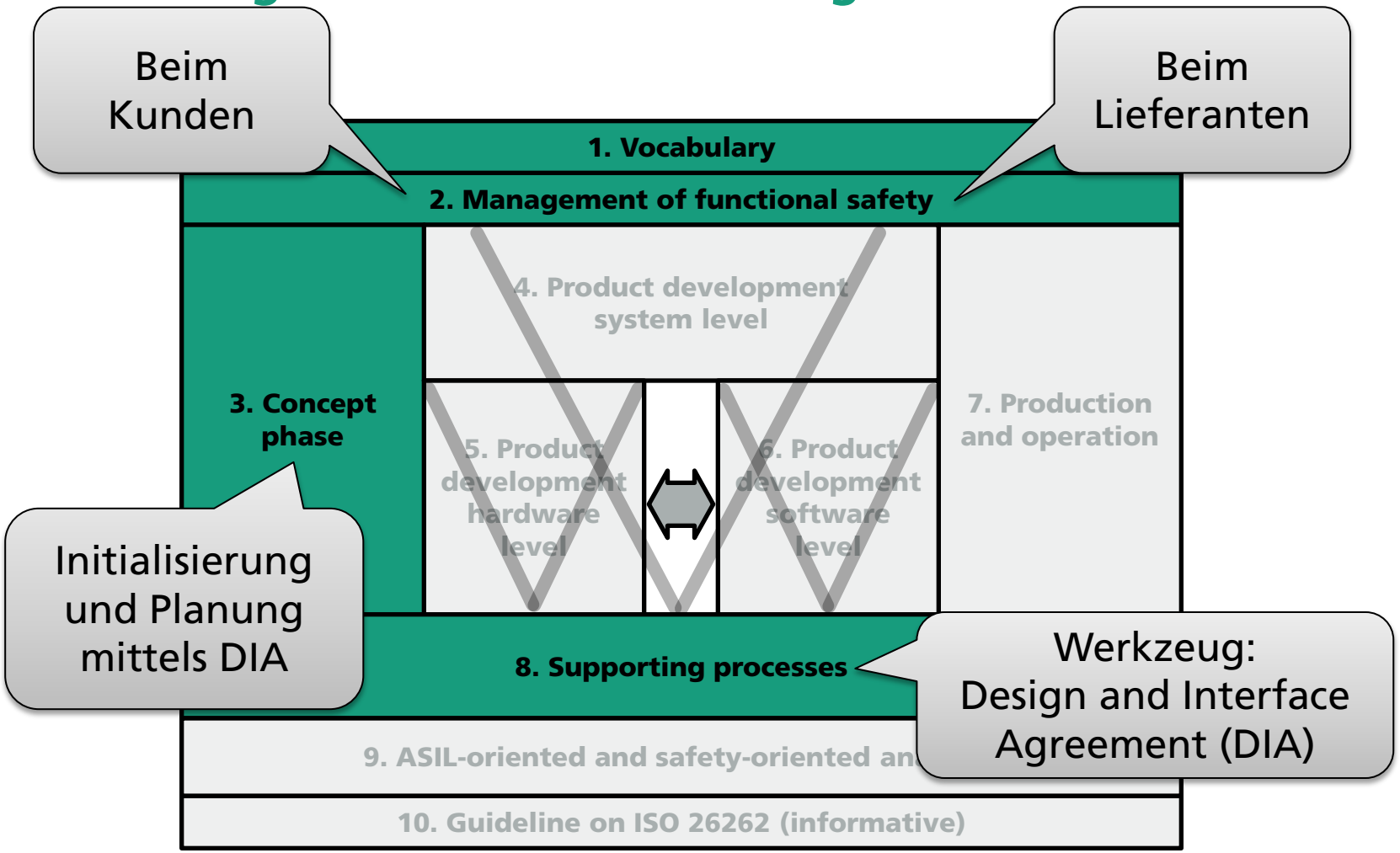
Kriterien der Zuliefererauswahl (8-5.4.2)

- Bewertung der Fähigkeit des Zulieferers Items und Elemente vergleichbarer Komplexität und nach ISO 26262 entwickeln zu können
  - Nachweis eines QM-Systems, Qualitäts- und Performance-Nachweis, Nachweis der Fähigkeit zur Funktionalen Sicherheit, Ergebnisse früher Safety Assessments nach ISO26262-2-6.4.9
- Beauftragung (RFQ) von Kunde an Zulieferer muss enthalten
  - „formal request to comply with ISO 26262"
  - Definition und funktionale Spezifikation des Items bzw. Elements
  - the safety goals, the functional safety requirements or the technical safety requirements, including their respective ASIL if already available, depending on what the supplier is quoting for.

ROLLE DER DIA BEI VERTEILTER ENTWICKLUNG NACH ISO26262

Verteilte Entwicklung nach ISO 26262

Abstimmung verteilter Entwicklung

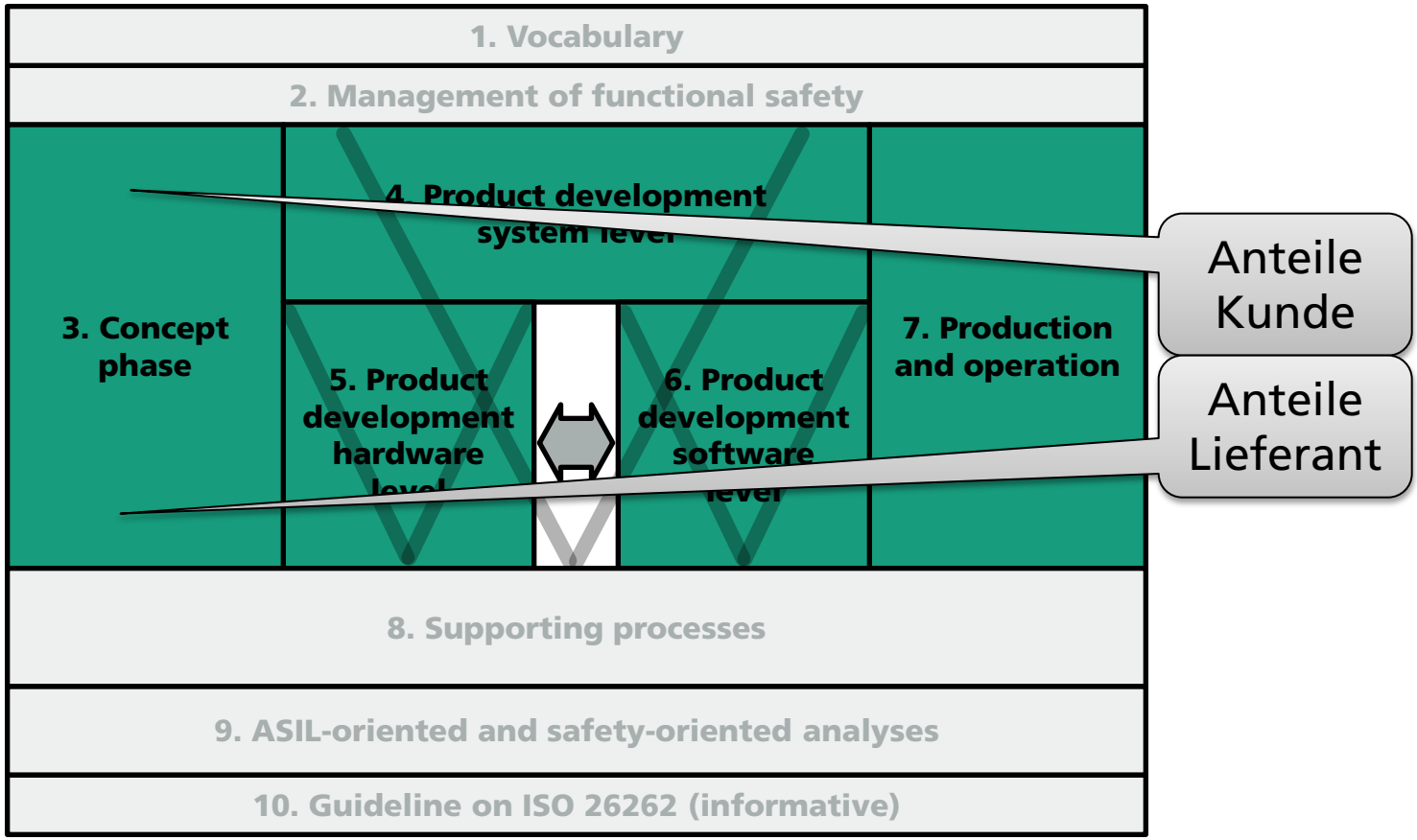


Quelle: ISO 26262

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Durchführung verteilter Entwicklung



Quelle: ISO 26262

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

Ziel des Abschnittes

- Vorgehensweise und Zuweisung der Verantwortlichkeiten bei verteilter Entwicklung von „Items“ und „Elementen“
- Abschnitt macht keine Gültigkeitseinschränkung für bestimmte ASILs

Anwendung der Anforderungen (8-5.4.1)

- gelten für **jedes Item und Element** mit Sicherheitsrelevanz (ASIL-Verknüpfung)
- gelten auf **jedem Level der Zuliefererbeziehungen**

INHALTE UND UMFANG DER DIA

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

Initialisierung und Planung verteilter Entwicklung (DIA) (8-5.4.3)

- Kunde und Zulieferer sollen eine DIA (Design and Interface Agreement) mit folgenden Inhalten erstellen:
  - Benennung beiderseitiger „Safety Manager“
  - Abstimmungen zum Sicherheitslebenszyklus (2-6.4.5)
  - vom Kunden durchzuführende Aktivitäten und Prozesse und vom Zulieferer durchzuführende Aktivitäten und Prozesse
  - Definition der auszutauschenden „Work products“ und Informationen
  - verantwortliche Abteilungen und/oder Personen für die Aktivitäten
  - Sicherheitszielvorgaben (ASILs, Metriken, etc.)
  - Beschreibung unterstützender Prozesse und Werkzeuge inkl. Schnittstellen zur Abstimmung zw. Kunde und Zulieferer

Verteilte Entwicklung nach ISO 26262

8-Annex B: DIA example

Customer: Item

Supplier: Hardware Component with ASIL C

ID	Activity	Data from customer to supplier	Data from supplier to customer
A.8	Select supplier 5.4.2	Proposed DIA (project-specific) 5.4.3	---
A.9		---	Selected project resources and their capability assessment, e.g. safety team members' skills, competencies and qualification (ISO 26262-2:2011, 5.5.2); Organization-specific rules and processes (ISO 26262-2:2011, 5.5.1), incl. tools, libraries; Preliminary plans, e.g.
A.10		Iterative evaluation and enquiries, e.g. regarding skill gaps	Iterative revisions addressing customer concerns
A.11		Acceptance of DIA. (5.5.2) Selection report (5.5.1)	Acceptance of DIA (5.5.2)

Verteilte Entwicklung nach ISO 26262

8-Annex B: DIA example

ID	Activity	Data from customer to supplier	Data from supplier to customer
B.1	• Initiate project • Create functional safety concept	• System level plans • Item definition and its lifecycle • Functional safety concept	---
B.2	---	---	• Customer Project plan (5.5.3) • Customer Safety plan (5.5.4) • Customer H&R analysis (5.4.3.2), • hardware component behaviour models, incl. fault metrics • …
B.3	---	Acceptance	---
…	…	…	…
B.7	System development lifecycle	• Technical safety concept • relevant parts of system design specs, hardware specs, design & implementation (D&I) constraints, • hardware-software Interface (HSI) specifications	• Iterative evaluation, clarification-queries, and feedback about conflicts, completeness, consistency, etc.; • technological limitations, if any; change requests, if any (5.4.4). • Updated behaviour models, incl. fault models.

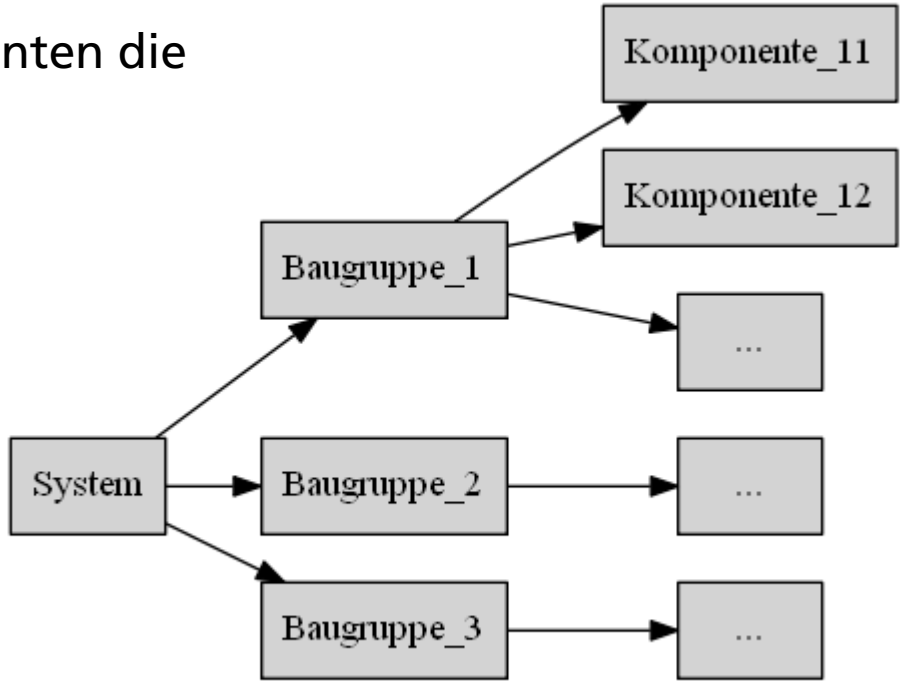
SINNVOLLE TEILUNG DER VERANTWORTLICHKEITEN

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Stücklistenkomplexität von E/E-Systemen mit sicherheitsrelevanter Funktion

- Bis zu den Einzelteilen (Zwang durch ISO26262) gedacht …
  - lassen elektronische Komponenten die Stücklisten extrem wachsen.
- Zusammensetzung E/E-Systeme
  - ggf. mehrere Steuergeräte
  - mehrere Sensoren und Aktuatoren (ggf. mit enthaltener Intelligenz und Platinen)
  - Verkabelung und Steck-verbindungen
  - Anbindung an mechanische, hydraulische oder pneumatische Systeme

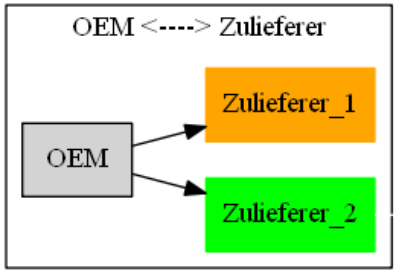


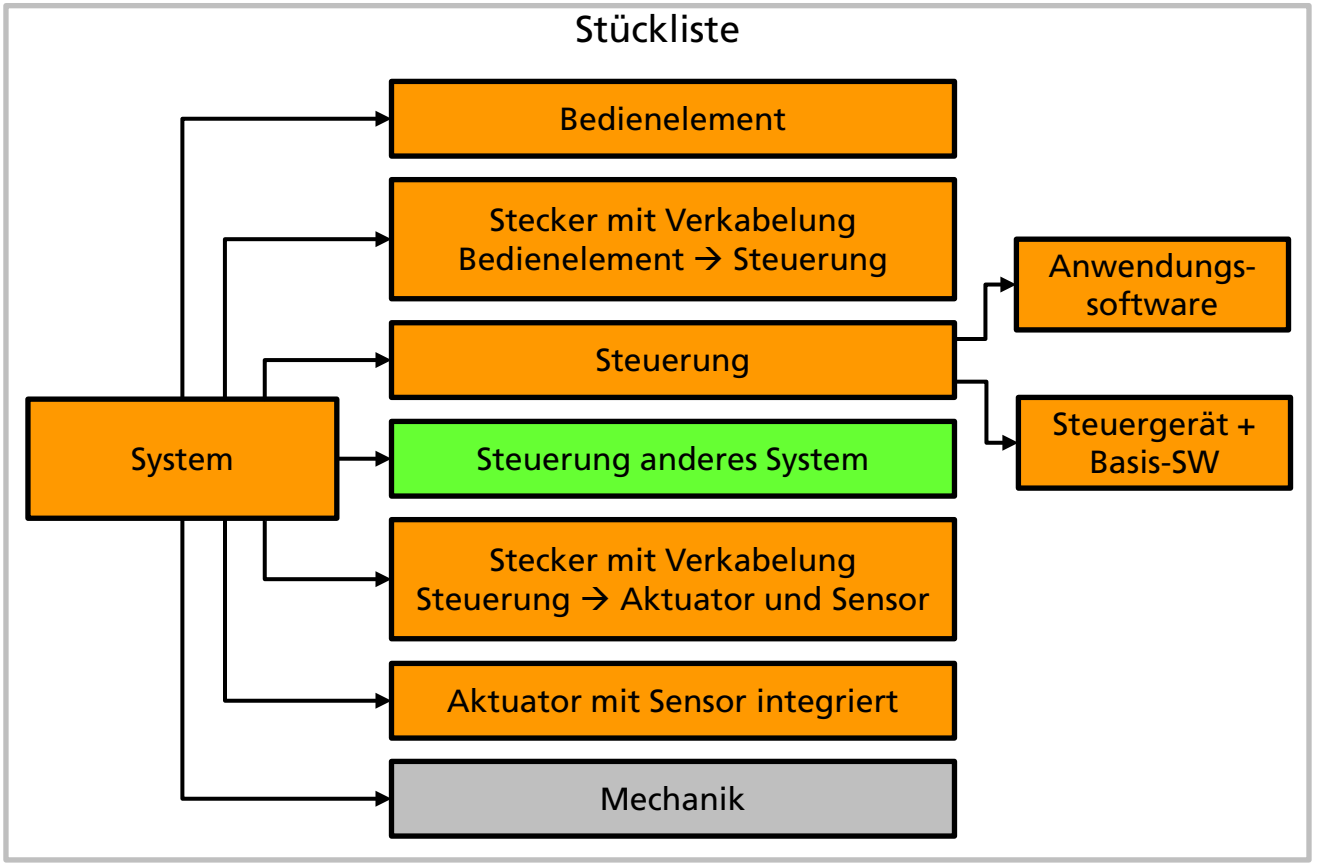
Stücklistenansatz

Verteilte Entwicklung nach ISO 26262

Verantwortungsteilung entlang Stückliste

Projekt A (frühere Systemgeneration)



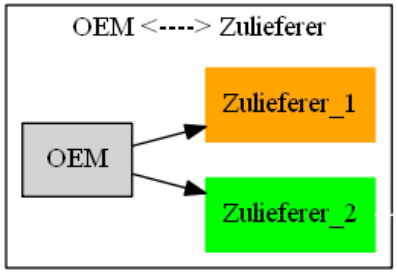


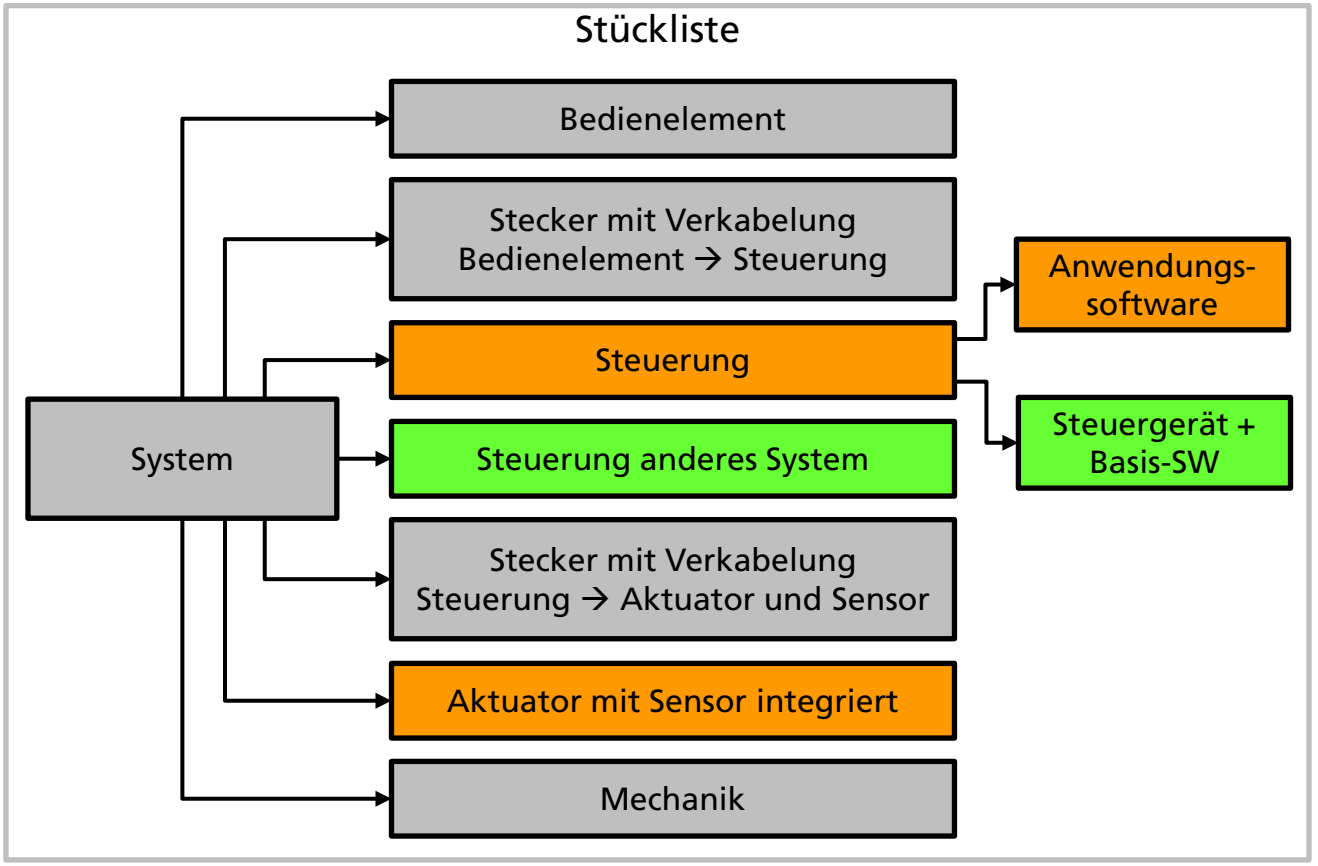
Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Verantwortungsteilung entlang Stückliste

Projekt A (jetzige Entwicklung)



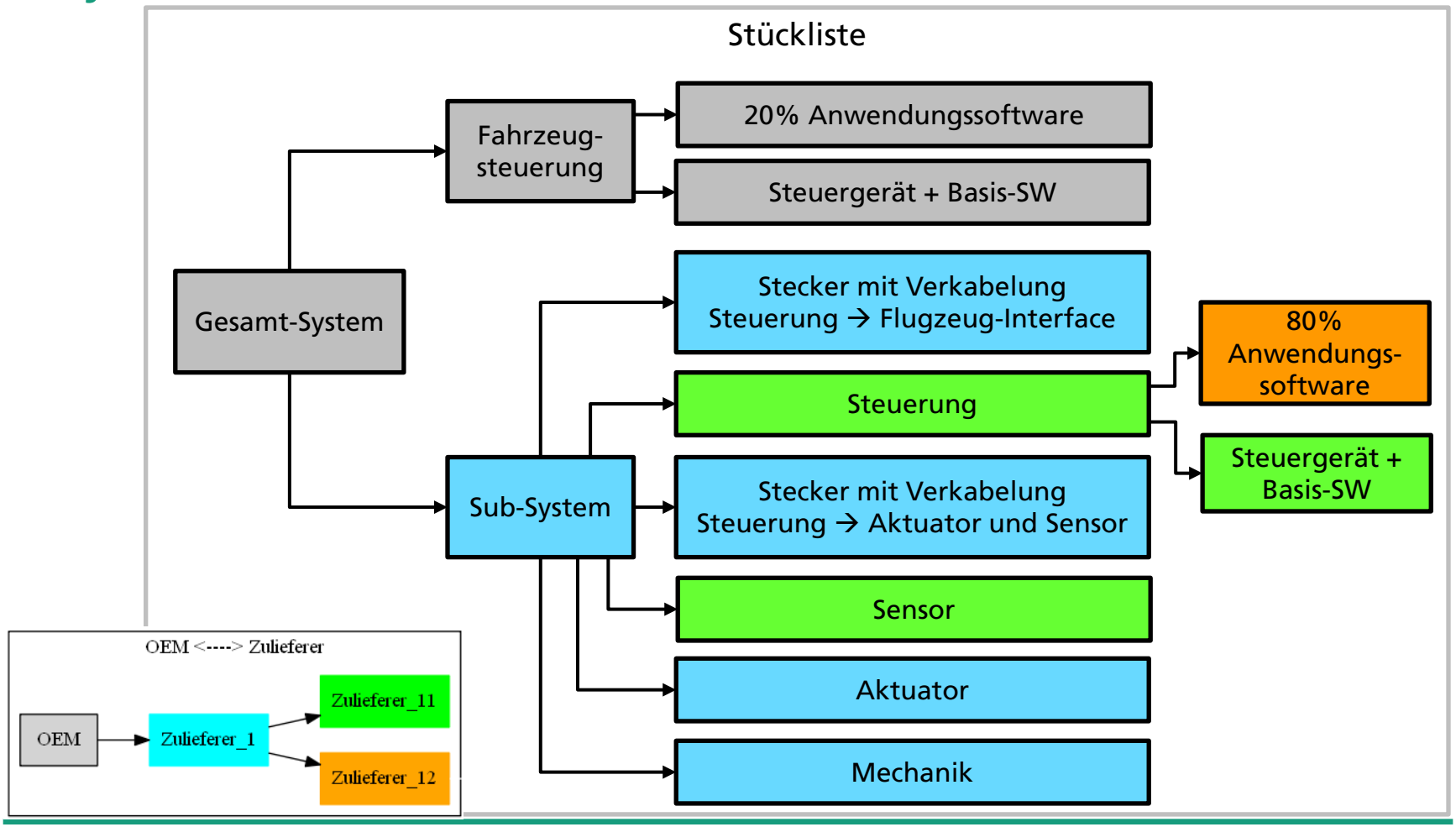


Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Verantwortungsteilung entlang Stückliste

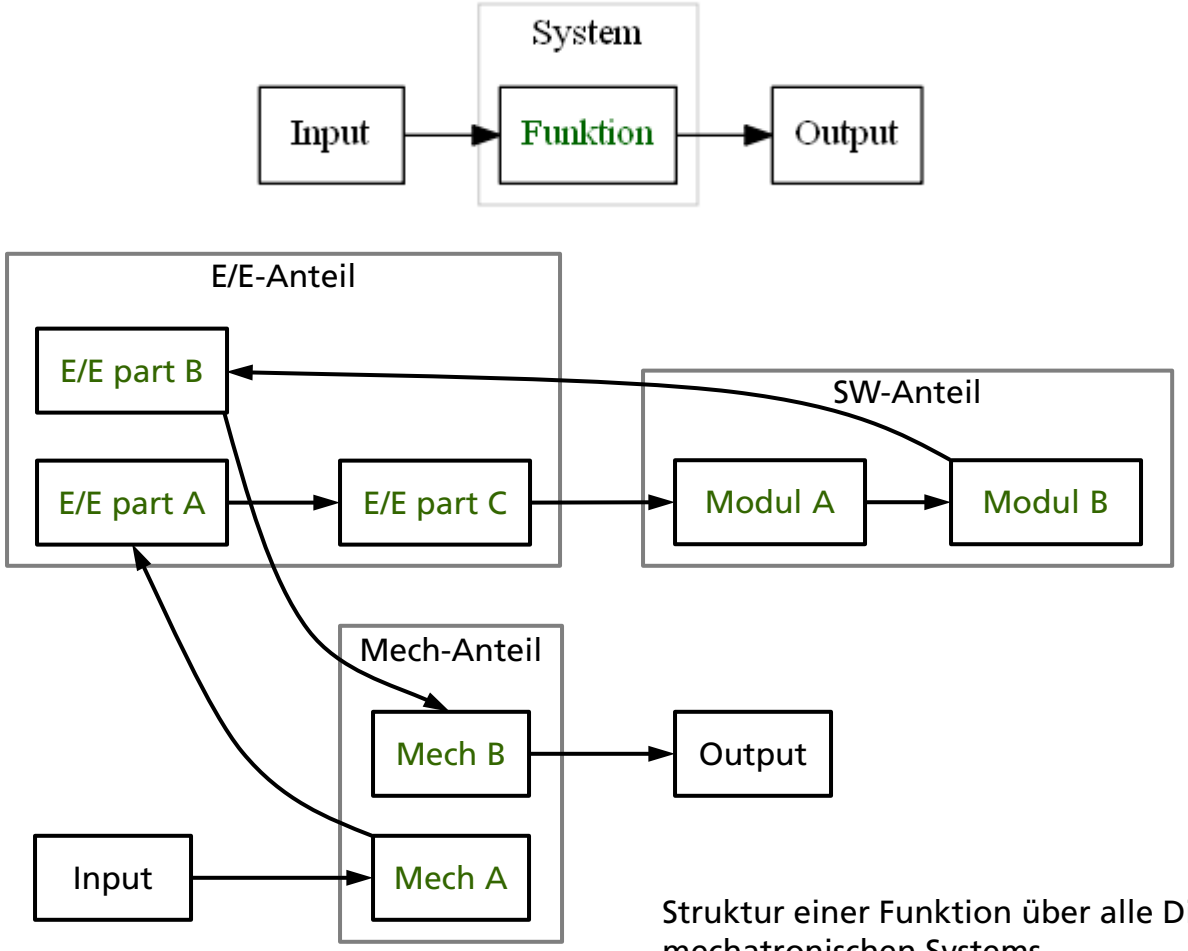
Projekt B (Innovatives Produkt)



Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Funktionsstrukturen innerhalb des mechatronischen Systems

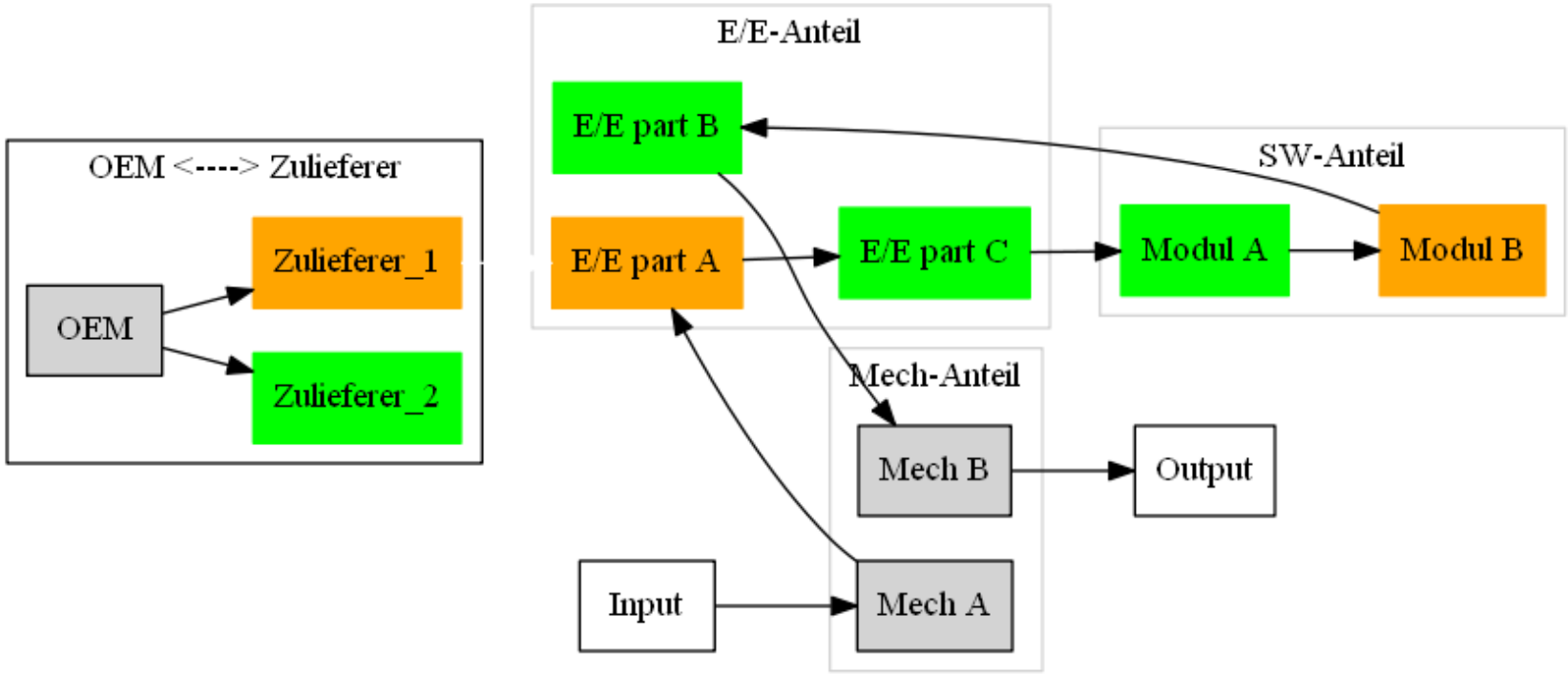


Struktur einer Funktion über alle Disziplinen eines mechatronischen Systems

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Verantwortungsteilung entlang Funktionsstruktur



Struktur einer Funktion über alle Dispziplinen eines mechatronischen Systems

Fraunhofer IPA

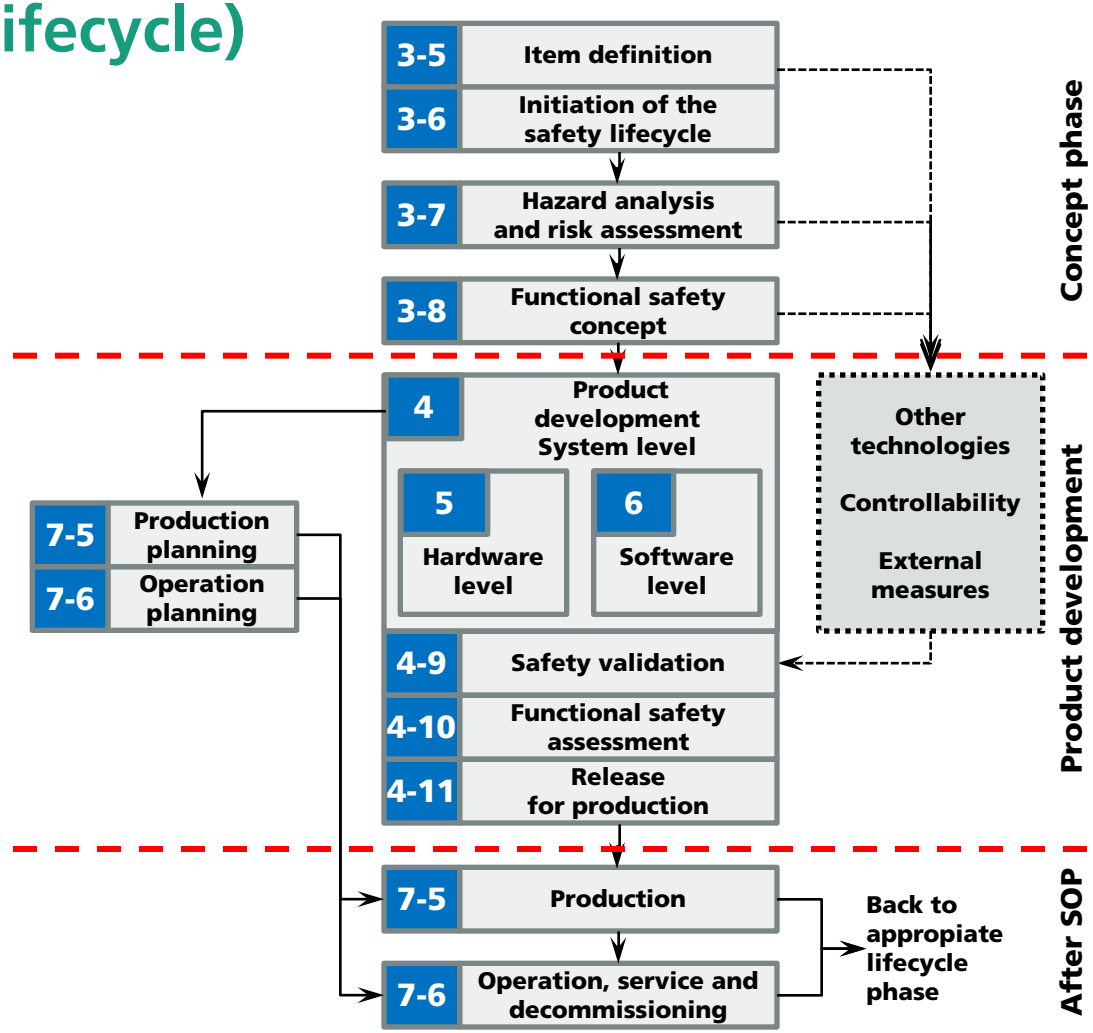
Verteilte Entwicklung nach ISO 26262

DIA-Inhalte zu Stückliste- und Funktions-Abstimmung

System / Komponente / Funktionsblock	Funktion / Anforderung	Proven in Use?	Kunde	Lieferant
Item	---	Nein	Resp. A.1	---
Item	Funktion 1	Ja	---	Resp. L.1
Item	Funktion 2	Nein	Resp. A.2	…
…	…	…	…	…
Komponente 1	---	Ja	---	Resp. L.2

Verteilte Entwicklung nach ISO 26262

Verantwortungsteilung entlang Sicherheits-Lebenszyklus (safety lifecycle)

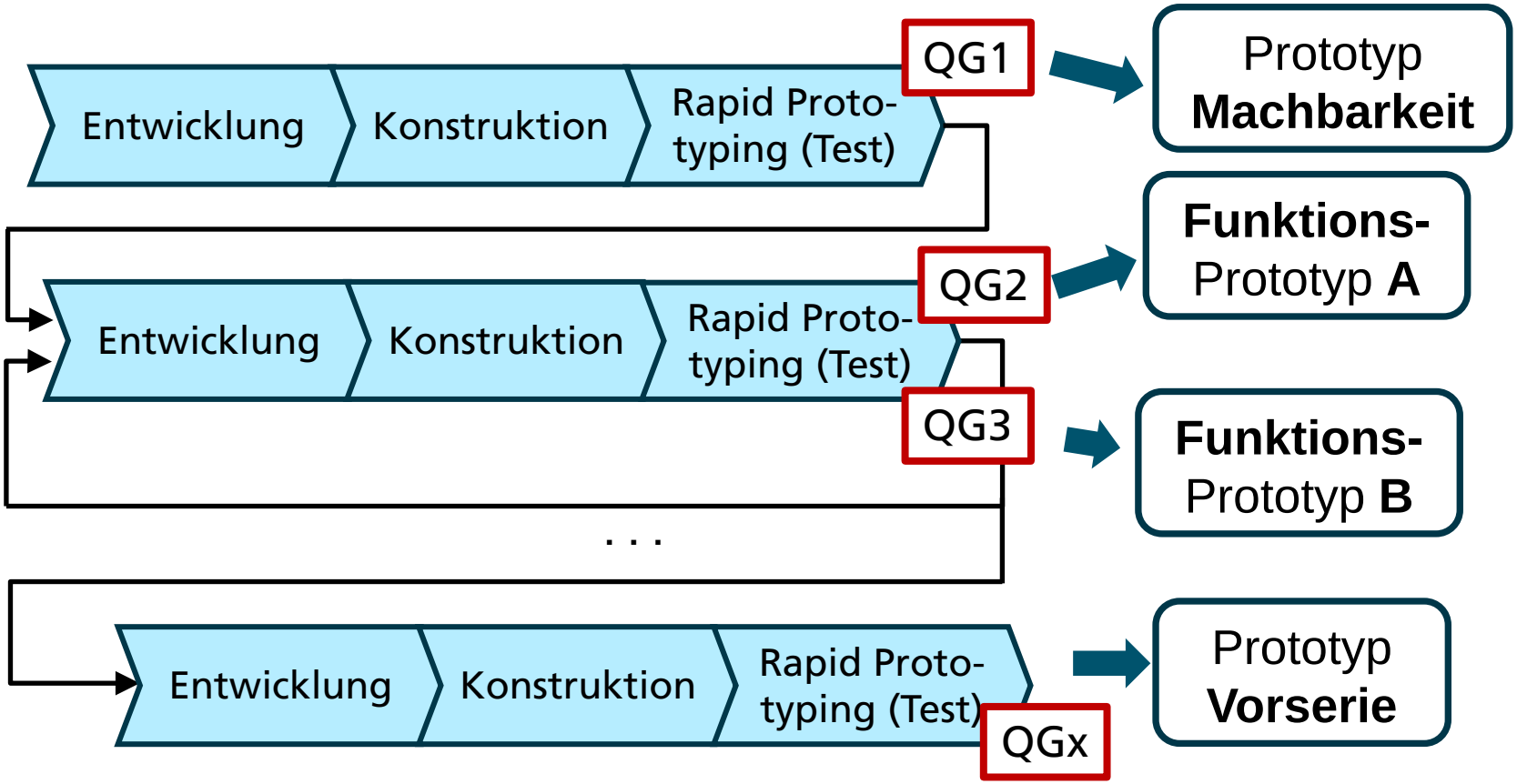


Quelle: ISO 26262-2

Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

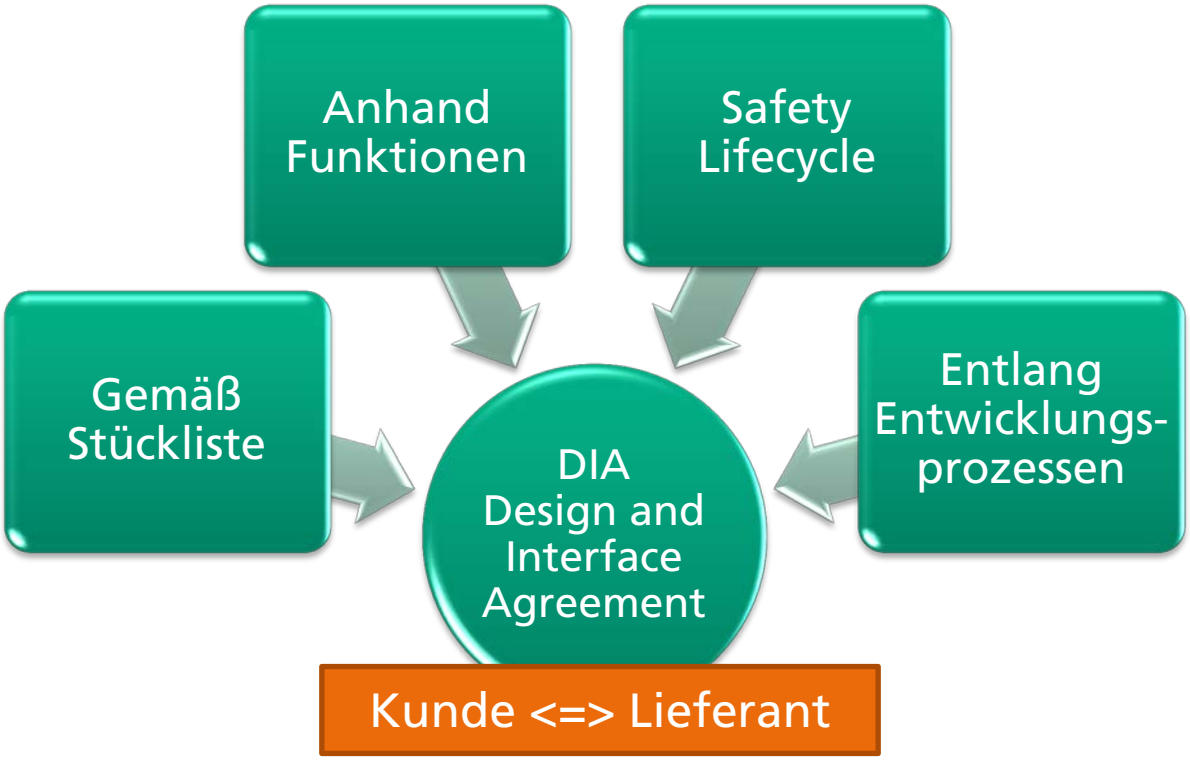
Verantwortungsteilung entlang Entwicklungsphasen



Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262

Sinnvolle Teilung der Verantwortlichkeiten



Fraunhofer IPA

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

Durchführung verteilter Entwicklung (8-5.4.4)

- Anforderungen zum gegenseitigen Berichtswesen bzw. zum Informationsaustausch
- Umgang mit Änderungen
- Verantwortlicher zur Durchführung der „Safety Validation“ (Durchführung im Fahrzeug) ist festzulegen => DIA

UMGANG MIT SAFETY ASSESSMENTS

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

Initialisierung und Planung verteilter Entwicklung (DIA) (8-5.4.3)

Zusätzliche Bedingungen:

- Erstellt der Zulieferer die „Gefahrenanalyse und Risikobewertung“, muss diese dem Kunden zur „Verification“ vorgelegt werden.
- Das „Functional Safety Concept“ soll von demjenigen Partner erstellt werden, der für die Entwicklung des „Item“ verantwortlich ist.
- Dem „Functional Safety Concept“ sollen beide Kunde und Zulieferer zustimmen.

Verteilte Entwicklung nach ISO 26262
8-5 Interfaces within distributed developments

Functional Safety Assessment (8-5.4.5)

- Assessment beim Zulieferer
  - Bewertung des Items bzw. Elements auf Einhaltung der Funktionalen Sicherheit
- Für ASIL C,D durch den Kunden

After release for production (8-5.4.6)

- Notwendige Abstimmungen sollen dokumentiert werden.
  Empfehlung: innerhalb der DIA bei Abstimmung zum Safety Lifecycle

FAZIT

Verteilte Entwicklung nach ISO 26262
Fazit

Ohne Abstimmung einer DIA

- System-Komplexität und Zuliefererverhältnisse erzeugen vielfältige Schnittstellen: funktional und organisatorisch
- Tätigkeiten der Funktionalen Sicherheit somit ungeplant nur äußerst schwer beherrschbar

Gut koordinierte verteilte Entwicklung kann

- Aufwände reduzieren
  - Durchführung einer ISO-Aktivität bei mehreren Partnern verhindern
- Qualität erhöhen
  - Erfüllung der Anforderungen der ISO26262 wird durch dokumentierte Abstimmungen vereinfacht. Notwendigen Reviews und Assessments an Zuliefererschnittstellen prüfen Konformität und Qualität