Sicherheitsrelevante eingebettete Systeme

Spezifikation projektspezifischer Software

Nov. 2018

Entwicklung gemäß EN 61508, EN 50128 (Bahn) etc.

- _Voraussetzung für Begutachtung bzw. Zulassung
  - __Sicherheitsbetrachtungen vorausgesetzt
- _Anforderungen an Entwicklungsprozess
  - __Fehler vermeiden, erkennen, beherrschen

Akzeptanz

_durchwachsen ...

Methodik

_Anforderungen spezifizieren
_Konfiguration referenzieren
_einfach, effizient, flexibel
_bis SIL4

Nov. 2018

Im Tagungsband

_Erläuterung des Modells
__Definitionen
__Anforderungen
__Architektur
_Evaluation von Methoden
__Fragenkatalog
__Referenzmodell

Nov. 2018

Im Vortrag

_Erläuterung der Methodik

Prämissen

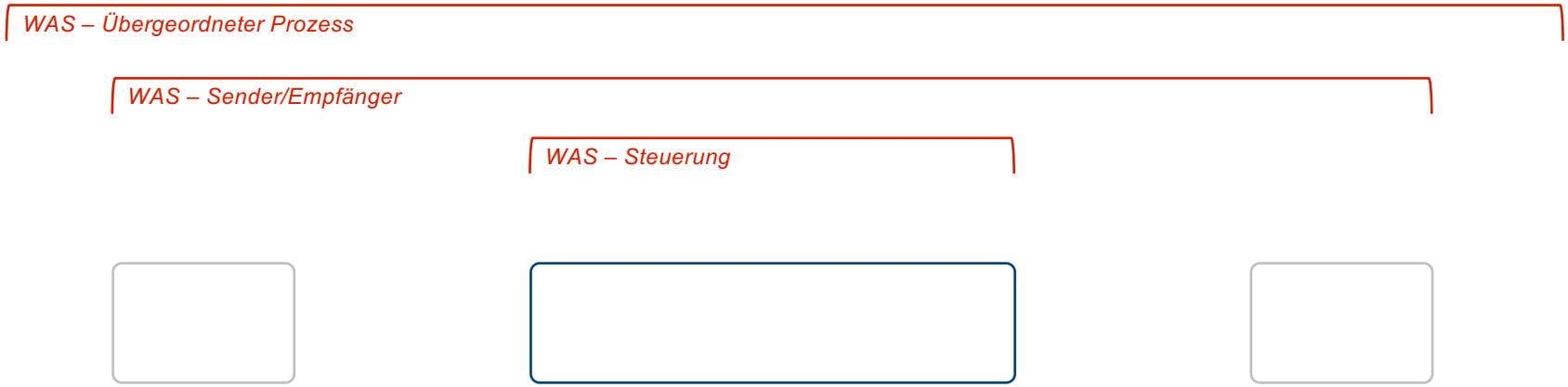
_Entwurf und Methoden möglichst einfach
_Konfigurierbare Hardware und Basis-Software
__Erfüllen bereits wesentliche Sicherheitsanforderungen
__Zyklischer Aufruf projektspezifischer Software

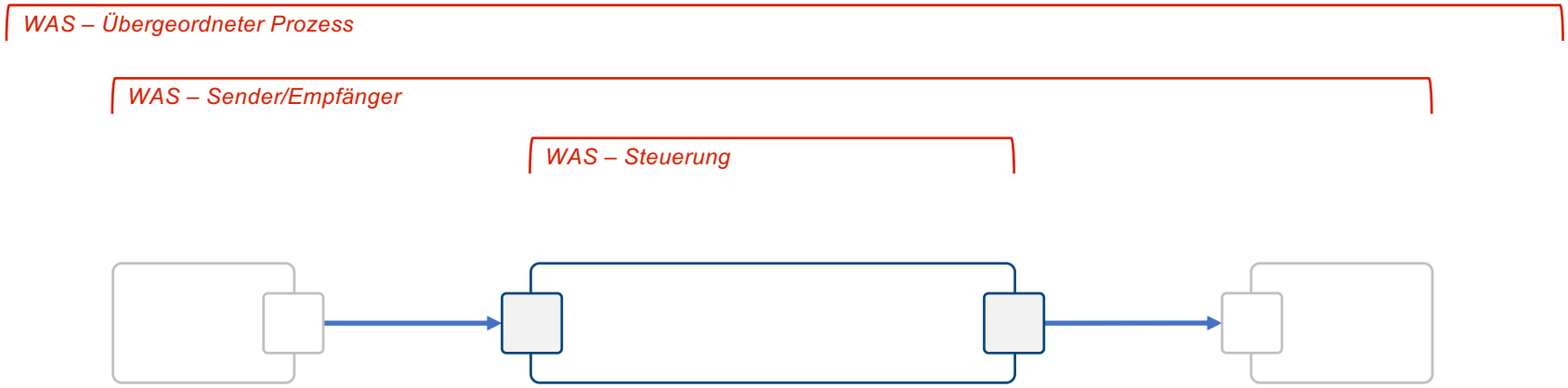
Prinzipien

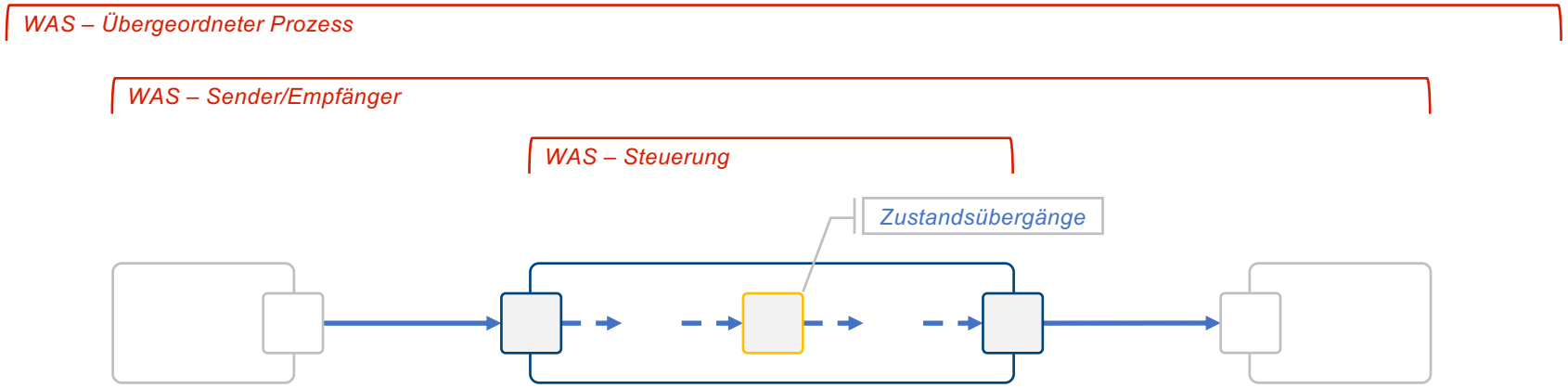
_Systemabgrenzung: Steuerung
_Signale ←→ Variable ←→ IST-/SOLL-Zustände
_Zustandsübergänge explizit spezifizieren

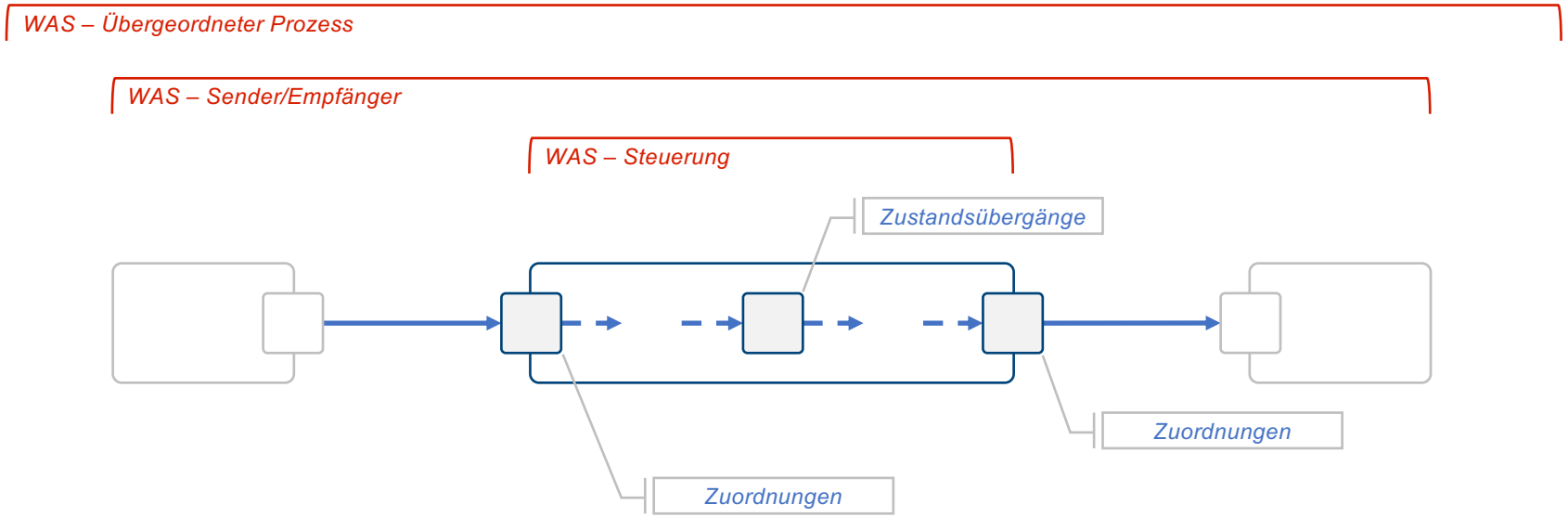
Steuerung

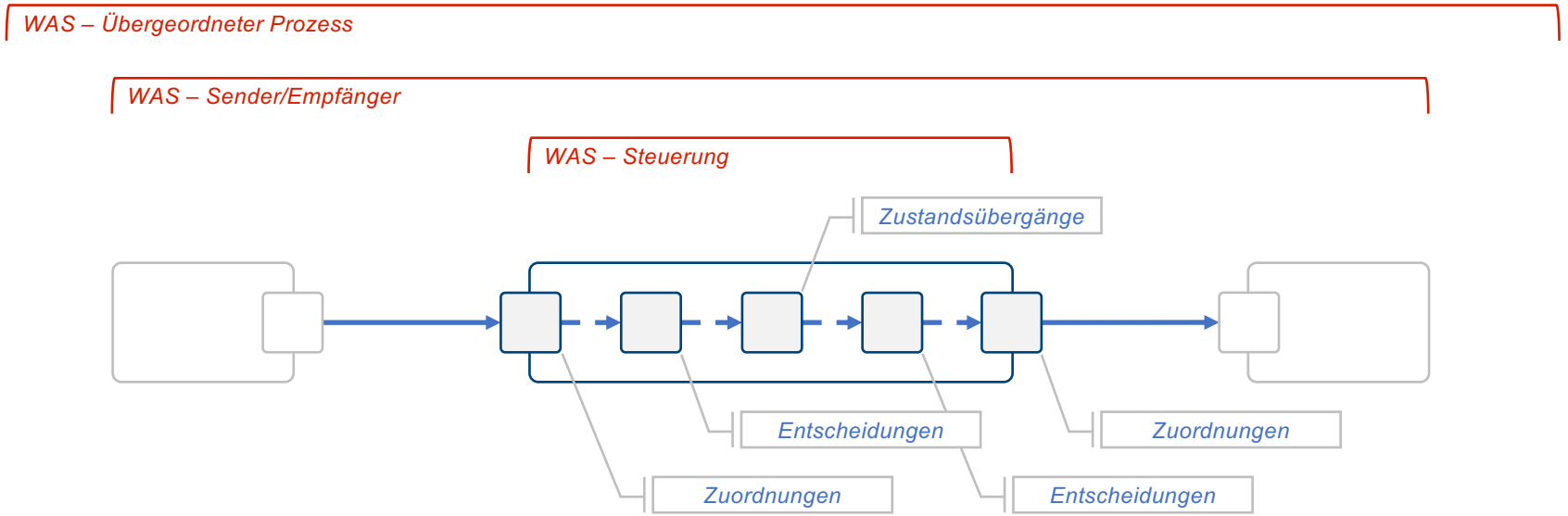
_Eingang: Benutzerschnittstelle oder übergeordnete Steuerung
_Ausgang: Parameter für Regler











Definitionen

_Schnittstellen
_Externe Kontroller
_Signale
_Betriebsarten/-Zustände
_Funktionen

Spezifikation der Anforderungen

_Allgemeines Schema
_Zuordnungstabellen
_Entscheidungstabellen
_Zustandsübergangstabellen

Nov. 2018

ID	Betriebsart	Funktion	Kategorie	Sicherheit
RQ#001	OM#Regular	AF#RecData	RC#FN	SIL2
Erläuterung				
Eingangssignale des externen Kontrollers (AE) wurden müssen in einem Status (AE_Input_Status) zusammen				
Beschreibung				
IF (AE_Restricted_valid == TRUE AND AE_Valid_valid == **THEN {** AE_Input_Status ← VALID **} ELSE {** AE_Input_St				
Eingangsvektor	{AE_Restricted_valid; AE_Valid_valid}			
Ausgangsvektor	AE_Input_Status			

Ausgangsvektor (Variable): e.dest	Eingangsvektor (Signal): e.src	Sicherheit
Bedienterminal des Fahrzeugs (en: Operating Terminal)		
X_Force_restricted	THIS.OT.FORCE_*	**SIL4**
X_Force_valid	THIS.OT.FORCE_*	**SIL4**
X_Max_valid	THIS.OT.MAX	SIL2
X_None_valid	THIS.OT.NONE	SIL2
X_Raise_valid	THIS.OT.RAISE	SIL2
X_Release_valid	THIS.OT.RELEASE	SIL2
X_Restricted_valid	THIS.OT.LIMITED	SIL2
X_Set_valid	THIS.OT.SET	SIL2
X_Stop_valid	THIS.OT.STOP	SIL2
X_Valid_valid	THIS.OT.VALID	SIL2
Geschwindigkeits-Kontroller (en: Speed Detection)		
SD_Restricted_valid	THIS.SD.LIMITED	SIL2
V_Detected_valid	THIS.SD.V_DETECTED	SIL2
SD_Valid_valid	THIS.SD.VALID	SIL2
Elektrodynamischer Antrieb (en: Traction Controller)		
FM_Detected_valid	THIS.TC.ACTUAL	SIL2
TC_Valid_valid	THIS.TC.VALID	SIL2

Ausgangsvektor	Eingangsvektor				
X_Input_Status	X_Restricted_valid	X_Valid_valid	X_Force_restricted	X_Force_valid	X_Raise_valid
Ergebnisvektor: e.res	**Vergleichsvektor: e.cmp**				
VALID	T	T	T	T	T
LIMITED	*	T	F	T	*
LIMITED	*	T	T	F	T
LIMITED	T	*	F	T	*
LIMITED	T	*	T	F	T
Ersatzwert					
CORRUPT					

Ausgangsvektor		Eingangsvektor								---
OperationMode	OperationState	X_Force	X_Max	X_None	X_Raise	X_Release	X_Set	X_Stop	Is_Stop	
Ergebnisvektor: e.res[]		**Vergleichsvektor: e.cmp**								**Sicherheit**
OM#Regular	OS#FORCE	T	*	*	*	*	*	*	*	**SIL4**
OM#Regular	OS#MAX	F	T	*	T	*	*	*	*	SIL2
OM#Regular	OS#MAX	F	T	*	F	*	*	*	*	SIL2
OM#Regular	OS#NONE	F	F	T	F	*	0	*	F	SIL2
OM#Limited	OS#NONE	F	F	T	F	*	#	*	F	SIL2
OM#Regular	OS#NONE	F	F	T	T	*	0	*	F	SIL2
OM#Regular	OS#RAISE	F	F	T	T	*	#	*	F	SIL2
OM#Regular	OS#NONE	F	F	F	F	*	0	*	F	SIL2
OM#Regular	OS#RAISE	F	F	F	F	*	#	*	F	SIL2
OM#Limited	OS#DEFAULT	F	F	F	T	*	0	*	F	SIL2
OM#Regular	OS#RAISE	F	F	F	T	*	#	*	F	SIL2

Zustandsübergänge

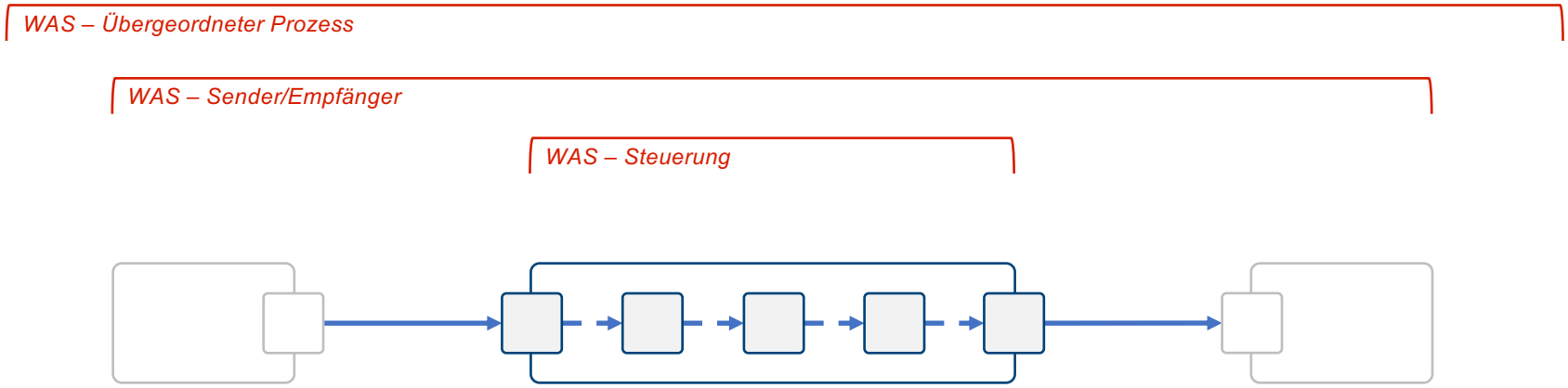
_funktional kritisch (korrekt oder robust)
_korrekt oder robust
_fehlerhaft

Referenzen zur Architektur

_Komponenten
_Verteilung (SW/HW)
_Datenfluss
_Kontrollfluss

Übergeordnete Anforderungen

_Signale ←→ IST-/SOLL-Zustände



Potential

_Referenz für Evaluation (Methoden, Prozesse oder Systeme)
_Generieren von Beschreibungen oder Prototypen
_Formale Analysen

Jens Lehmann, Dipl.-Ing./M.Sc.

OntoTec GmbH

Birkenleiten 41, 81543 München
www.ontotec.com

Nov. 2018