Wankkompensation FLEXX Tronic WAKO™

Elektronik & Sicherheitsnachweis nach EN 50126

Anlass	41. Tagung “Moderne Schienenfahrzeuge” Graz 2013
Redner	Richard Schneider
Titel	Vice President R&D
Datum	8. April 2013

BOMBARDIER
the evolution of mobility

Safety Case

Electronics

Wankkompensation FLEXX Tronic WAKO™

Elektronik & Sicherheitsnachweis nach EN 50126

Richard Schneider
Georg Edlbacher
Marc Breemeersch

BOMBARDIER
the evolution of mobility

Inhalt

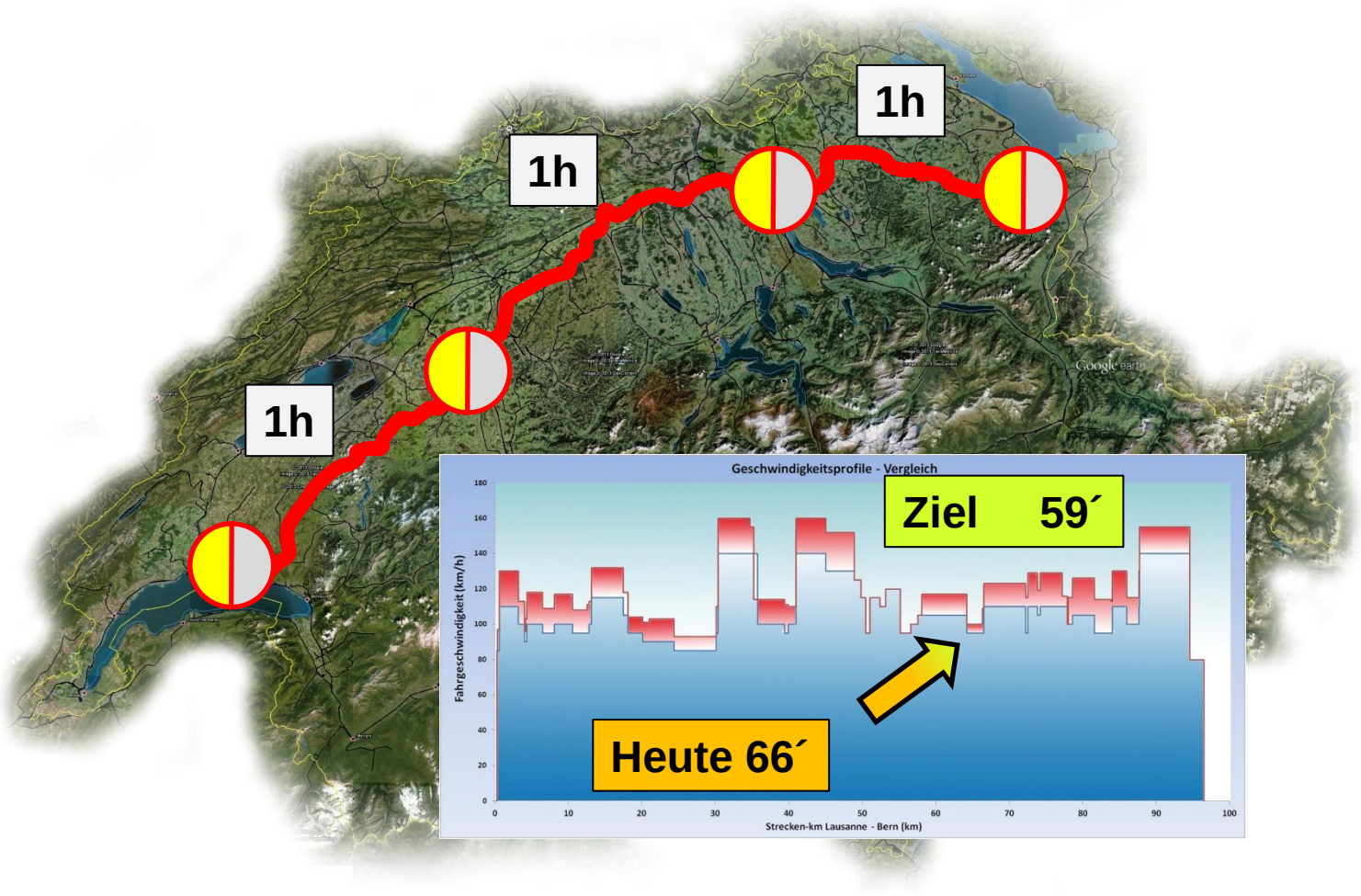
Die Schweiz rückt zusammen

BOMBARDIER
the evolution of mobility

Gesetz “ZEBG” seit September 2009 in Kraft

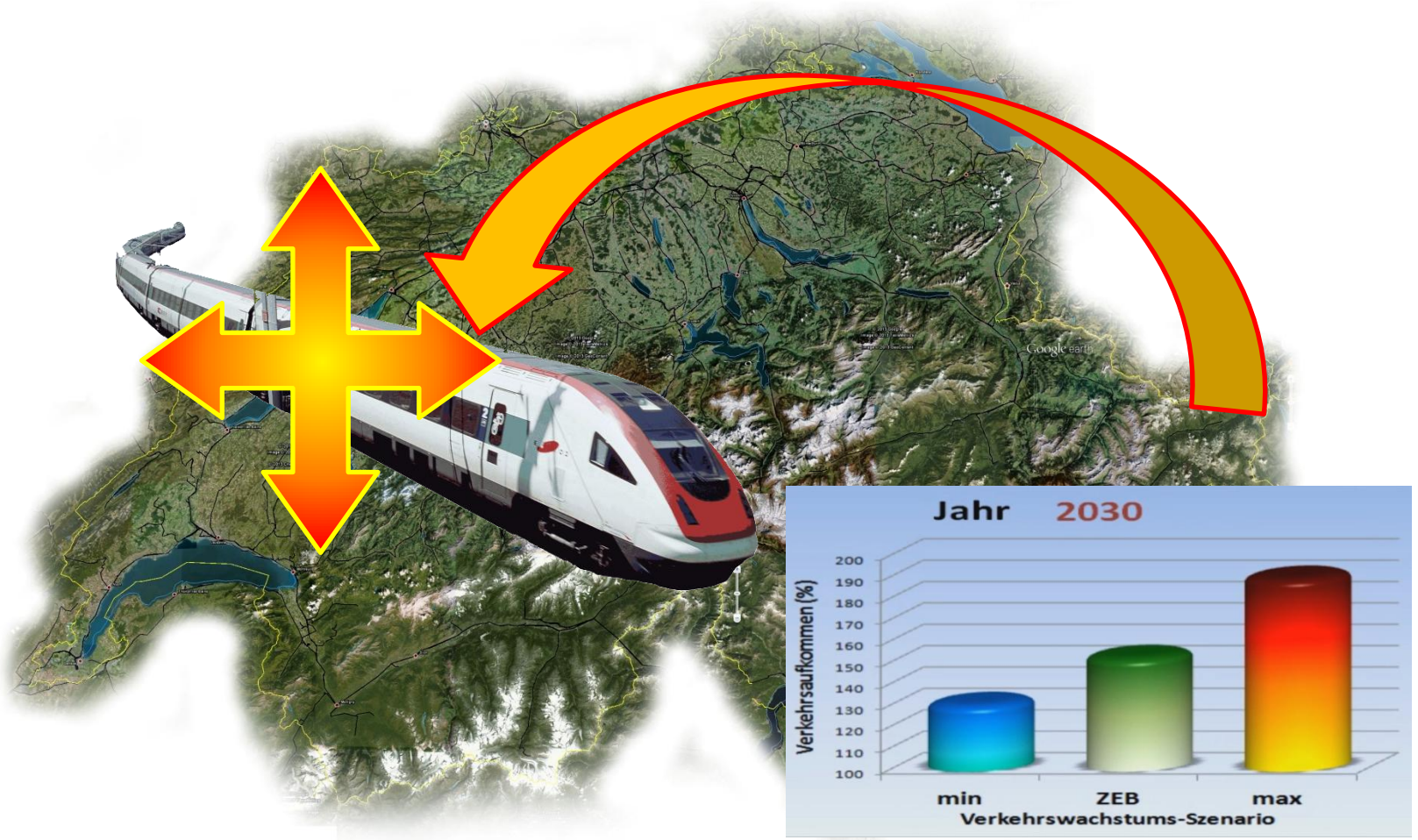
BOMBARDIER
the evolution of mobility

Knotenprinzip im Stundentakt



BOMBARDIER
the evolution of mobility

Konflikt: Neigezug / Verkehrsaufkommen



BOMBARDIER
the evolution of mobility

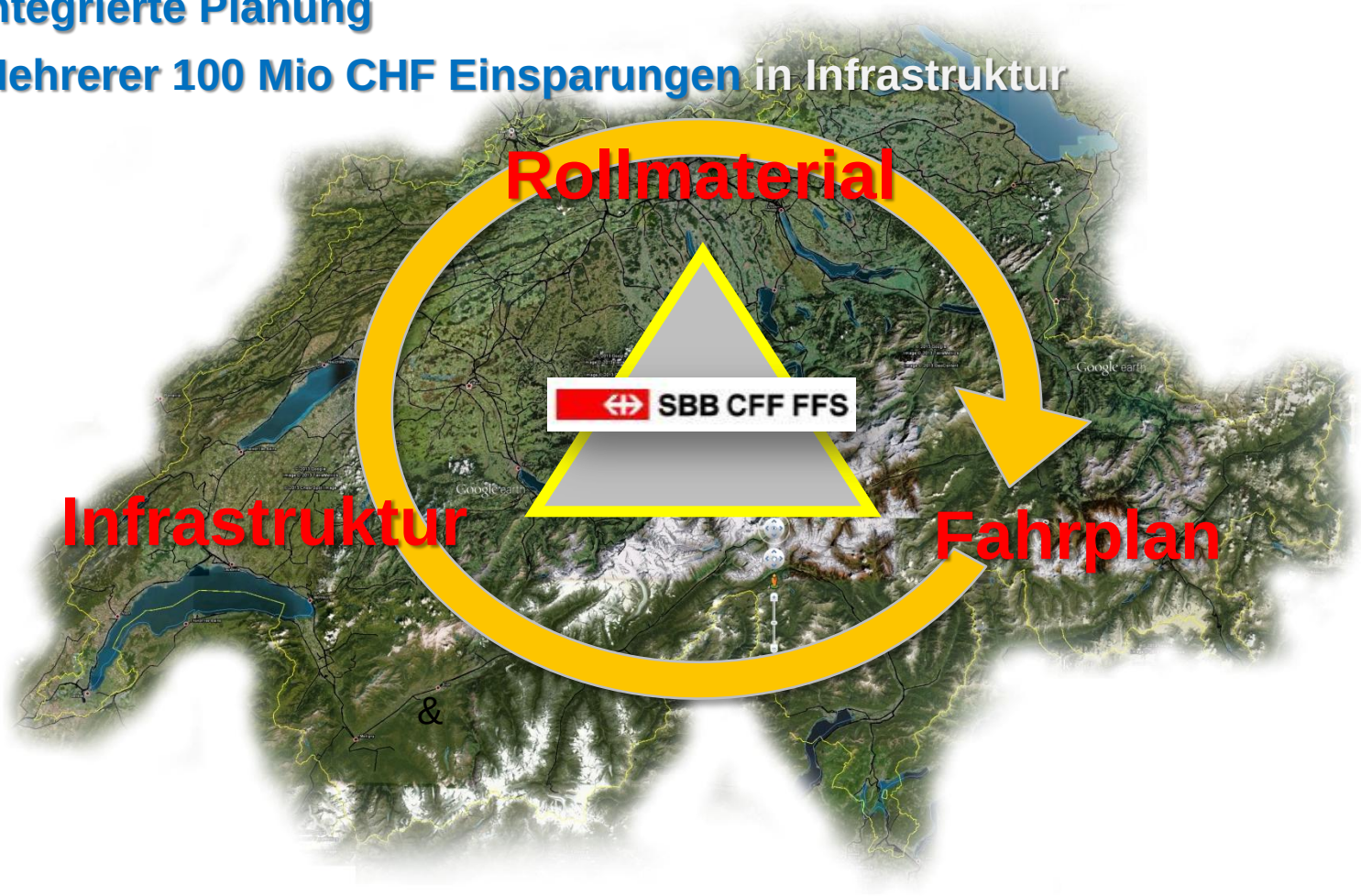
Konzept: Doppelstock & Wankkompensation

= WAKO™ & Twindexx von Bombardier

BOMBARDIER
the evolution of mobility

Konzept: Doppelstock & Wankkompensation

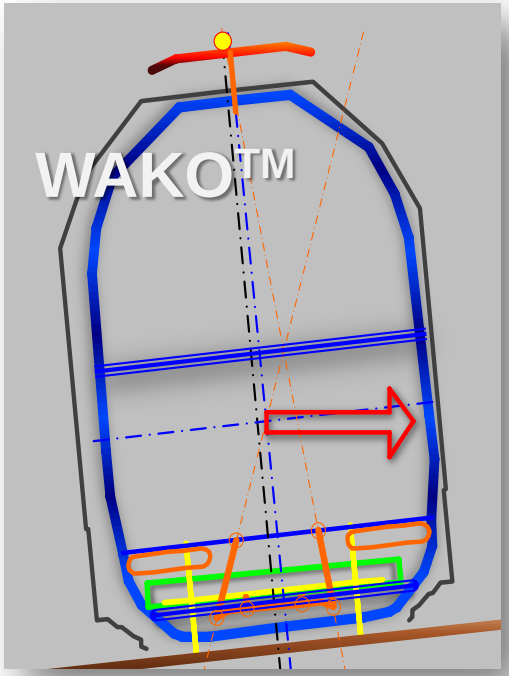
- **Integrierte Planung**
- **Mehrerer 100 Mio CHF Einsparungen in Infrastruktur**



BOMBARDIER
the evolution of mobility

Konzept: Doppelstock & Wankkompensation

12. Mai 2010 Vergabebentscheid an Bombardier

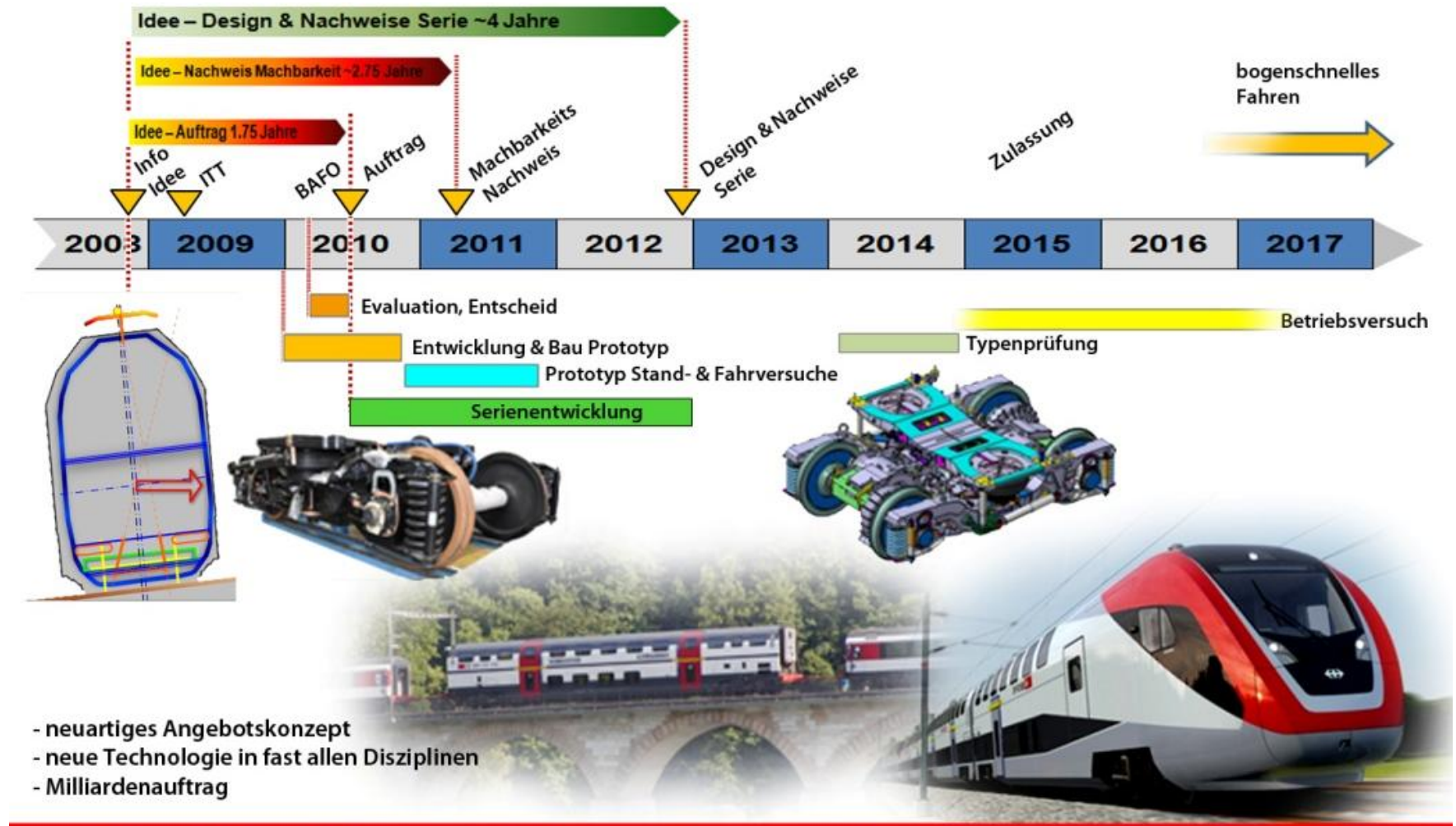


&

= Reisezeiten, Kapazität & Frequenzen

BOMBARDIER
the evolution of mobility

Rekord - Entwicklungszeit

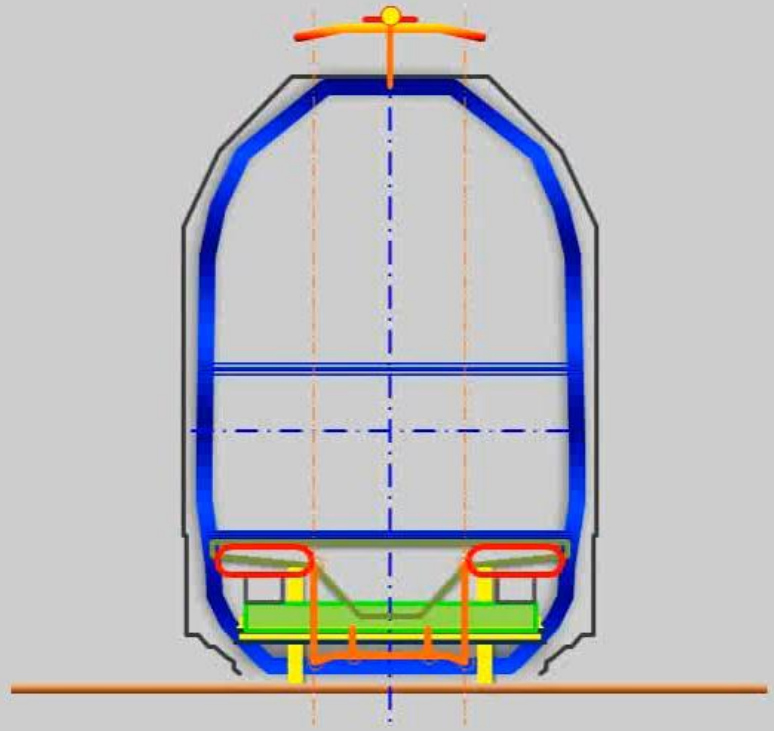


Rekord - Entwicklungszeit dank guter Zusammenarbeit & gegenseitigem Vertrauen

BOMBARDIER
the evolution of mobility

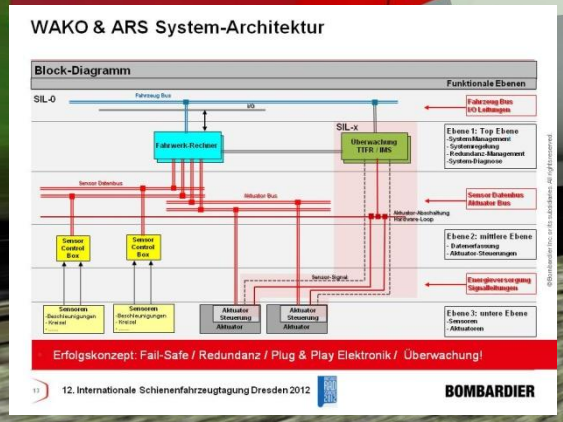
Inhalt

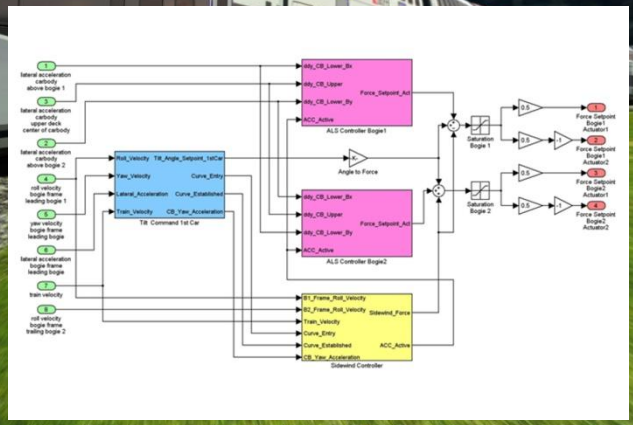
WAKO - Funktionsprinzip



WAKO - Funktionsprinzip

- Fail-Safe
- Sicherheit durch Überwachung
- Redundanz für Zuverlässigkeit
- Neigesensorik am vorl. FW
- Kraftregelung
- Aktive Neige- & Komfortregelung



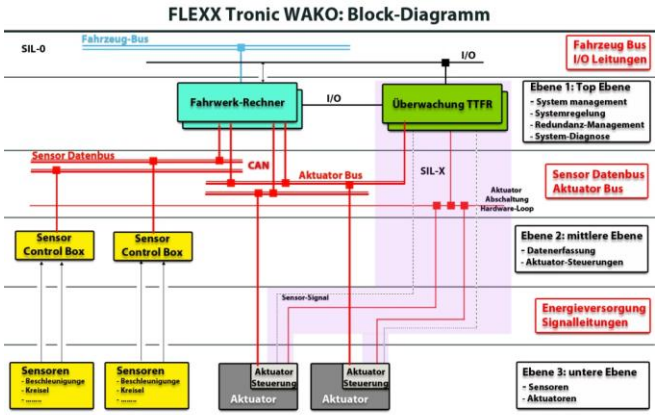


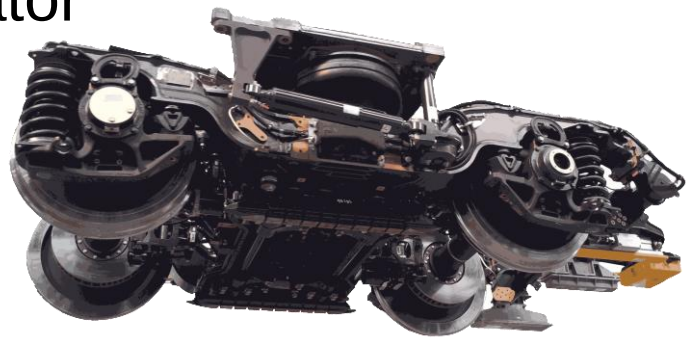
BOMBARDIER
the evolution of mobility

Inhalt

Plug & Play Elektronik

- Systemübersicht
- Elektronikkomponenten
- Aktuatoren
- Plug & Play
- Redundanz, Zuverlässigkeit
- Selbstkonfiguration und –kalibrierung
- Kommunikation
- Entwicklung & Prüfungen im Simulator
- Selbstdiagnose, Ausfallerkennung
- Hardware Tests
- Betrieb & Unterhalt





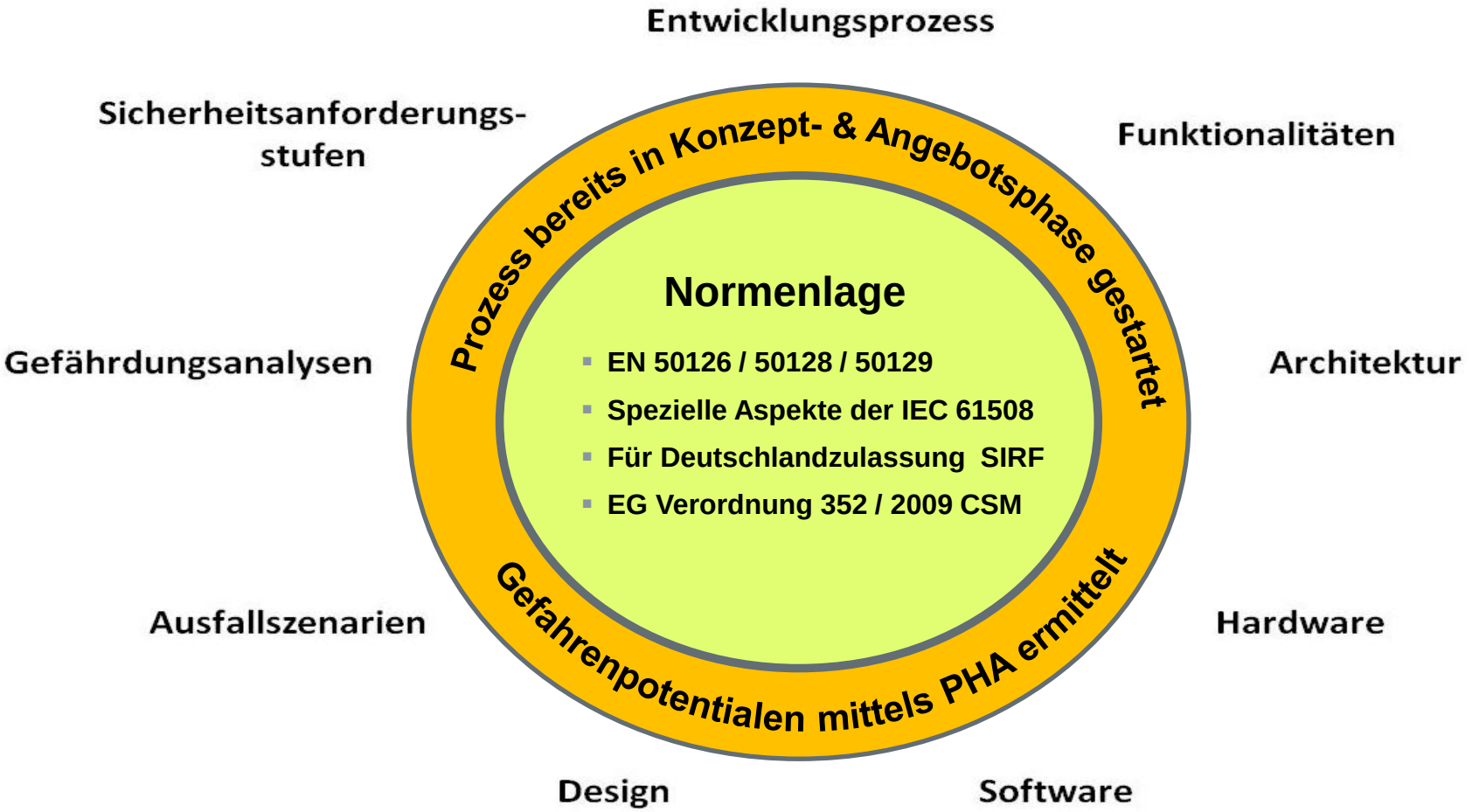
BOMBARDIER
the evolution of mobility

Plug & Play Elektronik

BOMBARDIER
the evolution of mobility

Inhalt

Iterativer Entwicklungs- und Nachweisprozess

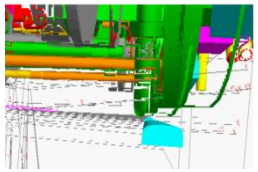


BOMBARDIER
the evolution of mobility

Gefährdungen

- **Verletzung des Fahrzeugumgrenzungsprofils (Bezugslinie)**
  - **Mögliche Kollision mit Infrastruktur oder anderem Zug**

- **Gefahr unzulässiger Radentlastung**
  - **Möglicher Verlust der Spurführung (Entgleisung)**



- **Gefahr unzulässiger Bewegungen zwischen Wagen**
  - **Mögliche Beschädigungen von Kupplung, Übergang, etc.**

- **Gefährdung von Passagieren im Fahrzeuginnern**
  - **Unzulässig hohe Querbeschleunigungen oder Rucke**

- **Gefährdung von Passagieren beim Ein- und Aussteigen**
  - **Fehlerhafte Wagenkastenbewegungen im Stillstand**

Sicherheitsnachweis

- **Drei Verfahren für den Sicherheitsnachweis**
  - **Nachweis auf Basis etablierter Regelwerke / CSM: Anerkannte Regeln der Technik**
  - **Nachweis auf Basis eines Referenzsystems / CSM: Ähnliche Referenzsysteme**
  - **Nachweis funktionaler Sicherheit / CSM: Explizite Risikoabschätzung**
- **Expliziter Nachweis der funktionalen Sicherheit wird für WAKO geführt**
- **Für SIL-Einstufung WAKO zwei Verfahren gewählt**
  - **Risikograph aus IEC 61508 Beispiel D1**
  - **Sicherheitsanforderungsstufe SAS gemäss SIRF Ausführungsbestimmungen 400**
- **Darstellung exemplarisch anhand „Verletzung des Fahrzeugumgrenzungsprofils“**
- **Aus Rücksicht auf laufendes Verfahren vorerst keine Veröffentlichung der zu erwartenden Ergebnisse**

Sicherheitsnachweis

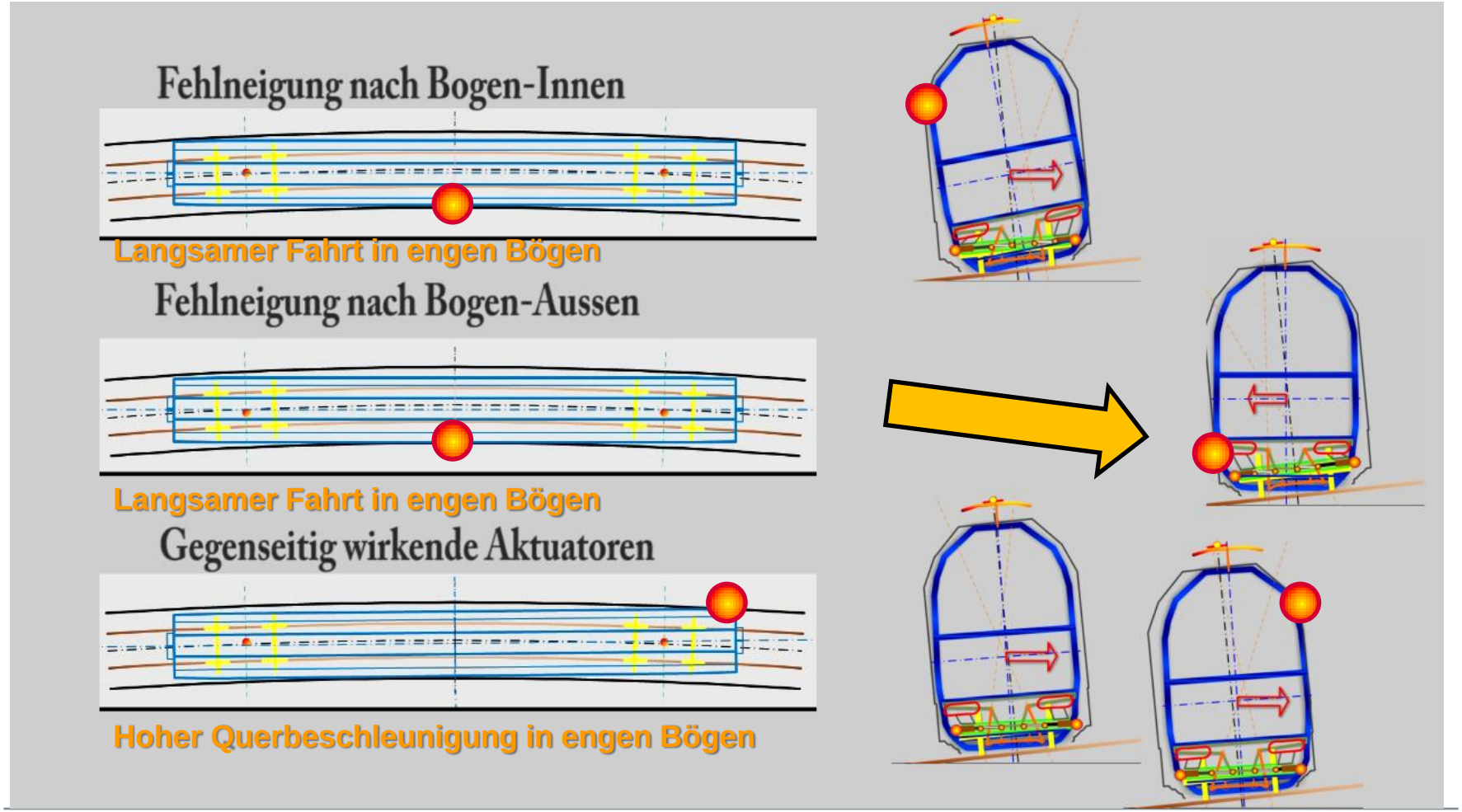
- **Technischer Sicherheitsplan TeSiP (Teil von SIRF)**
  - **Funktionsliste der Fahrzeugfunktionen**
  - **Generische Bewertung hinsichtlich SAS**
  - **Projektspezifische Einstufung obligatorisch**
  - **Begründete Abweichungen von generischer Einstufung möglich**

- **Identifikation des tatsächlichen Gefahrenpotentials**
  - **Bestimmung aller theoretisch möglichen Fehlfunktionen**
  - **Berechnung aller möglichen Fehlstellungen der Wagenkasten unter allen möglichen Betriebsbedingungen**
  - **Erweiterte Einschränkungsberechnung zur Ermittelung potentieller Überschreitungen der Bezugslinie**

Mögliche Fehlfunktionen

Tatsächliches Gefahrenpotential

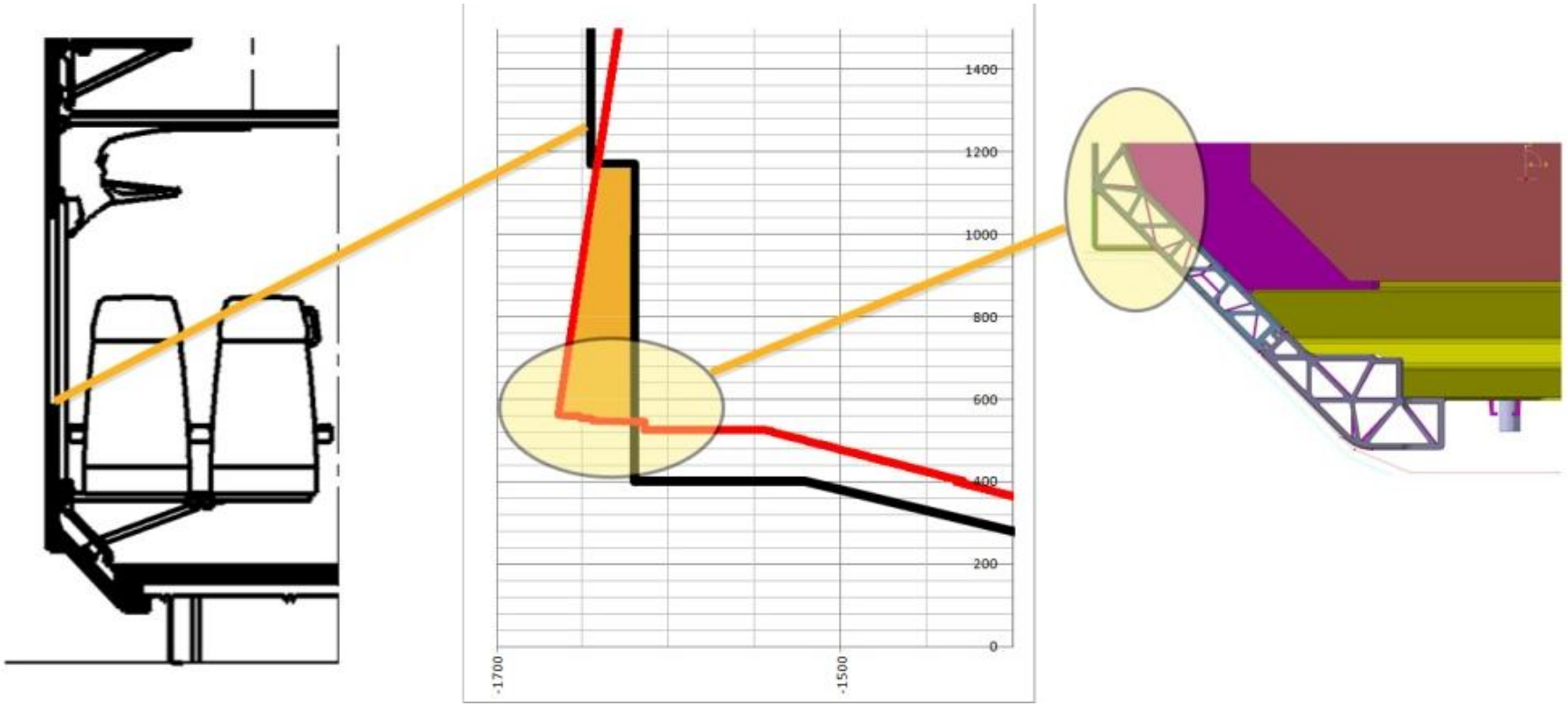
- **Potentielle Bezugslinienüberschreitung bei:**



BOMBARDIER
the evolution of mobility

Tatsächliches Gefahrenpotential

- **Bezugslinienüberschreitung im unteren Bereich in Mitte Wagenkasten**
- **Potentielle Gefahr der Kollision Langträger mit Infrastruktur (z.B. Platform)**
- **Fenster ausserhalb Gefahrenbereich**



BOMBARDIER
the evolution of mobility

Bestimmung Sicherheitsanforderungsstufe

Generische TeSiP Einstufung gemäss SIRF 400

Parameter zur Bewertun Sicherheitsrel gemäss SIRF 4			Formel zur Ermittlung Einstufungsindikator	
Schaden Anzah	Paramet			
Schaden Verletz	Paramet Verletzu		ungsindikator I	Sicherheitsan ngsstufe
Eintrittswahrsch	Parameter für Eintrittswahrscheinlichkeit (W)		0 21	SAS 0
Expositionszeit	Parameter für Expositions eit (E)		22 - 35	= SAS 1
Vermeidung	kurz	1	36 - 72	= SAS 2
Einstufungsindikat	lang	1.3	73 - 122	= SAS 3
	möglich	1.7		
Sicherheitsanforderungsstufe	SAS	SAS 3	123 - 281	= SAS 4

Ermittlung Einstufungsfaktor

$$I = \frac{S_A \times S_V \times W * E}{V}$$

= (5 * 9 * 1.7 * 1.3) / 1 = 99.45

BOMBARDIER
the evolution of mobility

Umsetzung im Projekt

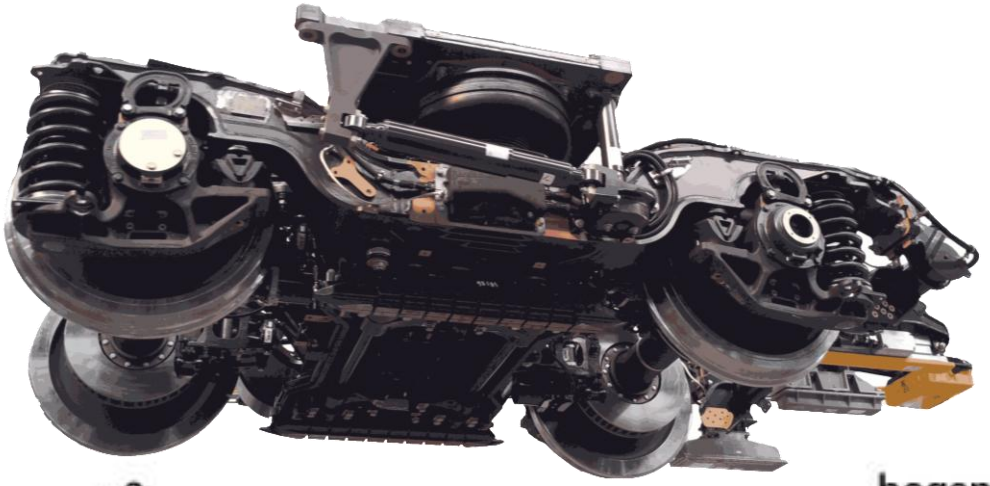
- **SIL/SAS-Einstufung als Grundlage für die Umsetzung im Projekt**
  - **Systemarchitektur**
  - **Anforderungen an Hard- und Software**
- **WAKO System**
  - **Eigentliches Regelungssystem für Wankkompensation & Komfort**
    - > **Keine Sicherheitsanforderungen dank Fail-Safe Konfiguration**
  - **Einfaches und unabhängiges Überwachungssystem TTFR**
    - > **Alleinige Sicherheitsverantwortung**
  - **Systemabschaltung bei sicherheitskritischer Fehlfunktion**
    - > **Überwachung der Aktuatorkräfte (Drücke) und Aktuatorbewegungen**
    - > **Stromlosschaltung der Aktuatorventile**
  - **Sicherer, passiver Zustand (Fail-Safe)**
  - **Der Sicherheitsstufe entsprechende Meldung an Fahrzeugleittechnik und Triebfahrzeugführer**
  - **Änderung der Fahrgeschwindigkeit**

Weiterführende Analysen

- **Sicherheitsanforderungsspezifikation**
- **Hard- und Softwareanforderungen (Spezifikationen)**
- **Interface Hazard Analyse für die Fahrzeugintegration**
- **Gefahrenprotokoll**
- **FMECA auf Bauteilebene**
  - **Ausschliessen von Einfach-Fehlern**
- **Fehlerbäume aller Teilsysteme**
  - **Ausschliessen von Common Cause Failures (Fehler auf Grund gemeinsamer Ursachen)**
- **Typentests mit Nachweis der korrekten Funktionalität**
  - **Labortests, Tests am Fahrzeug sowie Testfahrten**
  - **Nachweis der Sicherheit im Betrieb**
- **Eigentlicher Sicherheitsnachweis gem. EN 50129**

Inhalt

Weitere Entwicklung



BOMBARDIER
the evolution of mobility

Inhalt

Zusammenfassung

- Serienentwicklung praktisch abgeschlossen
- Erste Serienfahrwerke hergestellt
- Alle Erkenntnisse der Prototyp-Erprobung eingeflossen
- Wegweisende Elektroniksysteme modernster Technologie
- Plug & Play Architektur
- Vollständige Redundanz = ~100% Verfügbarkeit
- Fail-Safe Konfiguration erlaubt Sicherheit durch Überwachung
- Erfolgreiche Realisierung in kurzer Zeit
- Früher Einbezug von Gutachtern & Behörden
- Enge und vertrauensvolle Zusammenarbeit mit allen Beteiligten

HERZLICHEN DANK

BOMBARDIER

the evolution of mobility