TÜV NORD SysTec GmbH & Co. KG

Die neuen IC4 Diesel-Triebzüge für die DSB – Erfahrungen aus dem Zulassungsprozess unter Berücksichtigung der Entwicklung von der konventionellen hin zur CENELEC-basierten Sicherheitsnachweisführung

Autoren: Dr. Lutz Neumann, Reinhard Bühl (TÜV NORD)

39.Konferenz “Moderne Schienenfahrzeuge”, TU Graz, 11.-14. April 2010

TÜV NORD

Gliederung

1	Einleitung: IC4-Projekt aus der Gutachterperspektive
2	Grundlagen der CENELEC-Sicherheitsnachweisführung
3	Aufgaben des Independent Safety Assessors (ISA)
4	ISA IC4-
4.1	- Prozessbewertung
4.2	- Bewertung der Sicherheitsnachweisführung
4.3	- Ergebnisbewertung Sicherheitsbericht
5	Zusammenfassung und Ausblick

DMU IC4 – Typzulassung aus Sicht des ISA

1 Einleitung

- Zulassungsgrundlage: EN 50126 (CENELEC)
  - In Kraft seit ca. 2000
  - IC4- Liefervertrag und Spezifikation bereits davor vereinbart

- IC4- Sicherheitszulassungsprozess in Dänemark

Phase 1 (DSB)	•*Prüfung der Hersteller-Dokumentation gegen Vertragsanforderungen* •*Sicherheitsbeurteilung „nach bestem Wissen“ des Betreibers* •*DSB-Abnahme der Dokumentation als Basis für …* •*…zeitlich/ inhaltlich beschränkte Inbetriebnahmegenehmigung durch Behörde*
Phase 2 (ISA)	**CENELEC-basierte Sicherheitsbewertung durch unabhängigen Gutachter/ ISA:** **•Bewertung Sicherheitsnachweise (Safety Case)** **•Bewertung Hersteller-Sicherheitsmanagement/ Organisation und Prozesse:** ***Erstellen von Sicherheitsnachweisen,*** ***Typprüfverfahren,*** ***Änderungsverfahren,*** ***Bewertung von Abweichungen*** **•Gesamtgutachten für…** **•*…Typzulassung durch Behörde***

DMU IC4 – Spezifik der Aufgaben des ISA

- Projektstand zum Zeitpunkt unserer Beauftragung:
  - Mehrere IC4 im eingeschränkten Betrieb in Dänemark
  - Vorbereitung zur technischen Aufrüstung für den Tunnelbetrieb
  - Sicherheitstechnische Stellungnahmen des Betreibers zu Einzeldokumenten
  - Liste offener Punkte aus der bisherigen Projektentwicklung

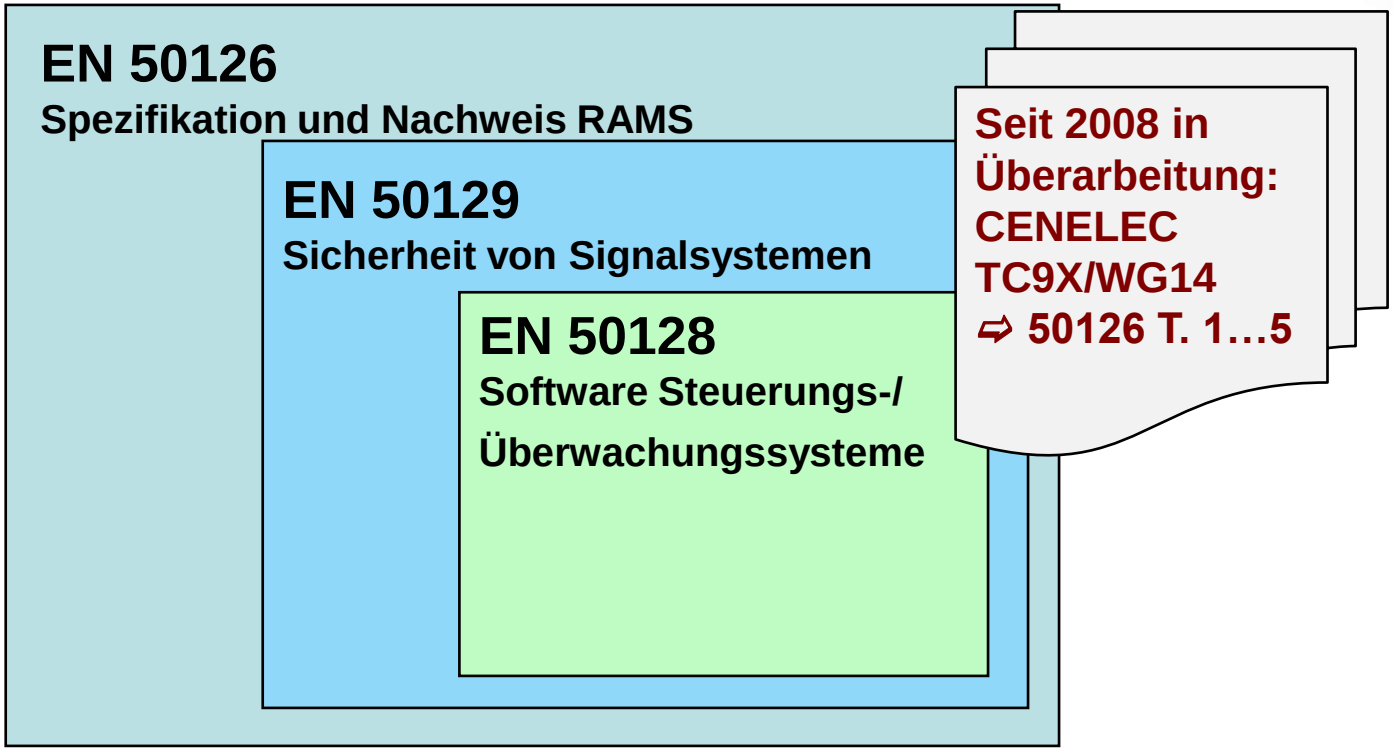
- Bewertung eines Sicherheitsberichtes mit >> 1000 Seiten:
  - Auswahl repräsentativer Dokumente für detaillierte Prüfung
  - Anerkennung vorliegender Stellungnahmen des Betreibers
  - Vermittlung der ISA-Zielstellung:
    Nicht Feststellung einer "*absoluten*" Sicherheit, *sondern*
    Bestätigung, dass Sicherheits*prozesse* etabliert sind und zu (beispielhaft geprüften) *verlässlichen* Nachweisen führen

Sicherheitsbegriff: klassisch versus “New Approach”

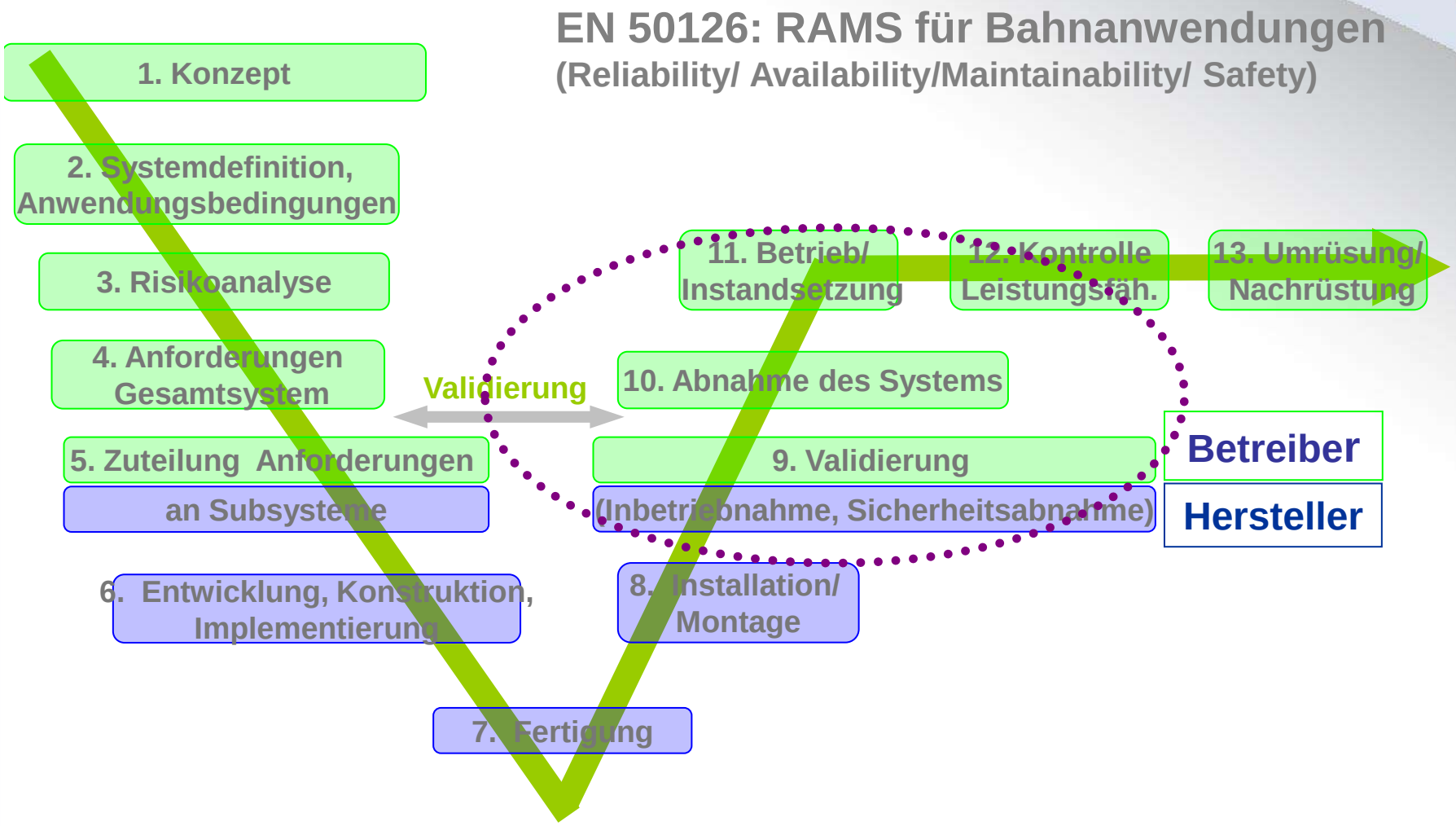
Traditionelle, regelorientierte Darstellung der Sicherheit	Risikobezgene Darstellung von Sicherheit nach CENELEC
Die Fähigkeit eines Systems mit Sicherheitsverantwortung, bei •***bestimmungsgemäßem*** *Einsatz,* •***ordnungsgemäßer*** *Instandhaltung,* •***vorschriftsmäßiger*** *Handhabung* über die definierte *Brauchbarkeitsdauer* ***Gefährdungen*** durch Funktionsversagen in dem nach *Stand der Technik* erforderlichen Umfang auch bei *Einzelfehlern* zu ***verhindern***	Sicherheit eins Systems gilt als ***ausreichend***, wenn das von ihm ausgehende ***Risiko*** (Schadenshäufigkeit x Schadensausmaß) durch definierte systemtechnische und organisatorische Maßnahmen bis zu einer ***Toleranzschwelle reduziert*** wird

Harmonisierung der Sicherheitsanforderungen: EN 5012x für Bahnanwendungen

- EN 50126: Spezifikation von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit/ Lebenszyklus
- EN 50129: Sicherheitsnachweisführung/ Sicherheitsbericht, Sicherheitsmanagement



Lebenszyklusmodell nach CENELEC



Struktur eines CENELEC-Sicherheitsnachweises

T.6: Zusammenfassung

T.5: Bezieh. zu anderen Sicherheitsnachweisen

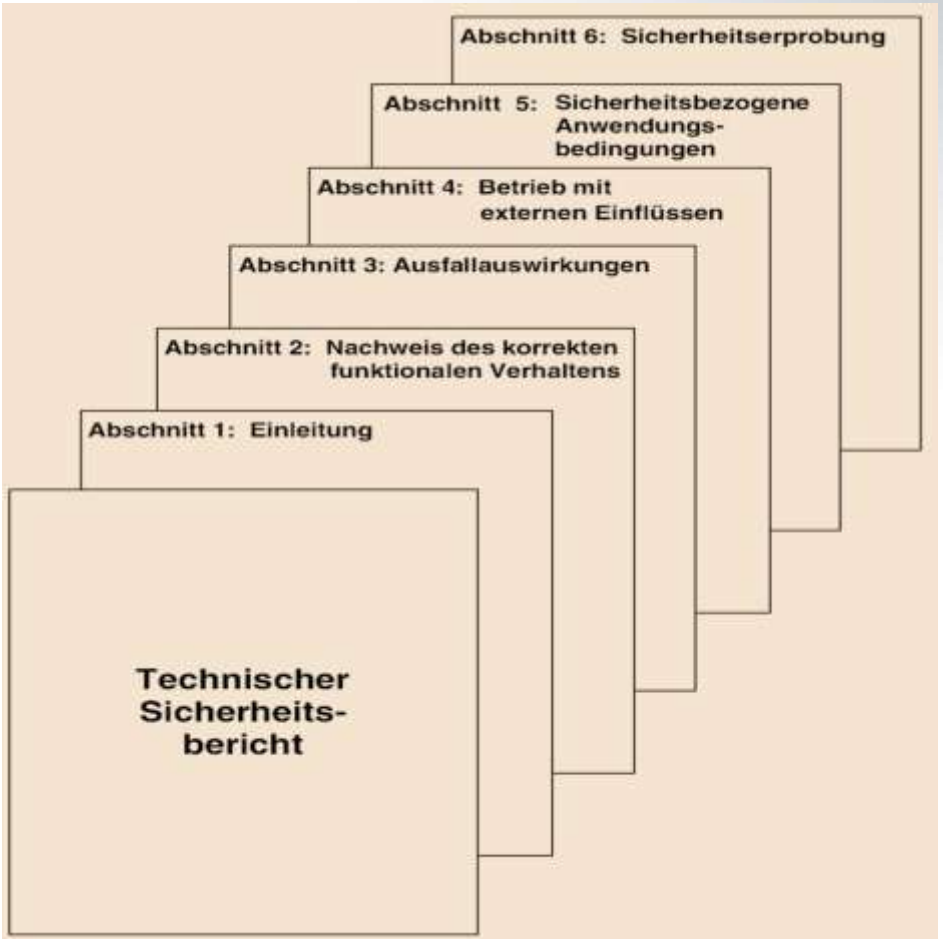
T.4: Technischer Sicherheitsbericht

T.3: Sicherheitsmanagementbericht

T.2: Qualitätsmanagementbericht

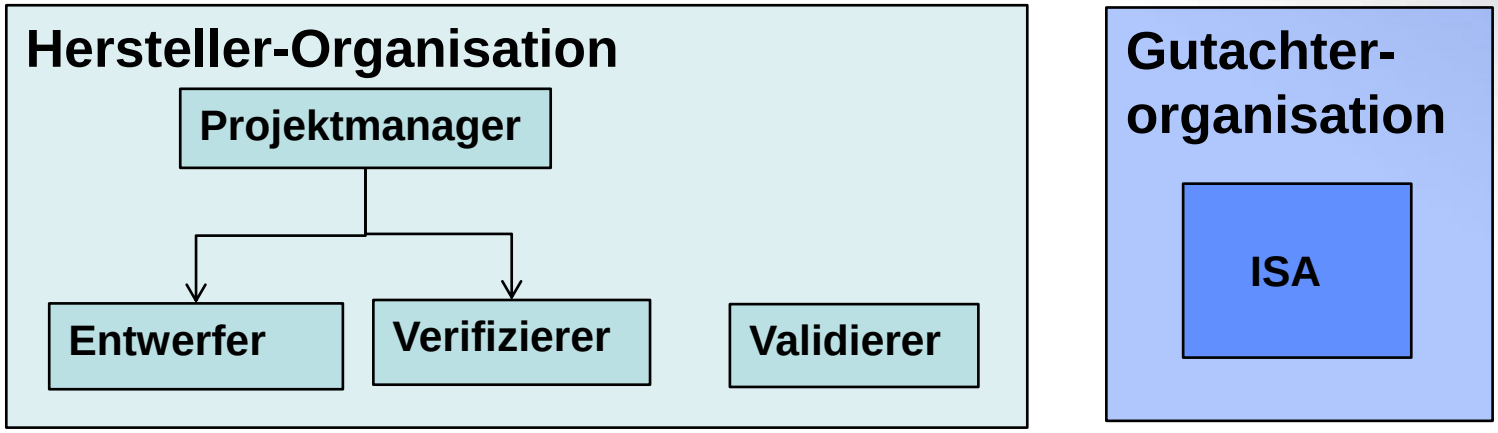
T.1: Definition des Systems

Systemsicherheits-nachweis



Unabhängige Sicherheitsbegutachtung

- Beispiel für Rollenverteilung nach EN 50129:
  - Unabhängigkeit zwischen Entwicklung und Prüfung im Werk
  - Begutachtung durch externe, zertifizierte Institution



- Fragestellungen des Sicherheitsgutachters:
  - Ist die Sicherheitsanforderungsspezifikation dem Einsatzzweck adäquat?
  - Erfüllt das Finalprodukt diese Anforderungen?
  - Ist das Sicherheitsmanagement normenkonform?

ISA- Aufgaben im finalen IC4-Zulassungsverfahren

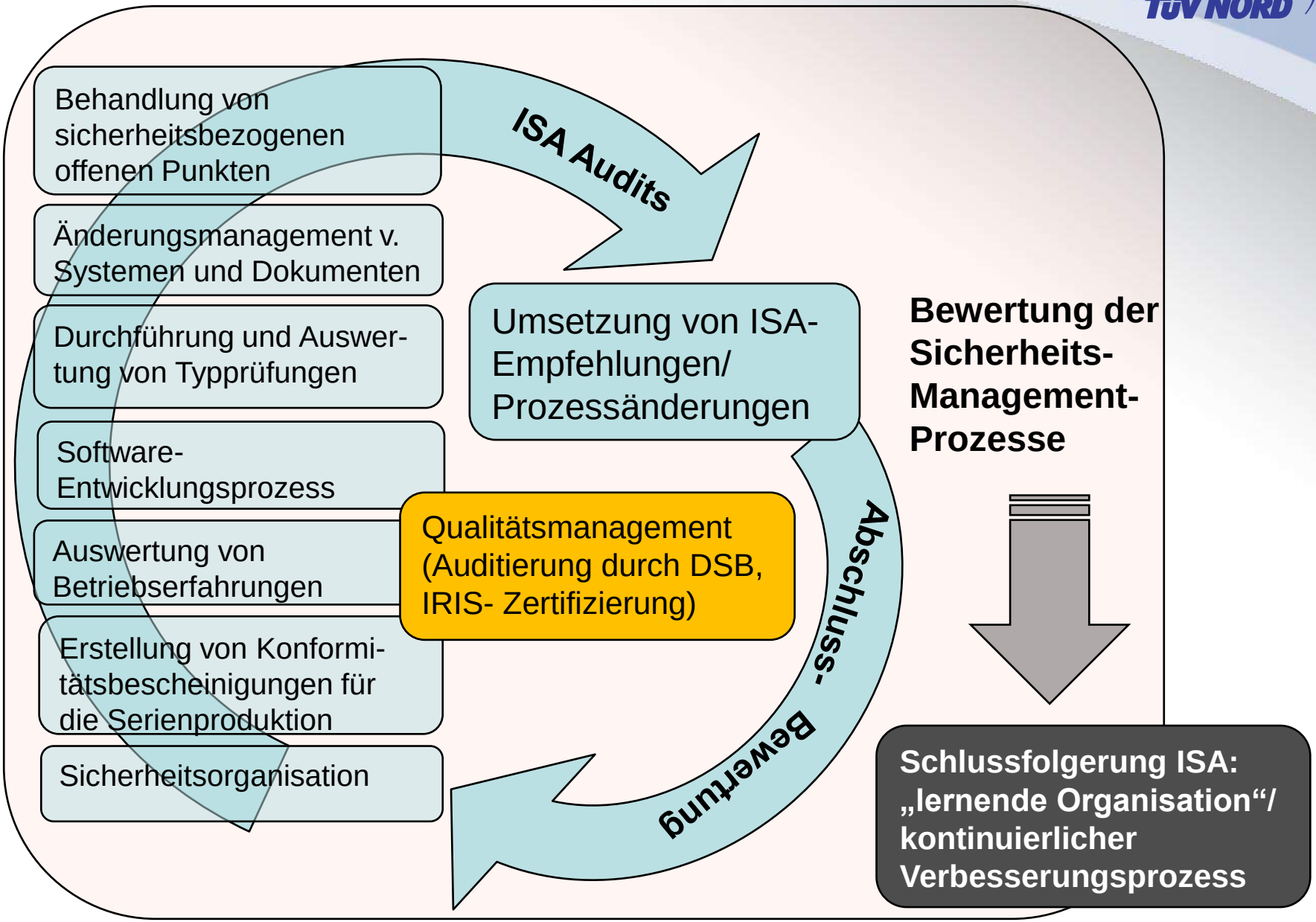
TÜV NORD

Begutachtung/ Überprüfung/ Bewertung…

- Sicherheitsmanagement incl. Änderungsmanagement
- Änderungen an geprüften Systemunterlagen und Sicherheitsnachweisen
- Noch vor der Typzulassung geplante technische Änderungen
- Vorprüfung System- und Sicherheitsspezifikation zum Kupplungssystem
- Sicherheitsanforderungen im Hinblick auf gesamten Lebenszyklus
- Betriebs-und Instandhaltungsberichte
- Nichtkonformitäten und offene Punkte
- “Sicherheitsbezogenen Anwendungsbedingungen”
- Hersteller-Konformitätserklärungen im Rahmen der IC4-Serienfertigung

…Erstellung ISA Abschlussbericht

Bewertung von Sicherheitsprozessen



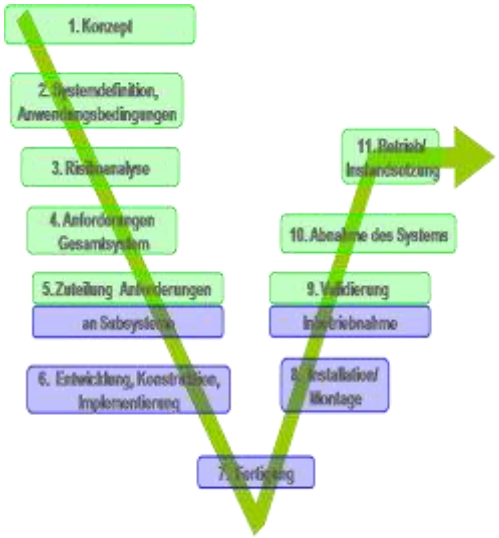
Bewertung von Sicherheitsnachweisen

Dokument/ Prozess	Detaillierte Dokumentenbewertung	Stichprobenbewertung	"Vertical slice assessment"	Interviews/ Audits	Besichtig. v. Prozessen vor Ort (Stichproben)	
Sicherheitsbericht- Hauptdokument	✓		✓			
Sicherheitsplan				✓		
Sicherheitsanforderungsspezifikation			✓			
Vorläufige Gefahrenanalyse			✓			
Sicherheitsanalyse Außentüren/ Innentüren			✓			
Sicherheitsanalyse Bremsen			✓			
Sicherheitsanalyse Kupplung	✓					
Sicherheitsanalyse Antrieb/ Treibstoffversorgung			✓			
Sicherheitsanalyse Steuerungssystem			✓			
Sicherheitsanalyse Fahrzeugaufbauten		✓				
Sicherheitsanalyse Drehgestelle		✓				
Gefährdungslogbuch			✓			
Sicherheitsanalyse Zugrechner/ Sifa			✓			
Testprozedur gekuppelter Betrieb	✓				✓	
Konformität zu aktuellen Standards			✓			
Sicherheitsmanagementprozesse	✓		✓	✓		
Vorläufiges Änderungsmanagement	✓				✓	
Umgang mit offenen Punkten			✓	✓		
Abschluss si-relev. offener Punkte	✓					
Softwareentwicklungsprozess		✓		✓		
Bewertung von Betriebserfahrungen						

„Vertical Slice Assessment“ für Ereignis „Brand im Tunnel“

„Vertical Slice Assessment“ [Yellow Book]

Bewertung einer definierten Gefährdung über den Lebenszyklusprozess hinsichtlich der…



…funktionalen Sicherheitsanforderungen

…technischen Lösung (Begrenzungsmaßnahmen)

…Prüfung der Wirksamkeit der implementierten Lösung

Ergebnis: Abbild des gesamten Sicherheitsengineering-Prozesses am konkreten Beispiel, mit begrenztem Aufwand

Auszug Gefährdungslogbuch/ Risikomatrix

Gefährdung	Beschreibung der Gefährdung
10	Unter-Flur-Ausrüstungsteile gelöst
11	Beschädigung von Drehgestell-Komponenten
29	Der Triebfahrzeugführer erhält keine Kenntnis von einem Brandereignis (Feuer, Rauch) im Zug
33	Im Falle eines Fahrzeugbrandes im Tunnel wird die von Passagieren ausgelöste Notbremsanforderung nicht überbrückt (Zug hält brennend im Tunnel)
40	Brandereignis durch Überhitzung von Unterflurkomponenten
51	**Im Gefahrenfall ist der Notausstieg aus dem Zug bei gleichzeitig eingeschränkten Evakuierungsbedingungen behindert**

Häufigkeit eines Gefahrenfalls	*Risikoeinstufung für ausgewählte Gefährdungen*			
häufig	unerwünscht	intolerabel	intolerabel	intolerabel
wahrscheinlich	tolerabel	unerwünscht	intolerabel	intolerabel
gelegentlich	tolerabel	unerwünscht	unerwünscht	intolerabel
selten	vernachlässigbar	tolerabel	unerwünscht	unerwünscht
unwahrscheinlich	vernachlässigbar	vernachlässigbar	tolerabel	Tolerabel *10, 11, 17, 70*
unvorstellbar	vernachlässigbar	vernachlässigbar	vernachlässigbar	vernachlässigbar *29, 33, 40,* **51**
	Unbedeutend leichte Verletzung	**marginal** Schwere Verletzung	**kritisch** 1 Opfer	**katastrophal** ≥10 Opfer
	Gefahrenstufen: Schweregrad der Gefährdungswirkungen			

4.2 ISA im IC4-Projekt

Ergebnis des „Vertical Slice“ Ansatzes

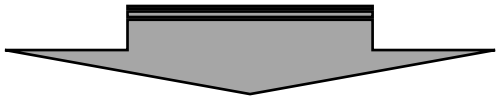
Nachvollzogene Sicherheitsdokumentation zu # 51 …

- Sicherheitsanforderungsspezifikation
- Systemsicherheitsanalysen
- Prüfvorschriften
- **Prüfergebnisse**
- Offene Punkte aus früheren LZ-Phasen

Nichtkonformität bei Testfahrten an Steigung im Tunnel

„Die Geschwindigkeit kann bei Anfahren an Steigung mit 3 betriebenen Antriebsaggregaten nicht über 6 km/h erhöht werden.“

- Betrifft die Fähigkeit des Zuges, einen Bereich mit Evakuierungs-einschränkungen anforderungsgemäß zu verlassen
- Zuordnung zu Gefährdungsereignis #51
- Technische Lösung: Änderungsmaßnahme „Neuer Datensatz für Antriebsaggregat“



Vertical Slice-Prüfung zeigte anforderungskonforme Auslegung auf

Erfüllungsgrad CENELEC- Gesamtanforderungen

4.3 ISA im IC4-Projekt

Anforderungs-Nr.		3	11	31
Lebenszyklus-Phase:		2- Systemdefinition	3- Risikoanalyse	8- Installation
Dokumentenbez.		Vorläufige Systemspezifikation	Risikoanalyse	Installationsbericht
Referenz EN 50126		6.2.3.1	6.3.3.1 ,6.3.3.2	6.8.3.1-2
Referenz EN 50129			Anhang, A.4.1	5.1-5.5
Zielstellung des Dokuments		Beschreibung der ➢ funktionalen, ➢ nicht-funktionalen, ➢ RAMS-bezogenen, ➢ schnittstellenbezog., ➢ begrenzungsbezog., ➢ physikalischen bzw. technologischen Anforderungen für die Projektentwicklung	Beschreibung der Aktivitäten zur Identifikation, Bewertung und Beseitigung bzw. Kontrolle der Gefährdungen bzw. der Reduktion der resultierenden Risiken auf ein tolerables Maß	Dieses Dokument dient der Synthese der „Bedingungen für eine Sicherheitsanerkennung“ und verweist auf die Nachweisdokumente zum Qualitätsmanagement, zum Sicherheitsmanagement, zur funktionalen und technischen Sicherheit
TÜV NORD Bewertung	**Erfüllungsgrad**	teilweise	sehr gut	gut
	IC4-Dokumente	AA02RX5, AA02RX6	AA02RX5, AA02RXH	AA01HXW, AA02RX5
	Erläuterung	Im Projekt wurden keine SIL-Anforderungen spezifiziert, wohl aber Sicherheitsanforderungen für die Sub-Systeme risikobezogen abgeleitet und im Hazard Log dokumentiert. Keine kritische Abweichung.	Das vorliegende Hazard Log über 84 Gefährdungen wird als hochqualifiziertes Dokument angesehen, das alle wichtigen Aspekte von Gefährdungsszenarien zu den Systemsicherheitsanalysen dokumentiert und nach qualitativen und quantitativen Kategorien bewertet.	Die Nachweisführung erfolgte im Sicherheitsbericht-Hauptdokument durch Verweise auf die entsprechenden Nachweisdokumente

Systemspezifikation

teilweise Erfüllung

keine SIL. spezifiziert, aber risikobezogene Anforderungen abgeleitet

⇒Abweichung nicht kritisch

Zusammenfassung und Ausblick

Ergebnisse und Erkenntnisse der IC4-ISA-Bewertung

- Grundsätzliche Konformität zu CENELEC- Standards
- Wirksame Sicherheitsmanagement-Prozesse beim Hersteller
- Sicherheitsbericht/ Gefährdungslogbuch als „lebendes“ Dokument
- Risikobasierte Auswahl von Stichproben/ „Vertical Slice Assessment“ für effektive Prüfung bewährt
- Unabhängige Prüfung führt zu mehr Transparenz, Effektivität und Vertrauen im behördlichen Zulassungsverfahren

Ausblick auf zukünftige Sicherheitsnachweisführung

- IC2-Projekt: Erfahrungsbasis IC4 + Berücksichtigung aktueller TSI
- Generell: Einzug risikobasierter Sicherheitsnachweisführung in TSI
- „Stand der Technik“ der Sicherheitsnachweisführung wird unter Federführung der ERA fortentwickelt (CCM, CCT, CCI)

Sammlung, Aufbereitung und Pflege von Felddaten

- Aus ISA Sicht wichtige Aufgabe zur Unterstützung einer CENELEC-konformen Sicherheitsnachweisführung („FRACAS“)

Danke für Ihr Interesse!

Dr.Lutz Neumann

TÜV Nord SysTec GmbH & Co.KG
Competence Center Safety Concepts
Zimmerstraße 23, D-10969 Berlin
Tel. ++49 30 201 774 43
e-mail LNEUMANN@TUEV-NORD.DE
www.tuev-nord.de

Reinhard Bühl

TÜV Nord SysTec GmbH & Co.KG
Inspektionsstelle Bahntechnik
Zimmerstraße 23, D-10969 Berlin
Tel. ++49 30 201 774 51
e-mail RBUEHL@TUEV-NORD.DE
www.tuev-nord.de