

Eine vergleichende Betrachtung globaler Sicherheitsstandards für Verkehrssysteme

Einleitung

- Spannungsfeld der Anforderungen

Motivation

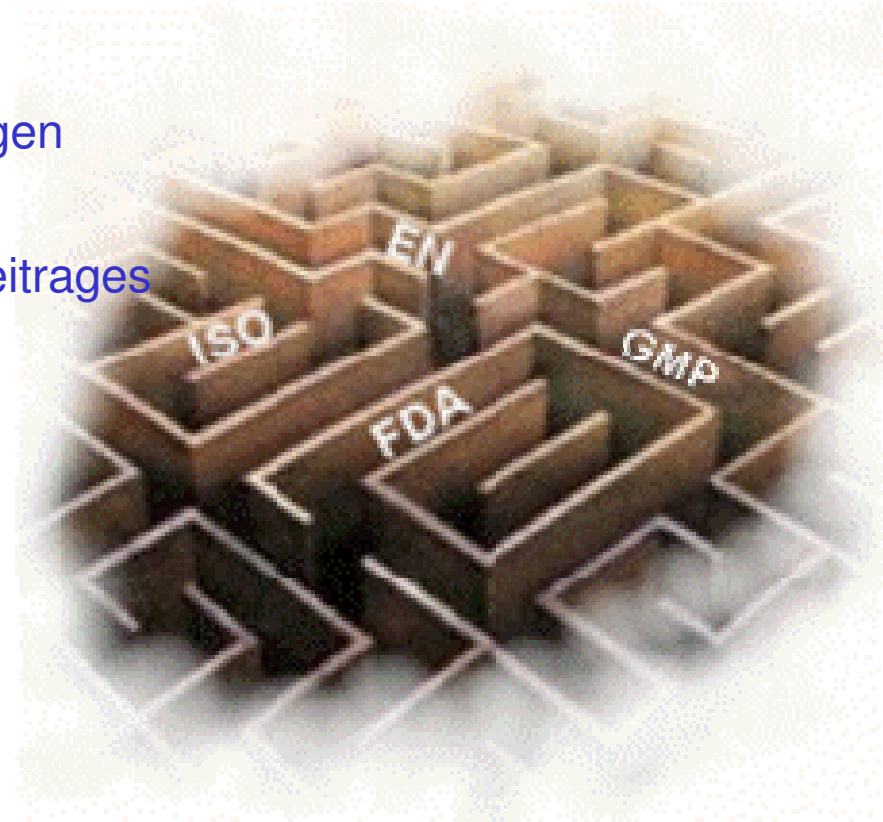
- Ausgangspunkt und Ziel des Beitrages

Standards

- IEC 61508
- Luftfahrt-Standards
- Eisenbahn-Standards
- Automobil-Standards

Vor- und Nachteile

Zusammenfassung und Ausblick



Dipl.-Ing. Tobias Ständer, Dr.-Ing. Uwe Becker

- die **Sicherheit** von Verkehrssystemen ist heutzutage in fast allen Branchen technisch und wirtschaftlich relevant und wird von der Gesellschaft als prior eingestuft
- mit der Forderung nach sicheren Systemen (Safety/Security) einher gehen steigende **Anforderungen an ein Konglomerat aus:**
 - System**zuverlässigkeit** (Reliability)
 - System**verfügbarkeit** (Availability)
 - **Wartbarkeit** (Maintainability)
- die **Komplexität** sicherheitskritischer Systeme in modernen Verkehrsmitteln nimmt rapide zu
- steigendes **Kundebewusstsein gegenüber Elektronikstörungen** aufgrund steigender Komplexität und Wichtigkeit von Elektroniksystemen in der Automobilarchitektur

- Fakt ist, dass **Sicherheit** und **Verlässlichkeit** von Verkehrssystemen nicht ausreichend geprüft werden können
- **Sicherheit** und **Verlässlichkeit** müssen bereits in Planung und Projektierung konstruiert werden
- um diesen **Anforderungen gerecht zu werden**, und um die von sicherheitskritischen Systemen (z.B. Kraftfahrzeugen) ausgehenden **Gefahren zu minimieren**, sind **Normen** und **Standards** erforderlich

Ziel des Beitrages:

Vergleichender Überblick über Normen, Richtlinien und Standards im Umfeld von Sicherheitsbetrachtungen von Verkehrsmitteln der Verkehrsträger Luft, Schiene und Straße

IEC 61508 (Meta- oder Grundnorm)

ISO TR 15497 MISRA-Guideline (Automotive)

ECSS-E-40A (EU, Raumfahrt)

RTCA DO-178B/C (Luftfahrt → SW)

RTCA DO-254 (Luftfahrt → HW)

SAE ARP 4754 (Luftfahrt → Zulassung)

SAE APR 4761 (Luftfahrt → HW)

NASA-GB-1740.13-96 (SW-Guidebook)

EGV 336/06 (sicherer Schiffsbetrieb)

DIN EN 9875 (Schiffe und Meerestechnik)

Sicherheit

VDI 4001-10

DIN EN 60300-2

Zuverlässigkeit

VDA Band 3.1 u. 4.ff

ISO 9000ff

Qualität**IEC 61508 – Derivate**

IEC 61513 (Nuklearsektor)

IEC 62061 (Maschinenindustrie)

DIN EN 50126/28/29 (Bahnanwendungen)

IEC 61511 (Prozess-Industrie)

ISO WD 26262 (Automotive)

- IEC 61508 („Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“):
 - wichtigste und am besten etablierte Norm in der umfassenden Normenlandschaft
 - kann auf zweierlei Wegen eingesetzt werden
 - Direkt von Industrieunternehmen zur Entwicklung sicherheitskritischer Systeme
 - Zur Entwicklung branchenspezifischer Standards

Normenlandschaft – Sicherheit, Zuverlässigkeit und Qualität

EUROPEAN STANDARD **EN 61508-1**
NORME EUROPÉENNE
EUROPÄISCHE NORM December 2001

ICS 13.110.25 040.29 020.35 240.50

English version

**Functional safety of electrical/electronic/programmable electronic
safety-related systems**
Part 1: General requirements
(IEC 61508-1:1998 + corrigendum 1999)

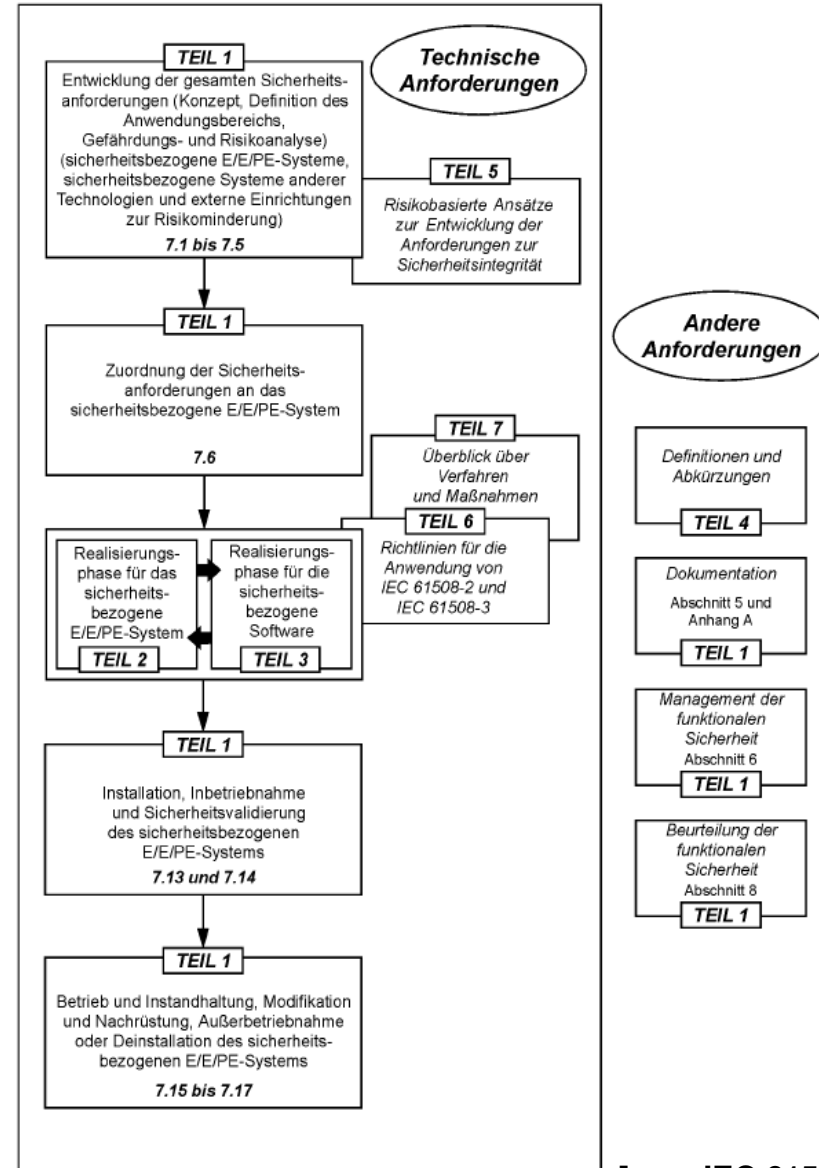
Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
Partie 1: Prescriptions générales
(CEI 61508-1:1998 + corrigendum 1999)

Funktionale Sicherheit
sicherheitsbezogener elektrischer/
elektronischer/programmierbarer
elektronischer Systeme
Teil 1: Allgemeine Anforderungen
(IEC 61508-1:1998 + Corrigendum 1999)

- Internationaler **generischer Standard**, welcher beschreibt, welche **Anforderungen** an die **funktionale Sicherheit** sicherheitsbezogener **E/E/PE-Systeme** gestellt werden
- schildert **allgemeinen Lösungsweg** für die Gesamtheit der Tätigkeiten während des **Sicherheitslebenszyklus**
- **allgemeiner Lösungsweg** wurde gewählt, um eine **branchen-unabhängiges** und **konsistentes** technisches Verfahren für alle elektrischen Systeme zu entwickeln

Struktur des Standards

- Teil 1: Konzept, Definition, Gefährdungs- und Risikoanalyse,
- Zuordnung von Sicherheitsanforderungen
- Teil 2: Realisierungsphase sicherheitsbezogener E/E/PE-Systeme
- Teil 3: Anforderungen an sicherheitsbezogene Software
- Teile 4 - 7: informative Teile



[aus: IEC 61508]

➔ Vorgehensbeschreibung (Leitfaden)

- **detaillierte Beschreibungen** der Vorgehensweise, welche die **Übereinstimmung mit der Norm vereinfachen** sind in den erläuternden Teilen (1 - 3) **nicht enthalten**
 - Teil 5 (informativer Teil) ist hinzu zu ziehen:
 - dieser beschreibt **risikobasierte Ansätze zur Entwicklung der Anforderungen an die Sicherheitsintegrität**
 - **Methoden** zur Durchführung von **Gefährdungs- und Risikoanalyse** (Anhang B)
- ➔ jedoch auch hier fehlt ein detaillierter **roter Faden** (Leitfaden) zur Durchführung der zur Zulassung erforderlichen Aktivitäten

➔ Übereinstimmung mit der Norm

- um Übereinstimmung mit der Norm zu erreichen ist zunächst eine strikte Abschnittserfüllung gefordert
 - Selbst auferlegte Anforderung nach Normerfüllung wird allerdings in Absatz 4.2 in sich selbst relativiert



„Wird Norm in Fällen, in denen keine internat. anwendungsspez. Norm vorhanden ist, direkt angewendet, so können bestimmte in der Norm festgelegte Anforderungen unnötig sein, und eine Befreiung von der Normerfüllung in Bezug auf solche Anforderungen ist akzeptabel, vorausgesetzt, dass dies begründet ist.“

	Luftfahrt	Automobiltechnik	Eisenbahntechnik
Bewegung	3-D (Raum)	2-D (Fläche)	1-D (Linie)
Pilot / Fahrer	i. d. R. 2 (Profis)	1 (Amateur v Profi)	1 (Profi [+ Sicherheitsfahr- ... (Sifa)])
Wetter			, ohne Sicht
Phasen			freie Strecke
Stückzahl			denz fallend)
Kosten (Elektroenergie)			€/kg ...; 25000€/15kg)
Frequenz d. Modellwechsel			hre
Unfalluntergrenze			wändig, ntation wird
Wartung, Instandhaltung			ne Werkstätte
	Betrieben	„Klitschen“, jeder	bei NE-Bahnen
Personenkilometer (2002 für Deutschland)	ca. 43 Mrd./a	ca. 76 Mrd./a	ca. 71 Mrd./a
Todesopfer (2002 in Deutschland)	ca. 120 1/a	ca. 6.800 1/a	ca. 200 1/a

→ Vor diesem Hintergrund sind verschiedene Normungskomitees bemüht in Anlehnung an die Sicherheitsgrundnorm IEC 61508 einen für ihren Bereich sinnvoll anwendbaren Standard zur Zertifizierung und zur Durchführung von Analysen im Bereich von Sicherheitsbetrachtungen zu entwickeln bzw. durchzusetzen und zu verbreiten

[aus: div. Quellen; s. Beitrag]

Charakteristische Unterschiede der verschiedenen Verkehrsträger

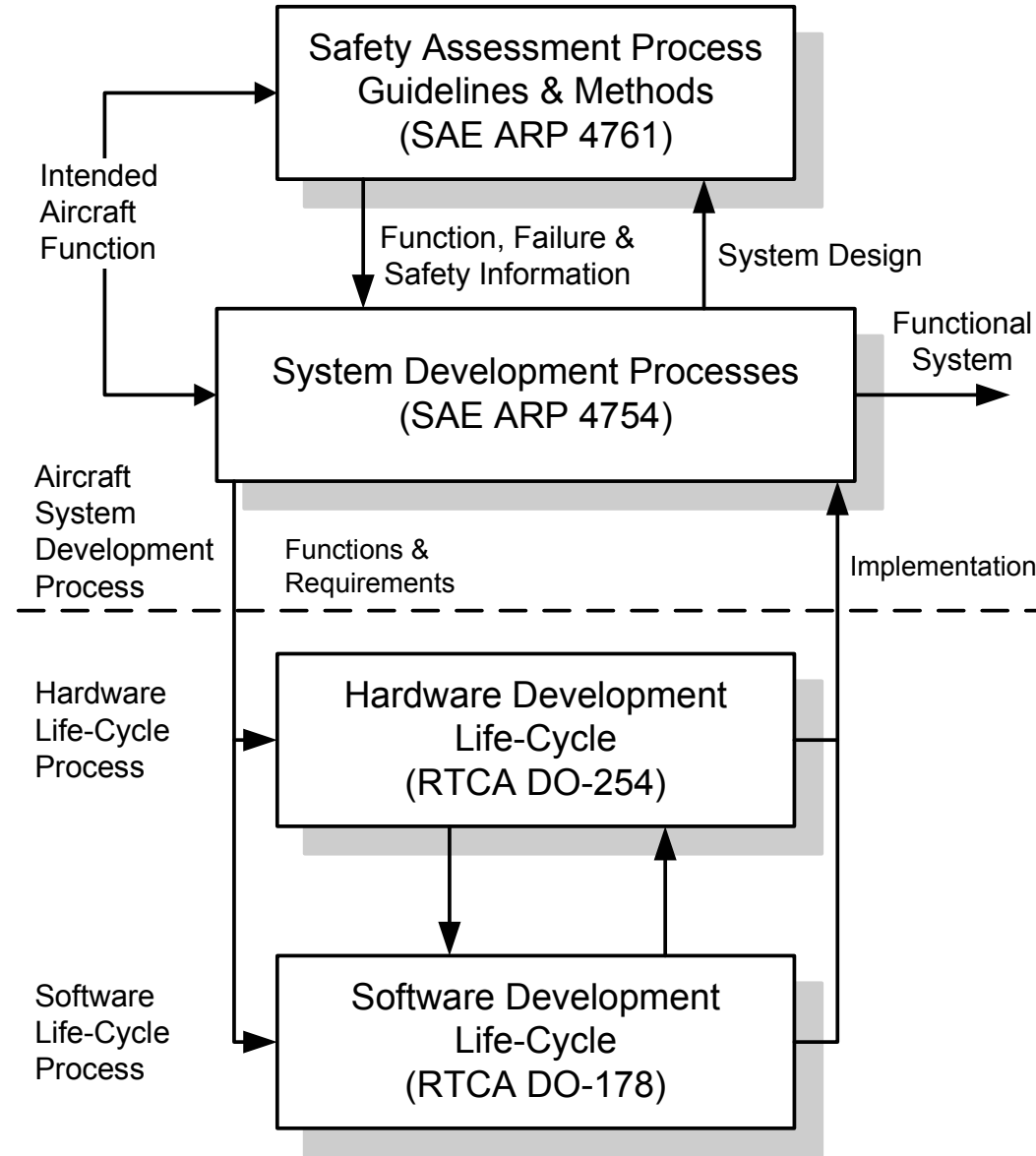
- Luftfahrtbranche ist anderen genannten Industriezweigen auch **ohne das Vorhandensein eines generischen Standards** um Jahre voraus



→ Warum diese **Vorreiterrolle**?

- Studien (z.B. EUROCONTROL) zeigen auf, dass:
 - die **Hälfte aller Unfälle** mit Flugzeugen auf **Design-Fehler** zurückzuführen ist
 - es in der Regel nicht ausreicht, die **Zuverlässigkeit und Sicherheit** von Systemen zu prüfen, sondern dass diese Eigenschaften schon frühzeitig detailliert **in das Design hineingeplant** werden müssen

→ **Luftfahrtnormen konnten so sogar teilweise in den Entstehungsprozess der IEC 61508 einfließen**

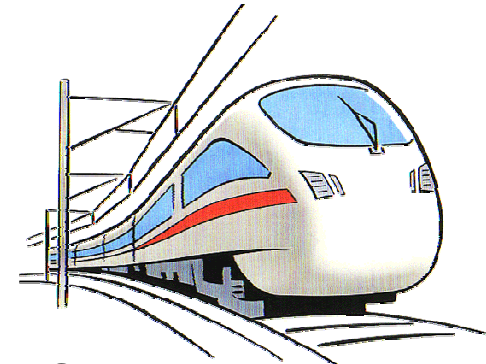


[aus: Koch, H., 2001]

System Development Process in der Luftfahrt

- SAE ARP 4761 (Safety Assessment Process Guidelines & Methods)
 - Systembezogene **Luftfahrt-Sicherheitsnorm**
 - Leitfäden und Methoden zur **Zertifizierung von zivilen Luftfahrzeugen** (konform FAR/JAR 25 1309)
 - Informationen zur **praktischen Anwendung** von Methoden zur Risikobeurteilung (Hinweise und Beispiele)
 - Fehlerbaumanalyse (FTA)
 - Zuverlässigkeit-Blockschaltbilder (RBD)
 - Markov-Analysen (MA)
 - Fehler-Möglichkeiten- und Effekt-Analysen (FMEA)
- DO-178 A(-C) (Software Development Life-Cycle)
 - Richtlinien zur **Zertifizierung** von Flugzeugsystemen und Luftfahrtgeräten mit **Schwerpunkt auf Aspekten der Software** in der Systementwicklung
 - Methoden und Werkzeuge, mit deren Hilfe sichere SW entwickelt werden kann, die den Anforderungen der Luftfahrtbehörden genügen
- DO-254 (Hardware Development Life-Cycle)
 - Strukturierte Vorgehensweise zur Entwicklung von **Hardware in Luftfahrzeugen**

- Eisenbahnbranche hat ihre branchenspezifischen CENELEC-Standards EN 5012x, wie es IEC 61508 vorschlägt, **basierend auf der Sicherheitsgrundnorm** formuliert
- sinngemäße Zuordnung der Standards
 - IEC 61508 (1) → EN 50126:
 - Gesamtheitlicher Überblick
 - Verfahren zur konsequenten Anwendung des RAMS-Managements
 - IEC 61508 (2) → EN 50129:
 - Anforderungen für Anerkennung und Zulassung von sicherheitsrelevanten elektronischen Systemen
 - IEC 61508 (3) → EN 50128:
 - Sichere Software in Bahnsystemen

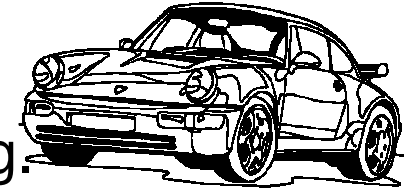


- obwohl mit der Inkraftsetzung der EN 50126 die grundlegende Forderung nach der Durchführung von Risikoanalysen in der Eisenbahntechnik verankert wurde...
- ...und in der EN 50129 Vorgehensweisen zur Durchführung von Risikoanalysen vorgeschlagen werden ist keine Vereinheitlichung in Sicht → **WARUM ?**

→ Formulierung der Vorgehensweise ist sehr **flexibel** („schwammig“)

- **Folgen der Flexibilität:**
 - beschriebene Methode konnte auf alle aufgetretenen Anwendungsfälle angepasst werden
 - es liess sich jedoch kein Standard-Vorgehen ableiten
 - sämtliche auf der Richtlinie basierende Risikoanalysen sind Unikate mit sehr geringem Überdeckungsgrad

Zukunftsweisende Innovationen sind zunehmend von komplexen Elektronik- und Softwaresystemen abhängig.



→ zertifizierbare Entwicklungsprozesse erforderlich, um die Zuverlässigkeit von sicherheitsrelevanten Systemen zu erhöhen

- Bestrebungen der Automobilbranche die Entwicklung von sicherheitsrelevanter Hard- und Software zu standardisieren
 - MISRA
 - Entwicklungsrichtlinien zur Entwicklung sicherer Software
 - FAKRA AK 16 Funktionssicherheit
 - Erarbeitung einer sektorspezifischen Adaption der IEC 61508, um die Vereinheitlichung von die Sicherheit beeinflussenden Entwicklungsaktivitäten voranzutreiben → ISO/WD 26262 (Entwurf)
 - Anforderungen an Softwareentwicklung
 - Übergreifende Aktivitäten (z.B. Zertifizierung von Entwicklungswerkzeugen)

- **Allgemeine Vorteile zertifizierbarer Entwicklungsprozesse**
 - eine **konsequente Anwendung strukturierter (zertifizierter) Methoden** zur Identifizierung von Störungen und resultierenden Gefährdungen hat einen erheblichen **positiven Einfluss auf Zuverlässigkeitseigenschaften von Systemen**
- **Vorteile der Nutzung existierender Standards, Normen oder Richtlinien**
 - **Doppelarbeit** kann **vermieden** werden, z.B. existentielle mehrfach hinterfragte Problemstellungen müssen nicht noch einmal gelöst werden
 - es kann vielmehr auf eine **erprobte Basis** aufgesetzt werden, und das **Hauptaugenmerk** kann **auf branchenspezifische Teilaspekte** gelenkt werden

- CENELEC-Standards

- der Vorteil des Aufbaus auf **vorhandene Basis** wurde **nicht konsequent genutzt**
- obwohl die IEC 61508 eine umfangreiche Definitionssammlung zur Verfügung stellt, definieren die CENELEC-Standards ihr Begriffe neu und nicht konsistent

- **EN 50126:**

- Validierung = „**Bestätigung** durch Überprüfung und objektiven Nachweis, **dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden**“
- Verifikation = „**Bestätigung** durch Überprüfung und objektiven Nachweis, **dass die festgelegten Anforderungen erfüllt wurden**“



- **EN 50129:**

- Validierung/Validation = „der auf Test und Analyse beruhende **Nachweis**, **dass das Produkt in allen Belangen seine spezifizierten Anforderungen erfüllt**“
- Verifikation = „die auf Analyse und Test beruhende **Feststellung** in jeder Phase des Lebenszyklus, **dass die Anforderungen der betrachteten Phase das Ergebnis der vorausgehenden Phase erfüllt** und dass das Ergebnis der betrachteten Phase die Anforderungen erfüllt“

Exemplarische Schwächen der CENELEC-Standards

Zusammenfassung (*im Hinblick auf ISO/WD 26262*)

- zertifizierbare Entwicklungsprozesse und Nachweisführungen erhöhen die Zuverlässigkeit von sicherheitsrelevanten Systemen
- **jede Norm** hat ihre **Fehler** und **Schwächen**
- grundsätzlich sollten jedoch zukünftige Normen **aus Missgeschicken** vorheriger Normungsgremien **lernen**
- denn **Erfahrungen** aus anderen Industriezweigen **bilden solide Basis**, um sinnvolle branchenspezifische Derivate der IEC abzuleiten

Ausblick

- **Vereinheitlichungsbestrebungen** werden vor allem vom dem Hintergrund der nachweislichen **Zuverlässigkeitssteigerung** vorangetrieben
- weg von „Allround“-Standards hin zu **branchenspezifischen Standards**, welche unterschiedliche Rahmenbedingungen gerecht werden

...Danke!

Technische Universität Braunschweig

Institut für Verkehrssicherheit
und Automatisierungstechnik **iva**