Erfahrungen mit den CENELEC-Normen

Probleme und Lösungsansätze

Dipl.-Math. Stefanie Schwartz, DLR

Überblick

- Projekt „Neue Konzepte für die Betriebsführung regionaler Strecken“
  - Zulassung und Sicherheitsbetrachtung
- Die CENELEC-Normen
  - DIN EN 50126-1
    - Inhalte
    - Lebenszyklus
- Ausgewählte Probleme und Lösungen aus den Bereichen
  - Begriffe
  - Inkonsistenzen
  - Umsetzung
  - Zuständigkeiten
  - Unterstützungsbedarf
- Fazit

„Neue Konzepte für die Betriebsführung regionaler Strecken“ – Zulassung und Sicherheitsbetrachtung

- Analyse der CENELEC-Normen
  - inhaltliche Vorgaben
  - Umsetzbarkeit
  - Verständlichkeit und Konsistenz
- Anwendung der CENELEC-Normen
  - Ortungssystem POSITRON
  - Lebenszyklusphasen vor der Entwicklung

Mehr als 100 Probleme

- Sammlung und Analyse von Methoden
  - zur Bearbeitung der Lebenszyklusaufgaben
- Vergleich von Methoden zur Sicherheitsbetrachtung und Zulassung
  - Schienenverkehr
  - Luftfahrt

CENELEC – Europäisches Komitee für Elektrotechnische Normung

Die CENELEC-Normen
für Bahnanwendungen

- **DIN EN 50126-1** (ehemals 50126)
  Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)
  Teil 1: Grundlegende Anforderungen und genereller Prozess

Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme:

- **DIN EN 50128**
  Software für Eisenbahnsteuerungs- und Überwachungssysteme
- **DIN EN 50129**
  Sicherheitsrelevante elektronische Systeme für Signaltechnik

- **DIN EN 50155**
  Elektronische Einrichtungen auf Schienenfahrzeugen

RAMS – Reliability, Availability, Maintainability, Safety
CENELEC – Europäisches Komitee für Elektrotechnische Normung

DIN EN 50126-1 (RAMS)
Inhalte

- Verfahren zur Anwendung eines Managements für Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)
- für alle Bahnanwendungen und für alle Systemebenen
- für Bahnunternehmen und Bahnindustrie

- Prozesse für die Spezifikation und den Nachweis von RAMS-Anforderungen
- risikobasierter Ansatz für Sicherheit

- Anforderungen sind generisch gehalten
- Definition von RAMS-Aufgaben und Verantwortlichkeiten
- keine Festlegung von RAMS-Zielen oder spezifischen Lösungen
- Definition eines Lebenszyklus

DIN EN 50126-1 (RAMS)
Lebenszyklus

1 Konzept
2 Systemdefinition und Anwendungsbedingungen
3 Risikoanalyse
4 Systemanforderungen
5 Zuteilung der Systemanforderungen
6 Entwicklung / Konstruktion und Implementierung
7 Fertigung
8 Installation / Montage
9 Systemvalidierung
10 Systemabnahme
11 Betrieb und Instandhaltung
14 Stilllegung und Entsorgung

12 Erfassung der Leistungsfähigkeit

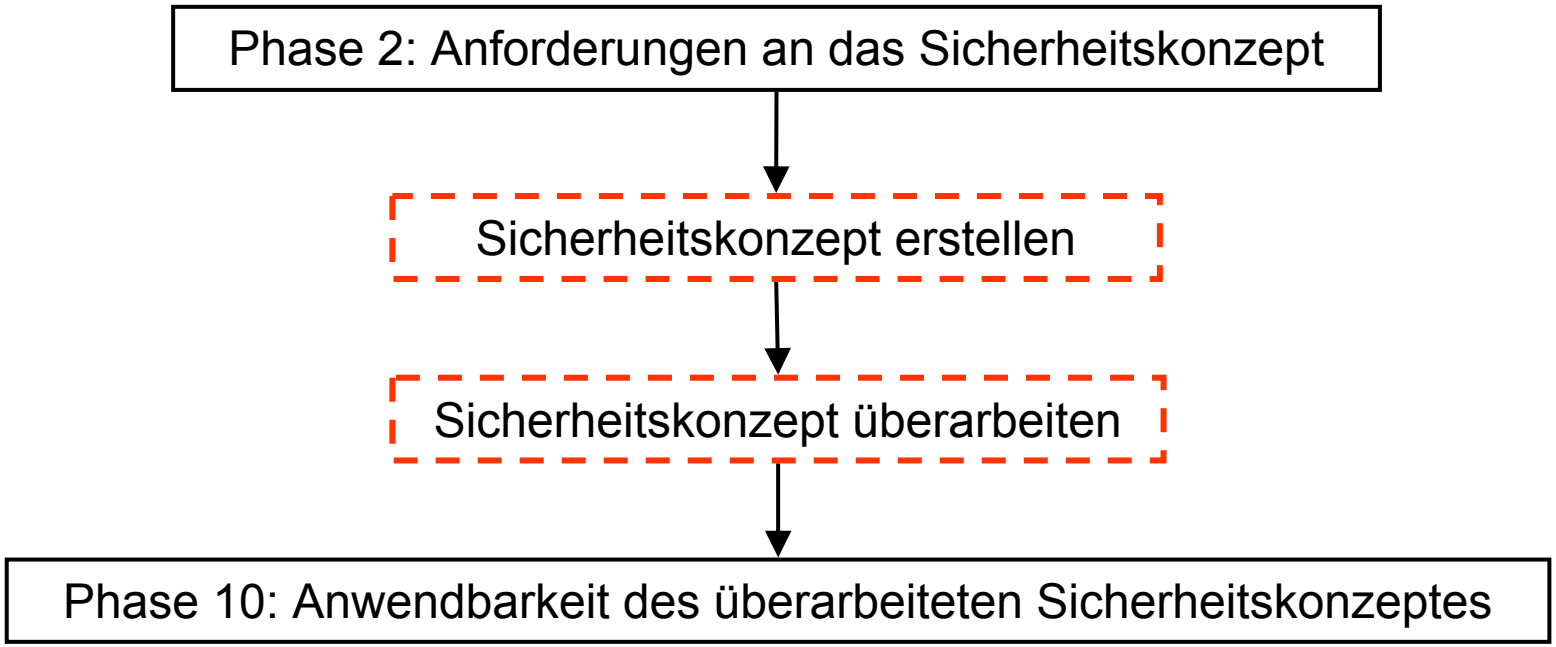
13 Änderungen und Nachrüstung

Ausgewählte Probleme und Lösungen: 1
Gefahr / Gefährdung

- 50126-1: Gefahr – „physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet“
- 50129: Gefährdung – „Bedingung, die zu einem Unfall führen kann“
- Unterschied?
  - im Sinne der Normen: kein Unterschied
  - englische Fassung der Normen hinzuziehen (beides *hazard)*
- Definitionen schwer greifbar. Problem wird deutlich beim Versuch, eine konkrete Gefahr zu beschreiben.
- Syntax aus dem Projekt Euro-Interlocking:
  - Möglichkeit einer *<Konsequenz (Unfallart)>* aufgrund einer *<Ursache>* unter Beteiligung einer *<Ressource>*.
  - Möglichkeit einer *Kollision mit einem anderen Eisenbahnfahrzeug* aufgrund eines *falschen Stellbefehls* an eine *Weiche*.

Ausgewählte Probleme und Lösungen: 2
Sicherheitskonzept (1)

- Was ist ein Sicherheitskonzept?
  - Definition fehlt, Inhaltsbeschreibung fehlt.



Ausgewählte Probleme und Lösungen: 2
Sicherheitskonzept (2)

- MbBO, §23: „Das Sicherheitskonzept muss die Ermittlung und Bewertung aller erkennbaren Sicherheitsrisiken nach Art, Häufigkeit und Auswirkungen beschreiben und die daraus abgeleiteten baulichen, technischen, betrieblichen und organisatorischen Sicherheitsmaßnahmen festlegen.“

Sicherheitsplan

Risikoanalyse

Gefahrenprotokoll

Sicherheitsnachweis

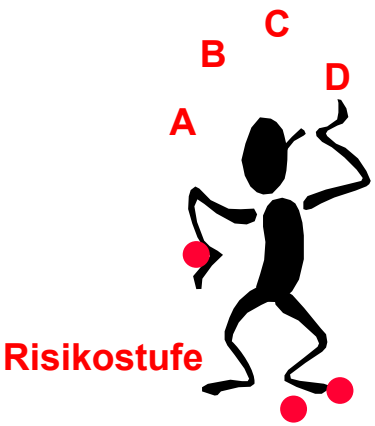
- Welchen Inhalt hat das Sicherheitskonzept?
- Eigenständiges Dokument „Sicherheitskonzept“ notwendig?

MbBO - Verordnung über den Bau und Betrieb der Magnetschwebebahnen

Ausgewählte Probleme und Lösungen: 3

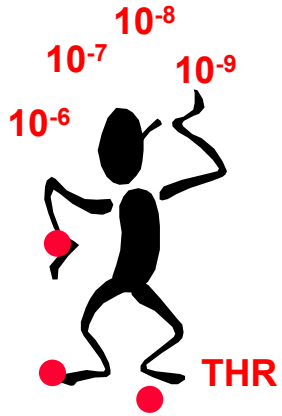
Risiko: qualitativ oder quantitativ

- 50126-1: Risikostufen
  - intolerabel
  - unerwünscht
  - tolerabel
  - vernachlässigbar
- 50129: tolerierbare Gefährdungsrate (THR)
- THR → SIL
  - $10^{-9} \leq THR < 10^{-8} \rightarrow$ SIL 4
  - $10^{-8} \leq THR < 10^{-7} \rightarrow$ SIL 3
  - $10^{-7} \leq THR < 10^{-6} \rightarrow$ SIL 2
  - $10^{-6} \leq THR < 10^{-5} \rightarrow$ SIL 1



qualitativ

quantitativ

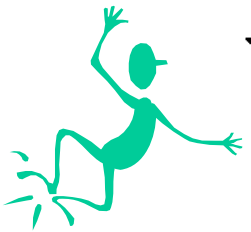


THR – Tolerable Hazard Rate

Ausgewählte Probleme und Lösungen: 4
Sicherheitsnachweise

- 50126-1:
  - ~~Grundsätzlicher System-Sicherheitsnachweis~~
  - ~~Anwendungssicherheitsnachweis~~

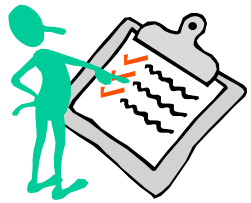
- 50129:
  - Generischer Produktsicherheitsnachweis
    - optional; für System, das in mehreren Anwendungen verwendet wird; unabhängig von der Anwendung; Cross Acceptance
  - Generischer Anwendungssicherheitsnachweis
    - optional; für System, das in mehreren Anwendungen derselben Klasse (z. B. Stellwerke) verwendet wird; Cross Acceptance
  - Spezifischer Anwendungssicherheitsnachweis
    - verpflichtend, wenn das System in Betrieb gehen soll; baut ggf. auf anderen Sicherheitsnachweisen auf



Ausgewählte Probleme und Lösungen: 5
pro forma Dokumentation

- CENELEC-konforme Dokumentation nachträglich erstellt
  - Gründe: Zeitdruck, mangelnde Motivation
  - lästiges Übel, zu hoher Aufwand

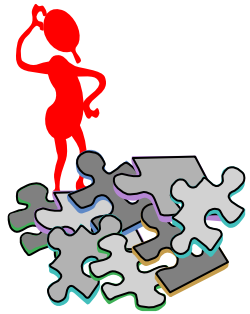
- nachträgliche Dokumentation, pro forma, ist uneffektiv!
- Ist zugehörige Aufgabe notwendig / sinnvoll
  - zeitnah und mit möglichst wenig Aufwand dokumentieren
- Ist Aufgabe (an dieser Stelle im Lebenszyklus) nicht von Bedeutung
  - Aufgabe verschieben oder ganz entfernen
  - Abstimmung mit Gutachter und Genehmigungsbehörde!



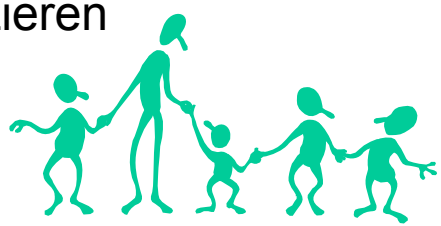
- Motivation: von jeder Aufgabe / Dokument wissen, warum wichtig
  - Schulung oder Prozess begleitende Dokumentation

Ausgewählte Probleme und Lösungen: 6
Das Bahnunternehmen

- Bahnunternehmen: „Die Gesellschaft mit der Gesamtverantwortung für den Betrieb eines Bahnsystems gegenüber einer Aufsichtsbehörde.“
- Richtlinie 91/440/EWG: Trennung von Netz und Verkehrsleistung
  - Verantwortung für den Betrieb eines Bahnsystems in der Regel aufgeteilt
  - „das Bahnunternehmen“ gibt es nicht mehr

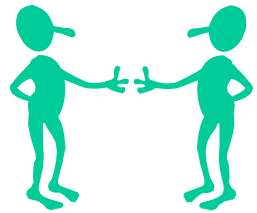


- CENELEC-Normen berücksichtigen Trennung nicht
  - Probleme bzgl. Zuständigkeiten, insbes. bei Verlagerung von Funktionen (Strecke → Fahrzeug)
- Für die Praxis: Kunde muss alle Beteiligten identifizieren und Zuständigkeiten frühzeitig festlegen
- CENELEC-Normen: Trennung berücksichtigen



Ausgewählte Probleme und Lösungen: 7
CENELEC-Prozess ohne Kunden?

- Initiative: Hersteller
  - 1 Produkt für mehrere Kunden (generisch)
  - vorgefertigte Lösungen (Preisfrage)
- 50126-1: Kunde, Hersteller, Genehmigungsbehörde
- Kunde hat besondere Rolle in den frühen CENELEC-Phasen (1-4):
  - Konzept
  - Anwendungsbedingungen
  - tolerierbares Risiko (THR)
- Hersteller
  - Erfahrung nutzen
  - Aufgaben des Kunden übernehmen
  - Sichtweise des Kunden vertreten (z.B. 1 Mitarbeiter des Herstellers)
  - Kunden später in den Prozess mit einbinden



Ausgewählte Probleme und Lösungen: 8
Unterstützungsbedarf

- z.B. Kunde: Konzept, Anwendungsbedingungen, tolerierbares Risiko
  - mangelnde Kenntnis der CENELEC-Normen
  - Zeitmangel
  - Überforderung
  - Kunde nimmt seine Aufgaben nicht wahr
- Vorlagen
  - Deckblatt, Struktur, relevante Normen-Anforderungen
    - Überforderung
- Erläuterungen zu den Normen, Leitfaden
- genaue Anweisungen
- Beispiele
- Schulung
- Lehrbuch

Ausgewählte Probleme und Lösungen: 8
Leitfaden zur Anwendung der CENELEC-Normen

- großer Bedarf

- Der Leitfaden sollte:
  - Begriffe erläutern
  - Inkonsistenzen bereinigen
  - Einstieg in die CENELEC-Normen erleichtern
  - Hilfestellung bei der Prozessdurchführung geben
  - Zusammenhänge aufzeigen
    - zwischen den Normen
    - zwischen Phasen, Aufgaben, Dokumenten
  - als Nachschlagewerk dienen
- Lehrbuch über eine CENELEC-konforme Entwicklung zum Selbststudium

Erfahrungen mit den CENELEC-Normen
Fazit

- CENELEC-Normen verpflichtend für Bahnunternehmen und Bahnindustrie
- Anwendung problematisch
  - Inkonsistenzen
  - Verständnis
  - Umsetzbarkeit
- Unterstützungsbedarf
- Projekt „Neue Konzepte für die Betriebsführung regionaler Strecken“
  - zeigt Probleme auf
  - gibt Lösungsansätze
- Bedarf
  - Leitfaden
  - Lehrbuch

Vielen Dank für Ihre Aufmerksamkeit

- Dipl.-Math. Stefanie Schwartz

  Deutsches Zentrum für Luft- und Raumfahrt e.V.
  Institut für Verkehrssystemtechnik

  Lilienthalplatz 7
  38108 Braunschweig

  Tel: +49 (0) 531 295 3444
  Fax: +49 (0) 531 295 3402
  E-Mail: stefanie.schwartz@dlr.de
  Internet: www.dlr.de/ts