SCHIG

Schieneninfrastruktur-Dienstleistungsgesellschaft mbH

CSM
Divergenzen bei der Anwendung

Verpflichtende Anwendung laut TSI

- TSI SRT
  - Für alternative Lösungen für sichere Bereiche in Tunneln
  - Für den Betrieb neuer Fahrzeuge in bestehenden Tunneln
- TSI LOC&PAS
  - Wachsamkeitskontrolle
  - Dynamisches Fahrverhalten (aktive Systeme)
  - Sicherheitsanforderungen an Bremsen
  - Fahrgastalarm
  - Außentüren, Tür-Notöffnung
- TSI WAG
  - Bremse
- TSI CCS
  - für Sicherheit allgemein gültig

Allgemeine Anwendungspflicht

- Signifikante technische, betriebliche und organisatorische Änderungen des Eisenbahnsystems

- Organisatorische Änderungen mit Auswirkungen auf Betriebs- oder Instandhaltungsprozesse

- Signifikanzprüfung
  - auf Basis notifizierter nationaler Vorschriften
  - auf Basis der Entscheidungsfaktoren „Sicherheitsauswirkung“ (Folgen von Ausfällen), „innovative Elemente“, „Komplexität“, „Überwachbarkeit“, „Umkehrbarkeit“ und „additive Wirkung“

Abweichungen bei der Signifikanzprüfung

- Die Signifikanzprüfung ist nicht durch eine Sicherheitsbewertungsstelle zu prüfen.
- Die Prüfung erfolgt stichprobenartig bei der Prüfung des Sicherheitsmanagementsystems.
- Unter der CSM-Verordnung 352/2009 wurde die Signifikanz unnötig häufig festgestellt – die Sicherheitsbewertung war intern und kostete „nichts“.
- Seit der CSM-Verordnung 402/2013 wird die Signifikant restriktiver gehandhabt – die Sicherheitsbewertung ist extern und kostet etwas.
- Problem 1:
  Die Erfahrungen aus der Signifikanzprüfung von 352/2009 sind nicht 1:1 verwendbar.

Verwendung unterschiedlicher Begriffe

- Problem 2: Es kursieren unterschiedliche Begriffe.

- Beispiel „Sicherheit“
  - CSM: „Das Nichtvorhandensein von unvertretbaren Schadensrisiken“
  - EN 50126: „Das Nichtvorhandensein eines unzulässigen Schadensrisikos“
  - EN 50129: „Freisein von nicht akzeptierbaren Risiken eines Schadens“
  - EN 50128: „Freiheit von nicht-akzeptablen Risiken für Personenschäden“
  - prEN 50126-1: „freedom from unacceptable risk to human health or to the environment“

Unterschiedliche Lösungswege

- Die CSM erlaubt unterschiedliche Grundsätze der Risikoakzeptanz.
  - Verwendung anerkannter Regelwerke
  - Analyse der Ähnlichkeit mit Referenzsystemen
  - Explizite Risikoabschätzung

- Problem 3: Die Qualität der Referenzsysteme legt die Messlatte für zukünftige Entwicklungen fest.

- „schlechte Referenzsysteme“ → niedriges Sicherheitsniveau prolongiert
- „übertriebene Referenzsysteme“ → überteuerte Systeme entstehen

Wahl von Referenzsystemen

- Bei der Wahl von Referenzsystemen können viele Fehler passieren.
- Die Wahl eines Referenzsystems ist einwandfrei zu begründen. Ohne das kommen ungeeignete Referenzsysteme zum Einsatz.
- Die Eigenschaften eines Referenzsystems passen nicht zum eigenen System, wie zB
  - ungleiche Betriebsbedingungen
  - unterschiedliche Verkehrszahlen
  - unterschiedliche Anwendung
- Wenn das nicht angepasst wird, kommen fehlerhafte Ergebnisse heraus.

Änderungen durch 2015/1136

- Führen Funktionsausfälle eines technischen Systems zu Gefährdungen, gelten … die folgenden harmonisierten Entwurfsziele für diese Ausfälle:
  a) Ist bei einem Ausfall davon auszugehen, dass dieser unmittelbar zu einem katastrophalen Unfall führt, muss das damit verbundene Risiko nicht weiter reduziert werden, wenn es nachweislich höchst unwahrscheinlich ist, dass es zu einem Ausfall der Funktion kommt.

‚katastrophaler Unfall': ein Unfall, bei dem in der Regel eine große Zahl von Personen Schaden erleidet und mehrere Menschen zu Tode kommen

‚höchst unwahrscheinlich': das Auftreten eines Ausfalls mit einer Ausfallrate von höchstens 10^{-9} je Betriebsstunde

Änderungen durch 2015/1136

- Führen Funktionsausfälle eines technischen Systems zu Gefährdungen, gelten … die folgenden harmonisierten Entwurfsziele für diese Ausfälle:
  b) Ist bei einem Ausfall davon auszugehen, dass dieser unmittelbar zu einem kritischen Unfall führt, muss das damit verbundene Risiko nicht weiter reduziert werden, wenn es nachweislich unwahrscheinlich ist, dass es zu einem Ausfall der Funktion kommt.

‚kritischer Unfall': ein Unfall, bei dem in der Regel eine sehr geringe Zahl von Personen Schaden erleidet und mindestens ein Mensch zu Tode kommt

‚unwahrscheinlich': das Auftreten eines Ausfalls mit einer Ausfallrate von höchstens 10^{-7} je Betriebsstunde

Probleme bei den Definitionen

- ‚katastrophaler Unfall': ein Unfall, bei dem in der Regel eine große Zahl von Personen Schaden erleidet und mehrere Menschen zu Tode kommen
- Problem 4: Wie viele sind das? Es ergibt sich eine uneinheitliche Bewertung der „katastrophalen Folge".

- ‚kritischer Unfall': ein Unfall, bei dem in der Regel eine sehr geringe Zahl von Personen Schaden erleidet und mindestens ein Mensch zu Tode kommt

- Problem 5: „Mindestens" ein Mensch kommt zu Tode. „Mindestens" ist eine völlig ungeeignete Definition.
- Zwei oder drei Tote nähern sich schon „mehreren Toten", das Sicherheitsniveau sinkt hier durch den Auslegungsspielraum der Formulierung ab.

- Problem 6: Die Interpretation der Zwischenstufen wird uneinheitlich.

Risikoakzeptanzkriterium

- Die Beispielsammlung der ERA zur CSM-Verordnung versuchte das für die Verordnung 352/2009 zu korrigieren.

- Sie verweist einige Male auf die Stufen aus der EN 50126:
  - katastrophal: Unfalltote und/oder zahlreiche Schwerverletzte und/oder schwere Umweltschäden
  - kritisch: einzelner Unfalltoter und/oder Schwerverletzter und/oder nennenswerte Umweltschäden
  - marginal: kleinere Verletzung und/oder nennenswerte Bedrohung der Umwelt
  - unbedeutend: mögliche, geringfügige Verletzung

Risikoakzeptanzkriterium

- Problem 7: Durch die neue Kategorie „kritischer Ereignisse“ ändert sich die Einstufung. Darstellung aus der Beispielsammlung des EBA zur SIRF:

Unfallhäufigkeit	Schwere des Unfalls			
häufig (10^{-4} pro Stunde)	intolerabel	intolerabel	intolerabel	intolerabel
wahrscheinlich (10^{-5} pro Stunde)	intolerabel	intolerabel	intolerabel	intolerabel
gelegentlich (10^{-6} pro Stunde)	tolerabel	intolerabel	intolerabel	intolerabel
selten (10^{-7} pro Stunde)	tolerabel	tolerabel	intolerabel	intolerabel
unwahrscheinlich (10^{-8} pro Stunde)	tolerabel	tolerabel	tolerabel	intolerabel
unvorstellbar (10^{-9} pro Stunde)	tolerabel	tolerabel	tolerabel	RAC-TS
	unbedeutend	marginal	kritisch	katastrophal

Abbildung -2: RAC-TS

- Für „kritisch“ war hier 10^{-8} h^{-1} nötig, neuerdings laut CSM 10^{-7} h^{-1}.

Verwendung von Analysenmethoden

- Problem 8: unpassende Analysemethoden

- Am elegantesten sind die Anforderungen an eine Analyse in prEN 50126-4 beschrieben:

1. Die verwendete Methode muss gut belegt sein, eine wissenschaftliche Basis haben, die Wiederholbarkeit sicherstellen und sowohl Kreativität als auch Systematik ermöglichen.
2. Die Analysetechnik muss zur Problemstellung passen.
3. Wenn eine Analysetechnik allein nicht ausreichend ist, ist ein Kombination aus geeigneten Techniken zu wählen.
4. Die Wahl der Analysetechniken ist zu begründen. Die Eignung der Werkzeuge zur Analyse ist zu zeigen.

- Auch wenn diese Anforderungen für manche Probleme zu umfassend sind, die Eignung ist sicherzustellen.

Natürliche Barrieren zur Minderung von Folgen

- Alle expliziten Risikokriterien befassen sich mit Fehlern, die direkt zu zB katastrophalen Folgen führen.

- „Barrieren“ können die Eintrittswahrscheinlichkeit der Folgen reduzieren, zB:
  - wenig Verkehrsaufkommen
  - Hilfe durch andere Fahrgäste
  - große Reserven in der Infrastruktur oder aus dem Betrieb

- In diesem Ausmaß kann die Sicherheitsanforderung reduziert werden.
- zB 10 % Wahrscheinlichkeit für katastrophale Folgen: SIL 3 statt SIL 4.

- Problem 9: Fehler in der ERA-Beispielsammlung, vielfach falsch abgeschrieben

Reduktion der Sicherheitsanforderung durch Barrieren

Eintritt katastrophaler Folgen	Wahrscheinlichkeit infolge Barrieren	Gefährdungsrate	Sicherheitsan-forderungsstufe
Unmittelbar	1	10^{-9}	4
	0,5	$2 \cdot 10^{-9}$	4
	0,2	$5 \cdot 10^{-9}$	4
Wahrscheinlich	0,1	10^{-8}	3
Gelegentlich	0,01	10^{-7}	2
Selten	0,001	10^{-6}	1
Unwahrscheinlich	0,0001	10^{-5}	-

Sicherheitsrichtlinie Fahrzeug

- Das Eisenbahnbundesamt hat die SIRF als CSM-Realisierung für Schienenfahrzeuge festgelegt.
- Für länderübergreifende Zulassungen ist sie kaum umgänglich.
- Die SIRF wird wegen ihrer Einfachheit gerne auch außerhalb Deutschlands verwendet.
- Problem 10: Die SIRF liefert teilweise sehr konservative Ergebnisse.

Unterschiede in der Risikoeinstufung

- Die SIRF-Formel zur Ermittlung der Sicherheitsanforderungsstufe liefert Ergebnisse mit folgender Entsprechung:
  - 1 Toter = 10 Schwerverletzte = 100 Leichtverletzte
- Der Einfluss der Eintrittswahrscheinlichkeit eines Ereignisses ist geringer als bei anderen Verfahren.
- Zwischen
  - nahezu zwangsläufiges Eintreten bei hoher Exposition der Personen gegenüber der Gefährdung und keinerlei Vermeidungsmöglichkeit und
  - nahezu ausgeschlossenes Eintreten bei kurzer Exposition der Personen gegenüber der Gefährdung mit einiger Vermeidungsmöglichkeit

  liegen nur zwei Sicherheitsanforderungsstufen.

Auswirkungen – neue EN 50128 für Fahrzeuge

- Mit der SIRF kommen teilweise höhere Sicherheitsanforderungen zu Stande, als mit CSM oder EN 50126.
- Das erhöht die Entwicklungskosten für deutsche Anwendungen.
- Die Fahrzeughersteller in Deutschland versuchen das über die reduzierte Anwendung von Normen auszugleichen.
- Die Softwarenorm EN 50128:2011 wird in Deutschland für Fahrzeuge abgelehnt.
- Eine eigene Fahrzeug-Softwarenorm soll entstehen.
- Problem 11: Zukünftig könnte SIL x nicht mehr in allen Fällen die selbe Bedeutung haben.

Danke für die Aufmerksamkeit!