

Sicherheitsnormen im Umbruch

Revision der EN 5012X Suite

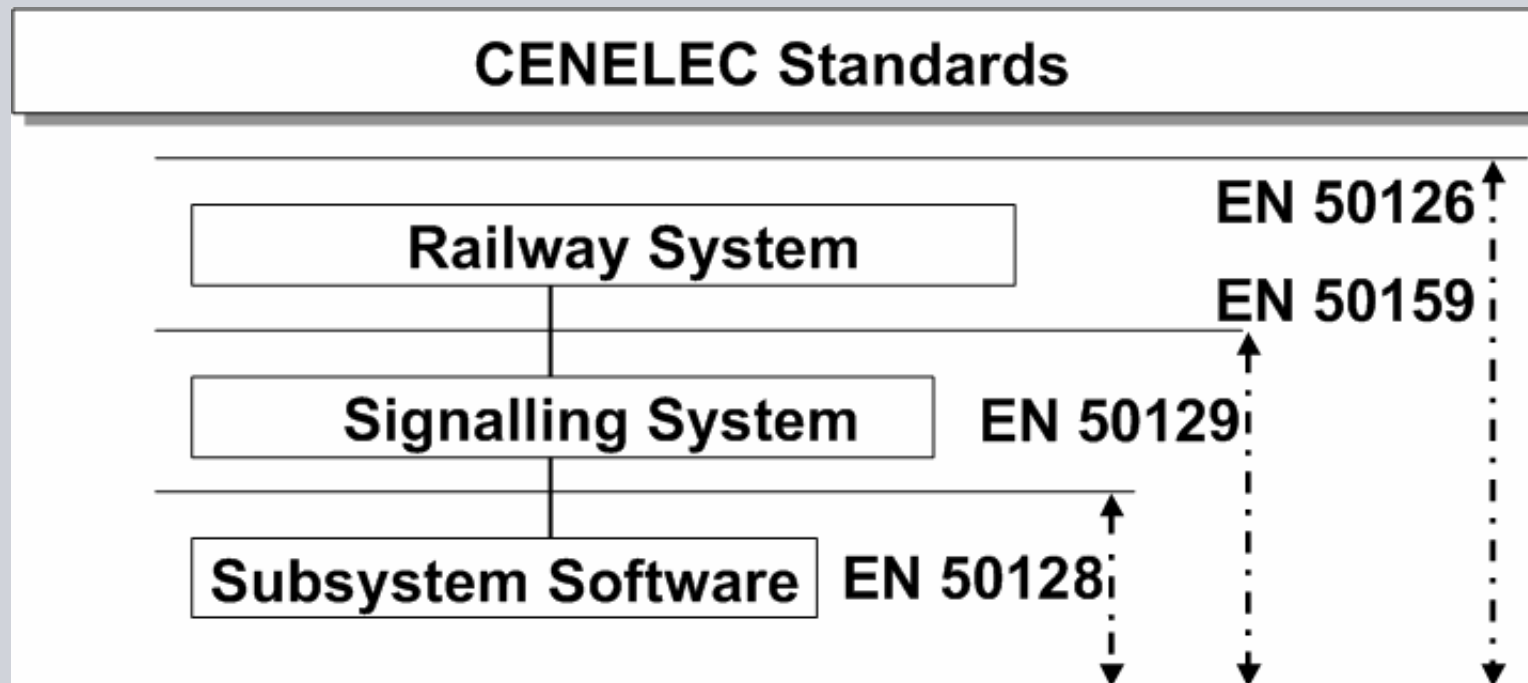
Stephan Griebel
Siemens AG
Industry Sector, Mobility Division
01. Dezember 2008

Überblick

- Revision der EN 5012X-Suite
- Relevante Änderungen bei der IEC 61508
- Ausblick

Revision der EN 5012X-Suite

Status quo der funktionalen Sicherheitsnormen für die Eisenbahntechnik bei CENELEC



Revision der EN 5012X-Suite

Hintergründe zur Revision der EN 5012X

Aus der Resolution des europäischen CENELEC-Gremiums "Railway Applications" TC9X:

With respect to problems in applying the signalling safety standards for rolling stock and fixed installations, TC9X resolves to set up a Survey Group to investigate common requirements and special requirements for safety systems ... with a view to having a coherent approach across all application fields ... Therefore the Survey Group should identify common areas of applicability and identify issues that need to be added to apply to non-signalling subsystems

...



Gründe für Neustrukturierung der EN 5012X-Suite

- Notwendigkeit, ein Gesamtsicherheitskonzept einschließlich der Fahrzeuge und Infrastruktur zu entwerfen. Dieses hat Auswirkungen auf alle drei Geschäftsgebiete (Rail Automation, Electrification, Rolling Stock)
- Widerspiegelung des Stands der Technik (normaler Vorgang alle 5 - 7 Jahre)

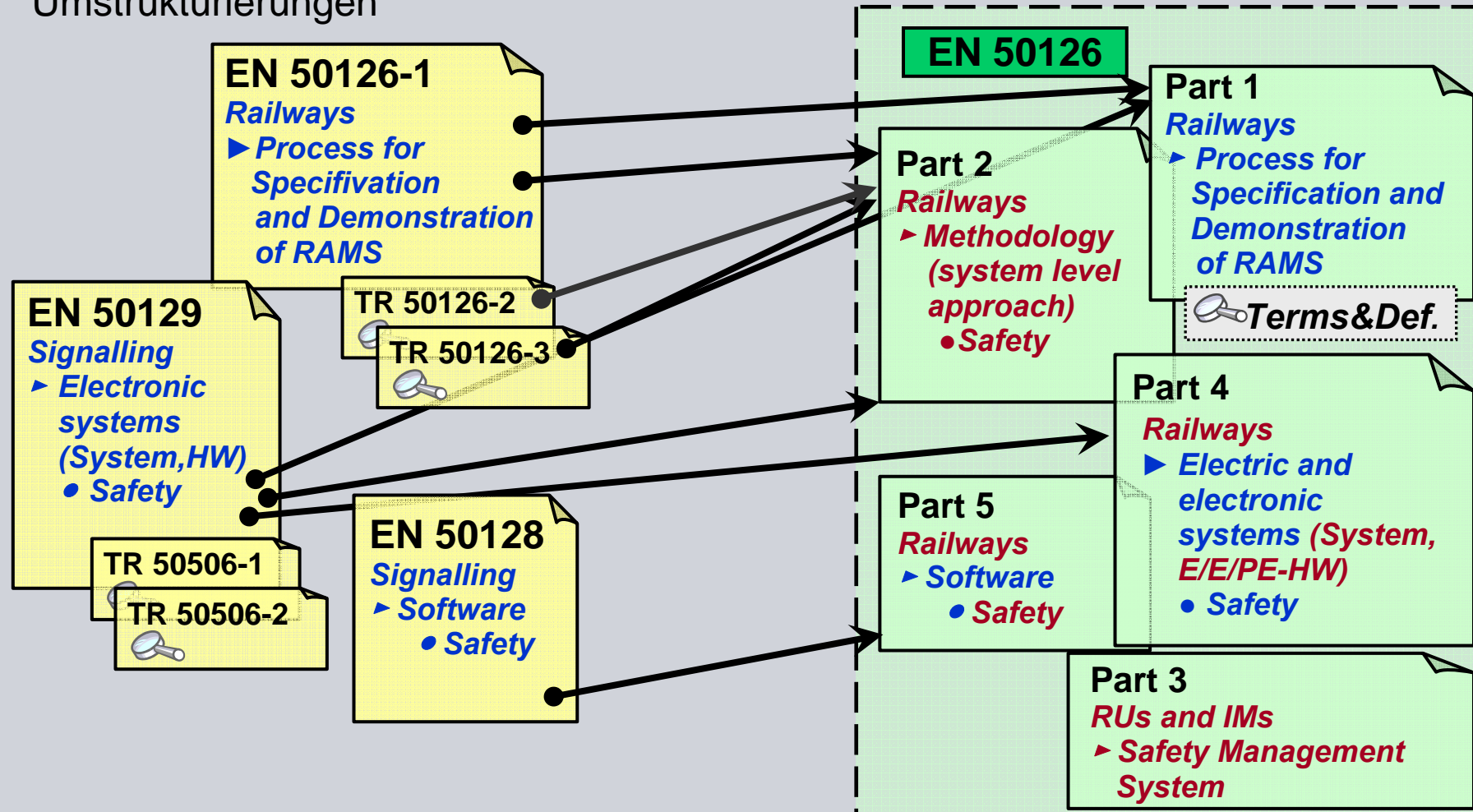
Revision der EN 5012X-Suite

Spezifische Handlungsfelder

- Spezifizieren funktionaler Sicherheitsanforderungen und Ableiten der Anforderungen an Subsysteme aus Sicherheitsvorgaben
- Anwenden des Safety Integrity Concept, einschließlich der Anwendungsvoraussetzungen bei Mechatronik, Fahrzeugen, ortsfesten Anlagen – Aufklären von Missverständnissen bezüglich der Safety Integrity Level (SIL)
- Praktikable und wirtschaftliche Methoden für das Kombinieren probabilistischer und deterministischer Argumente beim Nachweis ausreichender Sicherheit
- Inkonsistente Begriffe/Definitionen (z. B. safety critical, safety function) führen zu unterschiedlichem Vorgehen, reduzierter Vergleichbarkeit, Missverständnissen und Zusatzkosten
- Vertiefen der Aspekte von Betrieb und Instandhaltung sowie der Nachrüstung und Änderungen

Revision der EN 5012X-Suite

Umstrukturierungen



Revision der EN 5012X-Suite

EN 50126 - Railway applications: The Specification and Demonstration of RAMS Objective and contents according to Revision Outline Specifications (ROS)

Part 1: Generic RAMS process (Largely based on EN 50126-1)

- Terms and Definitions
- RAMS process based on System Lifecycle and Safety Case

Part 2: Systems Approach to Safety

- Methods of risk analysis and hazard control
- SIL and Allocation of Safety Requirements

Part 3: Safety Management System for RU/IM

Part 4: Functional Safety -Electric and electronic systems (Based on EN 50129)

- Generic system (e. g. SIL and architecture) and hardware aspects of E/E/EP functions
- Applicable to all application fields of Railways

Part 5: Functional Safety -Software (Based on EN 50128)

- Development and operation of safety relevant software within all application fields of railway

Revision der EN 5012X-Suite

Organisatorisches

Organisation der europäischen Arbeitsgruppe bei CENELEC (TC9X/WG14)

- 80 Personen
- 3 Revision Groups

Zeitplan

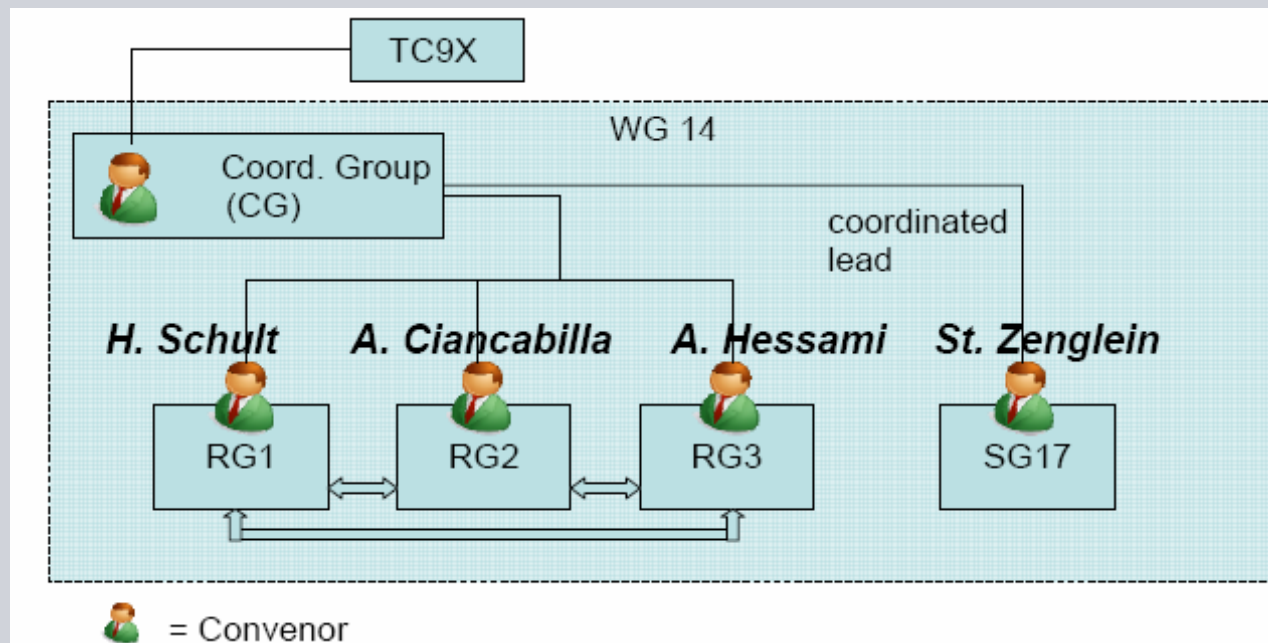
- Start im Mai 2008
- Bis Herbst 2008 Festlegung der Table of Contents
- Ab Herbst 2008 Start der inhaltlichen Arbeiten
- Abschluss der inhaltlichen Arbeiten in frühestens 2 Jahren
- Formale Verabschiedung in frühestens 3 Jahren

Revision der EN 5012X-Suite

Verantwortlichkeiten

- RG 1 → Teil 1 (EN 50126, EN 50129)
- RG 2 → Teil 2 (Neu, EN 50129)
- RG 3 → Teil 4 und 5 (EN 50128, EN 50129)

RG = Revision Group
 SG = Survey Group



Revision der EN 5012X-Suite

Arbeitsstände aus den Revision Groups RG1 und RG2

RG1

Part 1: Generic RAMS process (Largely based on EN 50126-1)

- Terms and Definitions (ROS)
- RAMS process based on system lifecycle
- Safety Case

RG2

Part 2: Systems Approach to Safety

- Risk based approach
- Relation to Common Safety Methods (ERA)
- Methods of risk analysis and hazard control
- Comparison with IEC 61508
- SIL and Allocation of Safety Requirements

Revision der EN 5012X-Suite

Arbeitsstände aus der Revision Group RG3

RG3

Part 4: Functional Safety -Electric and electronic systems (Based on EN 50129)

- Generic system (e. g. SIL and architecture) and hardware aspects of E/E/EP functions
- Applicable to all application fields of Railways

Part 5: Functional Safety -Software (Based on EN 50128)

- Development and operation of safety relevant software within all application fields of railway.

Überblick

- Revision der EN 5012X-Suite
- Relevante Änderung bei der IEC 61508
- Ausblick

Relevante Änderung bei der IEC 61508

Gegenwärtiger Zustand der Revision der IEC 61508

IEC 61508 is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i. e. E/E/PE safety related systems.

The standard is generic in that it applies to these systems irrespective of their application.

Ursprünglicher Zeitplan für Teil 1 – 7:

- Entwurf für nationale Komitees (CDV). **12/2007**
- Endentwurf für nationale Komitees (FDIS): **03/2009**
- Publikation der revidierten IEC 61508: **07/2009**

Aktueller Stand:

- CDVs an nationale Komitees : **3. Quartal/2008**
- Veröffentlichung der IEC 61508 2nd edition: **06/2010**

Relevante Änderung bei der IEC 61508

Notwendigkeit der Kohärenz von EN 5012X und IEC 61508

- Die Nutzung von Systemen/Produkten aus anderen Industriebereichen erfordert eine Anlehnung der Konzepte aus EN 5012X und IEC 61508, um auseinanderlaufende Sicherheitsauffassungen zu vermeiden und Zulassungsaufwände zu minimieren.
- Das “Dresden agreement“ zwischen CLC und IEC führt zu einer späteren Übernahme der EN5012X-Suite in das IEC-Normenwerk.
- Die Einführung zur EN 50129 erläutert:
“Diese Norm und EN 50126 basieren auf dem Systemlebenszyklus und sind in Einklang mit EN 61508-1, an deren Stelle die Normen EN 50126 / EN 50128 / EN 50129 treten, wenn es sich um Telekommunikations-, Signal- und Datenverarbeitungssysteme der Eisenbahnen handelt. Wenn die Anforderungen dieser Normen erfüllt werden, ist eine weitere Bewertung der Übereinstimmung mit EN 61508-1 nicht erforderlich.“

Relevante Änderung bei der IEC 61508

Einige Änderungen mit möglichem Bezug zu EN 5012X

- Definitions (average frequency, systematic capability, ...)
- Synthesis of elements to achieve the required systematic capability
- Safety manual for “compliant items“ to define requirements for suppliers of products who claim compliance with IEC 61508
- Personal competence: It is proposed that personal competence will be a normative requirement (informative in the current version).

Relevante Änderung bei der IEC 61508

Begriff der “Systematic capability”

Systematic capability

measure (expressed on a scale of SIL 1 to SIL 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.



- Das Konzept wird im Prinzip schon seitens der Hersteller angewandt.
- Im Gegensatz zum SIL, der sich auf Funktionen bezieht, wird die SIL-capability einzelnen Komponenten (elements) zugeschrieben.

Relevante Änderung bei der IEC 61508

Neue Definitionen in “SIL-Tabellen“

Safety integrity level	Average frequency of dangerous failure of the safety function (hr ⁻¹)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE See Notes 2 to 6 below for details on interpreting this table.	

Safety integrity levels: target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

- Anzuwenden auf High Demand und Continuous Mode
- Bisher: dangerous failure of the safety function
- Neu: “average“ and “frequency“

Überblick

- Revision der EN 5012X-Suite
- Relevante Änderung bei der IEC 61508
- Ausblick

Ausblick

- Konsolidierung der inhaltlichen Struktur bis zum Frühjahr 2009, anschließend Start der inhaltlichen Ausgestaltung
- Spiegelung der Arbeiten der CENELEC WG14 bei der DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE) im AK 351.0.2 RAMS



Offenes Fenster für konstruktive Beiträge über DKE-Gremien

Vielen Dank für Ihre Aufmerksamkeit!

Stephan Griebel
Siemens AG
Industry Sector, Mobility Division
01. Dezember 2008