Die CENELEC-Normen zur Funktionalen Sicherheit

The CENELEC-Standards regarding Functional Safety

Jens Braband, Bernd-E. Brehmke, Stephan Griebel,
Harald Peters, Karl-Heinz Suwe

EDITION SIGNAL + DRAHT

Eurail press

EDITION
SIGNAL + DRAHT

Die CENELEC-Normen zur Funktionalen Sicherheit

The CENELEC-Standards regarding Functional Safety

Prof. Dr. rer. nat. Jens Braband
Dipl.-Ing. Bernd-E. Brehmke
Dipl.-Math. Stephan Griebel
Dipl.-Ing. Harald Peters
Dipl.-Ing. Karl-Heinz Suwe

Eurail press

Inhaltsverzeichnis / *Contents*

Vorwort

Spätestens seit ihrer formalen Verabschiedung (beginnend mit der EN 50126 im Jahr 1999) haben die CENELEC-Normen zur Funktionalen Sicherheit (EN 50126, EN 50128, EN 50129, EN 50159) einen bemerkenswerten Siegeszug angetreten, der formal seinen Höhepunkt mit der Übernahme aller dieser Normen als IEC-Normen (endend mit der EN 50129 in 2007) finden wird. Danach werden diese Normen in ihrem Geltungsbereich die einzigen internationalen Normen darstellen, die im europäischen Wirtschaftsraum quasi verpflichtend angewendet werden müssen, aber bereits heute weltweit freiwillig aus Gründen der Effizienz und Harmonisierung anerkannt sind.

Im krassen Gegensatz zur Bedeutung der Normen stehen die wenigen professionellen Aus- und Weiterbildungsangebote zu diesem Thema, obwohl die EN 50126 selbst Kompetenznachweise verlangt. Dies stellt auch der SAMNET Synthesis Report vom Februar 2006 fest: „It is shame that the CENELEC reference system is not yet subject to formalised training. It is a trade reference system that is *learned on the job* in companies".

Diese Situation hat zu zahlreichen Schwierigkeiten und Missverständnissen aufgrund der weit verbreiteten Kenntnislücken geführt, was durch die Notwendigkeit zur Erarbeitung der beiden Application Guides zur EN 50126 sowie EN 50129 mit Lehrbuchcharakter bestätigt wird.

Diese Schwäche wurde in der Siemens AG, Transportation Systems, frühzeitig erkannt und deshalb bereits seit 1997 durch die Siemens Rail Automation Academy ein Kurs „Einführung in die CENELEC-Normen" angeboten, den seitdem mehr als 1.500 Mitarbeiter und Kunden besucht haben. Mittlerweile wurde daraus ein komplettes Kursprogramm mit insgesamt 12 Schulungsmodulen entwickelt. Im Jahr 2005 wurde insbesondere aufgrund der

Foreword

At the very least since being formally approved (beginning with EN 50126 in 1999), the CENELEC standards on functional safety (EN 50126, EN 50128, EN 50129, EN 50159) have been a remarkable success story, a story that will culminate from the formal point of view with the adoption of all these standards as IEC standards (concluding with EN 50129 in 2007). Thereafter, they will be the only standards in that field whose application is essentially mandatory in the European economic area, while indeed already being recognised on a voluntary basis worldwide in the interests of efficiency and harmonisation.

Out of all proportion to the importance of these standards is the fact that little is available in the way of education and training aids on the subject, even though EN 50126 itself calls for proof of competency. This was also referred to in the SAMNET Synthesis Report of February 2006: "It is a shame that the CENELEC reference system is not yet subject to formalised training. It is a trade reference system that is learned on the job in companies."

This situation has often led to difficulties and misunderstandings because of the widespread gaps in knowledge, as underscored by the need to draw up the two Application Guides for EN 50126 and EN 50129, which serve as textbooks.

These shortcomings were recognised at an early stage at Siemens AG, Transportation Systems, and thus since as far back as 1997 the Siemens Rail Automation Academy has been offering an introductory course to the CENELEC standards that has been taken to date by over 1,500 staff and clients. In the meantime, the course has developed into a full study programme with a total of 12 training modules. In 2005, notably in light of the strong demand from abroad, and building on the introductory course, a computer-based

starken internationalen Nachfrage auf Grundlage des Einführungskurses ein Computer Based Training (CBT) entwickelt, das die Basis für das auf der beiliegenden CD enthaltene CBT bildet.

Mit diesem Ansatz wird vom Verlag Eurailpress und der Fachzeitschrift SIGNAL+DRAHT ein zusätzlicher, neuer Weg eröffnet. Neben die Fachbücher der bekannten „Edition SIGNAL+ DRAHT“ tritt die CD-ROM für ein individuelles und interaktives Lernen in deutscher und englischer Sprache. Da sich die Fachzeitschrift SIGNAL+DRAHT häufig und eingehend mit den neuen Normen befasst hat, war es möglich, eine große Zahl von Fachbeiträgen aus den letzten 10 Jahren als Vertiefung und Ergänzung einzubringen. Diese gedruckte Einführung mit einer Auswahl an Fachliteratur sowie das Computer Based Training mit den ergänzenden Fachaufsätzen auf der CD-ROM bilden eine Einheit, die es Mitarbeitern von Firmen, Mitarbeitern von Betreibern (Technik und Betrieb), Mitarbeitern von Aufsichtsbehörden (Technik und Betrieb) sowie Mitarbeitern von Ingenieurbüros/Consulting-Firmen sowie anerkannten Sachverständigen als auch Mitarbeitern von Forschungseinrichtungen und Studenten gestattet, sich in die Materie einzuarbeiten und sich kompetent zu machen. Aber auch als Nachschlagewerk und zum Refreshing der Kenntnisse sind die Unterlagen hervorragend geeignet.

Möge dieses umfassende Werk eine hilfreiche Unterstützung für Ihre tägliche Arbeit mit den CENELEC-Normen sein.

training (CBT) module was developed, and this forms the basis for the CBT contained on the enclosed CD.

In taking this approach, publishers Eurailpress and the specialist journal SIGNAL+DRAHT are opening up a new additional channel. Alongside the reference books in the well-known “Edition SIGNAL+DRAHT” series, this CD-ROM aims to support interactive self-tuition in English as well as German. SIGNAL+DRAHT has frequently covered the new standards in depth, and so it has been possible to deepen and broaden the material on the CD-ROM by including a large number of specialist articles from the last 10 years. This print introduction, with a selection of specialist literature, and the Computer Based Training and supplementary articles on the CD-ROM together form a unified whole that will enable company employees, staff of operators (systems and operations), officials at regulatory agencies (systems and operations), staff of engineering bureaux and consultancies, as well as experts, researchers and students, to familiarise themselves with the subject matter and hone their competency. In addition, the material is eminently suited as a reference work and for knowledge refreshment.

We hope that this comprehensive work will provide highly useful support to you in your day-to-day work with CENELEC standards.

Einführung

Inhaltsverzeichnis

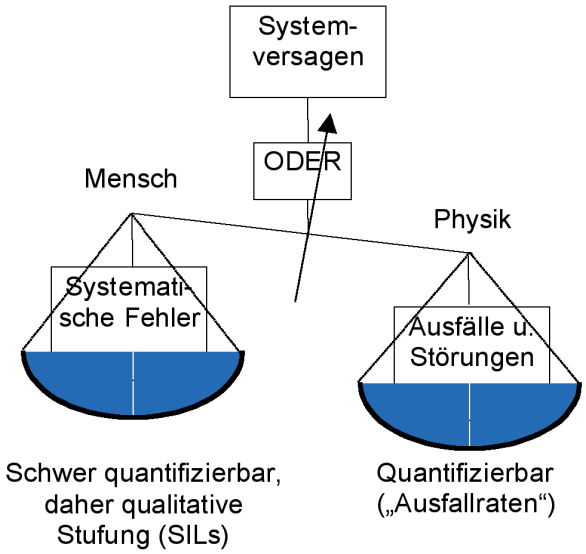

Bild 5: SIL-Konzept

beruht (*Bild 5*). Um dieses Ziel zu erreichen, wird das Konzept der Sicherheitsanforderungsstufen (SIL) verwendet.

3.2.5 Safety Integrity Level (SIL)

Durch die Zuordnung zu Sicherheitsanforderungsstufen soll ein Gleichgewicht zwischen den Maßnahmen zur Vermeidung systematischer Fehler und denen zur Beherrschung zufälliger Ausfälle hergestellt werden, da es anerkannter Stand der Technik ist, dass die Sicherheit gegen systematische Fehler nicht quantifizierbar ist (zumindest nicht bei Anwendungen mit einem hohen Sicherheitsniveau). Die detaillierten Anforderungen für die Erfüllung eines SIL sind in den Normen EN 50128 und 50129 zusammengestellt. Der quantitative Zusammenhang nach EN 50129 wird in *Tabelle 1* dargestellt.

Tolerierbare Gefährdungsrate THR pro Stunde und pro Funktion	**Sicherheitsanforderungsstufe (SIL)**
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Tabelle 1: Zuordnung von THR zu SIL nach EN 50129

Die Tatsache, dass systematische Fehler nicht quantifizierbar sind und daher stattdessen mithilfe der SIL die erforderlichen Maßnahmen gegen systematische Fehler festgelegt werden müssen, bedeutet jedoch nicht, dass solche Fehler nicht entstehen und Gefährdungen daraus nicht auftreten können. Man muss sich bewusst machen, dass das Sicherheitsziel nach den normativen Bestimmungen nicht quantitativ unterteilt und der Wert für zufällige Ausfälle nicht reduziert wird, obwohl ein erheblicher Prozentsatz des tolerablen Sicherheitsrisikos durch

4.3.1 Qualitätsmanagementbericht

Die Qualität des Systems, Teilsystems oder der Komponente muss durch ein entsprechendes Qualitätsmanagementsystem über den gesamten Lebenszyklus gewährleistet werden. Der dokumentierte Nachweis muss im Qualitätsmanagementbericht erfolgen.

Der Zweck des Qualitätsmanagementsystems ist es, die Häufigkeit menschlicher Fehler zu minimieren und damit das Risiko von systematischen Fehlern in dem System, Teilsystem oder der Komponente zu reduzieren.

Ein wichtiger Aspekt dabei ist die Wirksamkeit von Prüfungen, insbesondere Reviews und Audits.

Prüfungen

Grundsätzlich wird jedes Ergebnis einer Phase gegen seine Anforderungen geprüft (verifiziert, in der Regel durch Reviews) sowie jede Implementierungsstufe gegen die Anforderungen (in der Regel durch Analyse und Test). Das Endprodukt wird gegen die Anforderungen des spezifischen Einsatzfalls geprüft (validiert). Zusätzlich wird der Gesamtprozess begutachtet (häufig unterstützt durch Audits), wobei insbesondere die Einsatzfähigkeit festzustellen ist. In *Bild 12* wird der grundsätzliche Zusammenhang verdeutlicht.

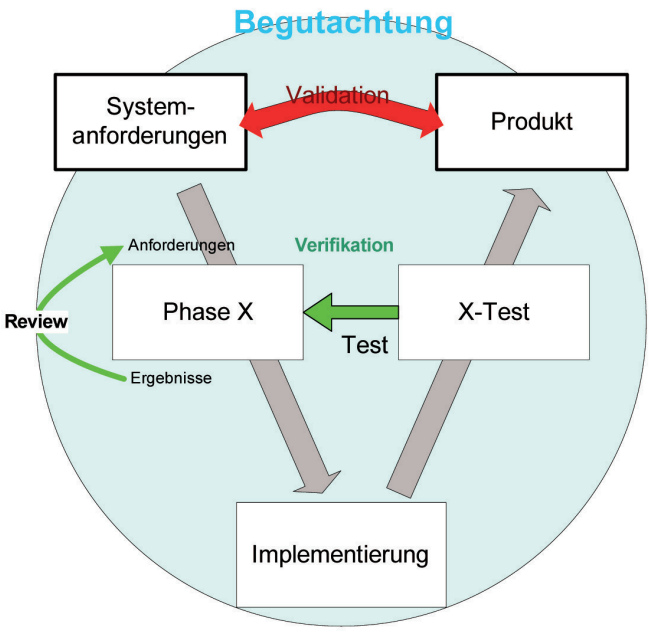

Bild 12: Grundsätzliche Prüfschritte im CENELEC-Lebenszyklus

Im Detail bedeutet dies bei den CENELEC-Normen:

Verifikation:
Analyse und Testen, um festzustellen, ob das Ausgangsprodukt jeder Phase des Lebenszyklus die Anforderungen aus der vorhergehenden Phase erfüllt.

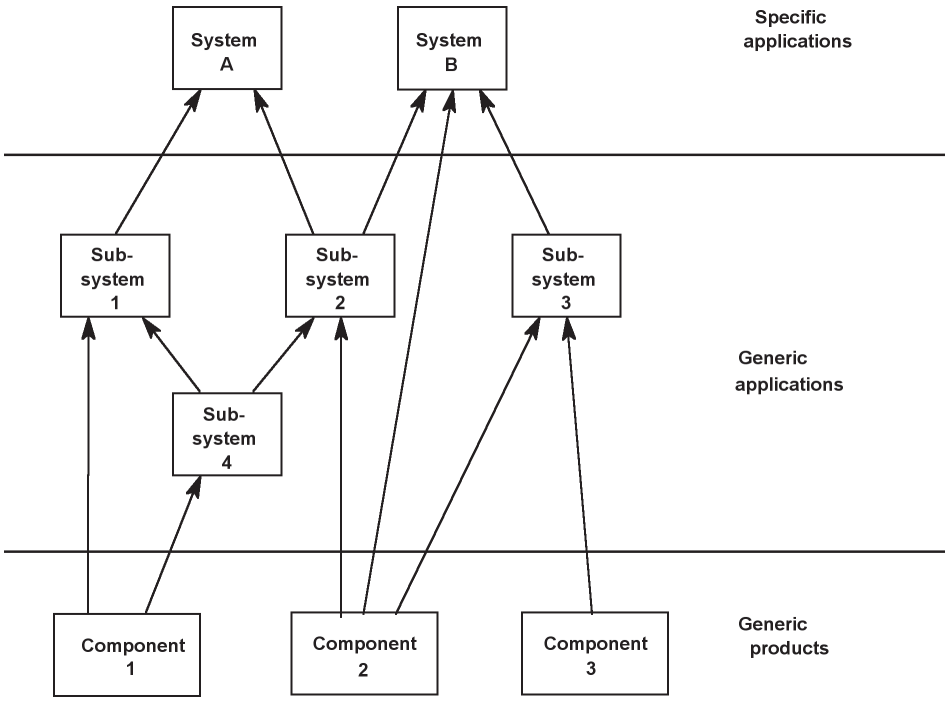

Figure 10: Hierarchy of safety cases in line with EN 50129

4.3 Structure and Content of Safety Cases

In accordance with EN 50129, a safety case must not only deal with technical aspects but must always comprise three components (*Figure 11*):

– demonstration of quality management (Quality Management (QM) Report),
– demonstration of safety management (Safety Management (SM) Report),
– demonstration of technical safety (Technical Safety (TS) Report).

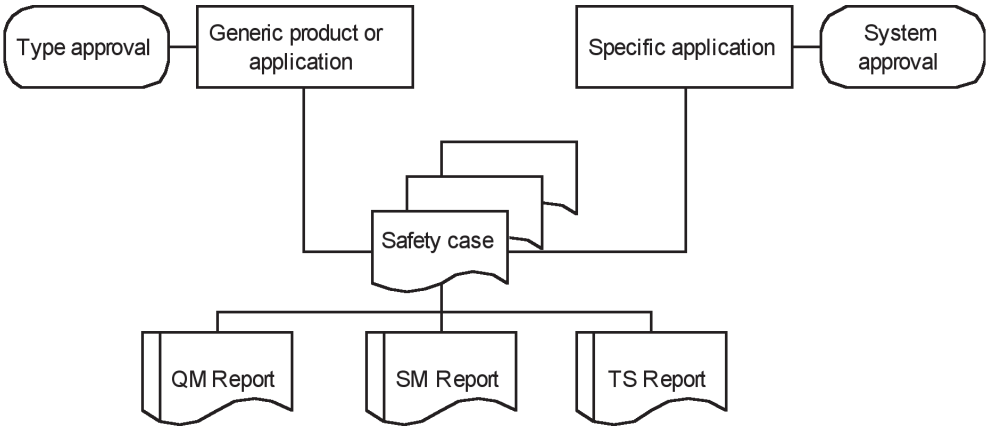

Figure 11: Safety case structure in line with EN 50129

Fachbeiträge/*Technical Papers*

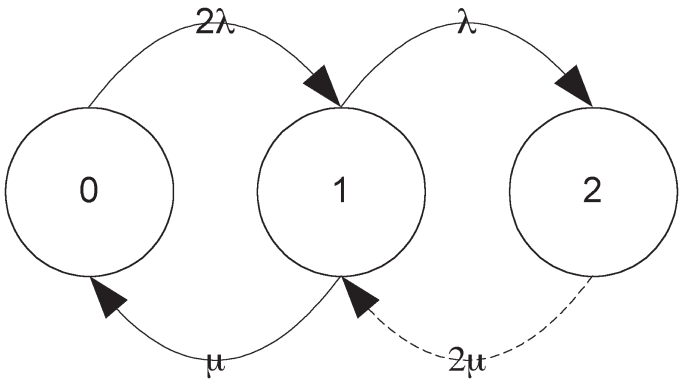

Figure 4: Markov model for a 1002 system

an overvoltage detector in applications where an undetected overvoltage can lead to a hazard. If the integrity requirement is high, two ore more overvoltage detectors might be required. A corresponding Markov model reveals that the resulting failure is extremely time-dependent. Here the hazard rate at the end of the lifetime of the unit which contains the protective devices should be taken as a conservative result for the safety analysis.

Rule 6: Only engineers who could theoretically perform all the calculations manually should use a tool. A tool is no remedy for a lack of qualification.

Another problem also relating to the definition of the failure rate is that a failure rate can only be defined meaningfully for systems which have not failed before. Thus, a Markov model must be stopped when the failure state is reached, i.e. failure states are absorbing states. *Figure 4* shows a Markov model for a simple 1-out-of-2 (1002) system. The states are labelled in accordance with the number of failed components (2 is the failure state). If a failure rate needs to be calculated, 2 should be an absorbing state, i. e. this state is never left. For availability calculations, repair must be considered and in such a model the transition from state 2 to state 1 (the dashed line in *Figure 4*) should be shown.

This slight difference has a big effect when it comes to the calculation of failure rates, as can be seen in *Figure 5*. In the absorbing model the failure rate converges to a non-zero constant;

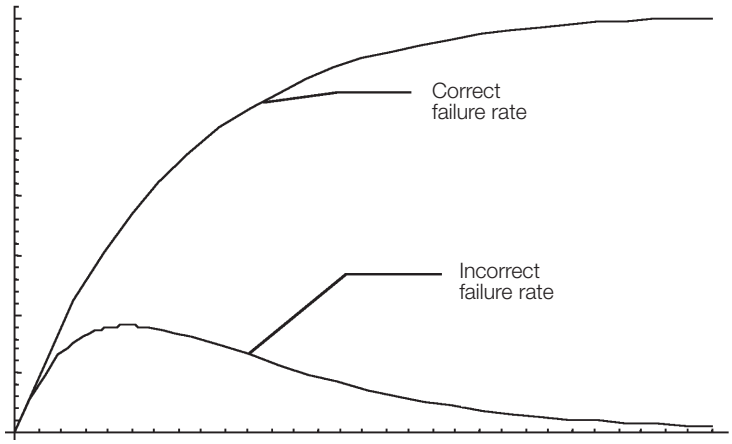

Figure 5: Effects of an incorrect calculation of a failure rate

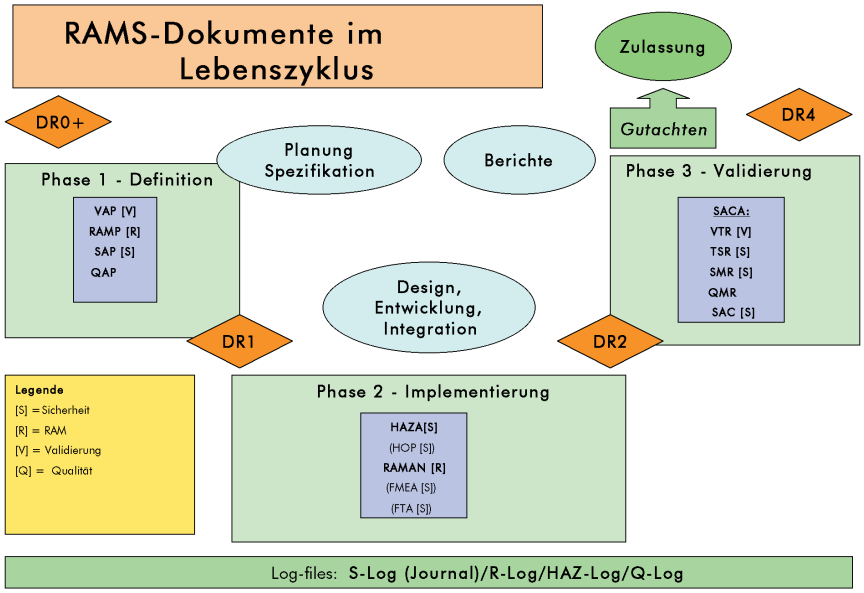

Bild 1: RAMS-Dokumente im Produktlebenszyklus

Bei den aus den englischen Begriffen abgeleiteten Acronymen bedeuten hierbei:

- VAP: Validierungs-Plan (Validation Plan),
- RAMP: RAM-Plan (RAM Plan),
- SAP: Sicherheitsplan (Safety Plan),
- QAP: Qualitätssicherungsplan (Quality Assurance Plan),
- HAZA: Gefährdungsanalyse (Hazard Analysis),
- HOP: Methode zur Gefährdungsanalyse (Hazard and Operability Study),
- RAMAN: Zuverlässigkeits- und Verfügbarkeitsanalyse (RAM Analysis),
- FMEA: Ausfall-Effekt-Analyse (Failure Mode and Effects Analysis),
- FTA: Fehlerbaum-Analyse (Fault Tree Analysis);
- SACA: Sicherheitsnachweis (Safety Case), bestehend aus: VTR: Validierungstestbericht (Validation Test Report), TSR: Technischer Sicherheitsbericht (Technical Safety Report), SMR: Sicherheits-Management-Bericht (Safety Management Report), QMR: Qualitäts-Management-Bericht (Quality Management Report), SAC: Sicherheitsbezogene Anwendungsrichtlinien (Safety Application Conditions),
- S-LOG: Sicherheits-Logbuch (Safety Log),
- R-LOG: Zuverlässigkeits- und Verfügbarkeits-Logbuch (RAM Log),
- HAZ-LOG: Gefährdungs-Logbuch (Hazard Log),
- Q-LOG: Qualitäts-Logbuch (Quality Log).

Auf oberster Ebene (hier nicht explizit als RAMS-Dokumente gekennzeichnet) stehen als Leitdokumente eines gesamten Projekts der Dokumentationsplan, der Assessmentplan und das Transferdokument. Der Dokumentationsplan bildet die integrierende Klammer. In ihm sind sämtliche im Projekt entstehenden und referenzierten Dokumente aufgelistet. Der Assessmentplan, das Pendant zum Prüfhandbuch nach der Mü 8004, legt in Absprache mit dem EBA fest, welche Dokumente zur Begutachtung herangezogen werden und durch welche Instanz (zum Beispiel EBA oder Prüfleitstelle) diese erfolgen wird. Das Transferdokument definiert im Detail den