Artikel für Signal + Draht Mai 2012

INESS: Toolunterstützung bei der Erstellung des Sicherheitsnachweises

Carsten Trog, Geltmar von Buxhoeveden

Das EU-Förderprojekt INESS (Integrated European Signalling System) hatte das Ziel, Techniken und Prozesse der europäischen Signaltechnik zu harmonisieren und dadurch Kosten für Bahnen und Hersteller zu senken. Der vorliegende Artikel beschreibt die Ergebnisse des INESS-Arbeitspakets „Safety Case Process". In diesem von Funkwerk IT und der TU Braunschweig geleiteten Arbeitspaket wurden der Sicherheitsnachweisprozess analysiert, die Spezifikation für eine Tool-Unterstützung erarbeitet und Prototypen des Tools implementiert.

Das Projekt INESS

Das Projekt INESS wurde 2006 initiiert und 2008 mit Unterstützung von EU-Fördergeldern gestartet. Im INESS-Projekt arbeiteten mehr als 30 Eisenbahninfrastrukturbetreiber, Hersteller und spezialisierte Universitäten aus Deutschland, England, Italien, den Niederlanden, Österreich, Schweden und Spanien gemeinsam daran, die Beschaffungskosten für Stellwerke durch klare und einheitliche Spezifikationen über Grenzen hinweg zu verringern. Mit dem 31.03.2012 wurde INESS abgeschlossen.

Im Rahmen von INESS wurden die folgenden Arbeitspakete (Workstreams) bearbeitet:

- Workstream A: Project Managment
  Dieser formale Workstream umfasste die Projektleitung von INESS.

- Workstream B: Business Case
  Unter Leitung der DB Netz AG wurde eine Analyse der Wertschöpfungskette vorgenommen, um die Einsparpotenziale der Harmonisierung herauszuarbeiten.

- Workstream C: System Design
  Unter Leitung von Bombardier (Deutschland) wurde RailML als ein geeignetes Datenformat zur Kommunikation zwischen Betreibern und Herstellern identifiziert. Um auch Stellwerke abbilden zu können, wurde eine Erweiterungsliste für RailML erarbeitet.

- Workstream D: Functional Requirements

In Erweiterung zu Eurointerlocking wurden die funktionalen Anforderungen von 12 europäischen Bahnen an Stellwerke analysiert und ein gemeinsamer Kern herausgearbeitet. Die Leitung hatte ProRail (Niederlande).

- Workstream E: Functional Architecture
  Hier standen die Identifizierung und Beschreibung der Kommunikationsschnittstellen zwischen den Stellwerkskomponenten im Vordergrund. Dieser Workstream wurde von Trafikverket (Schweden) geleitet.

- Workstream F: Testing and Commissioning
  Unter der Leitung von Network Rail (Großbritannien) wurde ein “best practice” Handbuch erstellt.

- Workstream G: Safety Case Process
  Funkwerk und die TU Braunschweig analysierten den Sicherheitsnachweisprozess und deckten Probleme im Prozess auf. Es wurden Lösungsansätze für eine Harmonisierung erarbeitet und ein Tool zur Unterstützung der Erstellung des Sicherheitsnachweises spezifiziert und entwickelt.

- Workstream H: Dissemination and Exploitation
  Die UIC leitete und organisierte die Veröffentlichungen und die Verbreitung der Ergebnisse dieses Projektes.

Dieser Artikel beschreibt die Ergebnisse des Workstreams G: Safety Case Process. Die Ergebnisse der übrigen Workstreams sind u. a. im Internet unter INESS.eu zu finden.

Zielsetzung des Workstreams G

Zielsetzung des Workstreams G war die Erarbeitung von Lösungsvorschlägen, um die Aufwände für den Sicherheitsnachweis zu senken. Durch die Analyse des bestehenden Verfahrens und der Entwicklung von Support-Tools sollten unnötige oder redundante Prozesse beim Sicherheitsnachweisprozess vermieden und Geld und Zeit eingespart werden.

Gründe für die Harmonisierung des Safety Case Processes

In der CENELEC Norm EN 50129 ist grundsätzlich die Erstellung des Safety Cases einer Entwicklung beschrieben und europaweit gültig. Obwohl bereits seit Mitte der 90er Jahre in Anwendung, bestehen noch immer viele Unsicherheiten und auch Unwissenheit hinsichtlich der Anwendung der Norm und es gibt weiterhin viele nationale und herstellerspezifische Lösungen und Werkzeuge. Dies erschwert das Verständnis der

umfangreichen Dokumentation eines Sicherheitsnachweises und erhöht den Aufwand bei Cross-Acceptance. Insbesondere der Aufwand zur Anerkennung der Technik über Ländergrenzen hinweg ist bisher in vielen Fällen unverhältnismäßig schwierig. Zwischenzeitlich wurden Guidelines zur Interpretation der Norm erstellt, die aber kaum Besserung brachten.

Vorgehensweise im Workstream G

Am Workstream G waren Fachleute von 10 INESS-Projektpartnern beteiligt. Im ersten Schritt wurden Interviews bei den Partnern durchgeführt, um Schwierigkeiten und Verbesserungspotenzial bei der Erstellung von Sicherheitsnachweisen zu erfassen. Zu Beginn wurde festgelegt, dass die CENELEC-Normen 50126/28/29 nicht geändert werden sollen.

Die Ergebnisse wurden in Workshops präsentiert und strukturiert. Die folgenden wesentlichen Felder für gewünschte Verbesserungen wurden in der Expertengruppe identifiziert:

- Dokumentzentrische Funktionen
    - Verfolgbarkeit von Dokumenten,
    - Verfolgbarkeit von Änderungen,
    - Suchen von Dokumenten und in Dokumenten,
    - Hinzufügen zusätzlicher Klassifizierungsmerkmale zu Dokumenten („Tagging“),
    - (automatische) Versionierung von Dokumenten,
    - Verknüpfen von Dokumenten aus unterschiedlichen Quellen.

- Prozessorientierte Funktionen
    - (automatischer) Abnahme- /Ablehnungsprozess,
    - (automatisches) Umbenennen / Verschieben von Dokumenten nach Abschluss eines Prozesses,
    - Informationen über Dokumentänderungen,
    - Übersichten über den Status von Dokumenten.

Die gewünschten Verbesserungen wurden zunächst in Ziele aufgeteilt, die innerhalb der dreijährigen Projektlaufzeit umsetzbar erschienen (short term goals) und Ziele, die darüber hinaus erkennbar sind, aber im Rahmen des Projektes nicht umsetzbar waren (long term goals). Der in Abbildung 1 aufgeführte Projektablauf gibt einen Überblick über die von Workstream G durchgeführten Tätigkeiten, deren jeweiliger Abschluss in einem Bericht mündete (Deliverable).

Gewünschte Verbesserungen

Das größte Problem bei der Erstellung und Bearbeitung des Sicherheitsnachweises ist es, die Übersicht über die Dokumente und deren Vollständigkeit zu bekommen und diese zu pflegen. Dies gilt insbesondere für Änderungen. Von der Vereinheitlichung der Struktur des Sicherheitsnachweis-Prozesses erwarteten alle Beteiligten eine höhere Verständlichkeit und Transparenz.

Die in CENELEC vorgegebene Entwicklungsmethode des V-Modells beschreibt eine phasenbezogene Entwicklung. Es wird beispielsweise davon ausgegangen, dass mit der Architektur des Systems erst nach der Fertigstellung und Abnahme der Spezifikation begonnen wird. In der Praxis werden allerdings mehrere Phasen parallel bearbeitet und häufig erst kurz vor der Inbetriebnahme abgeschlossen. Zudem ist die Entwicklung häufig in mehrere Unter- und Teilprojekte mit eigenen „V“ unterteilt. Die vollständige Dokumentation nach V-Modell steht daher erst beim Abschluss des Projektes zur Verfügung. Dieser Sachverhalt war bei der Entwicklung eines Lösungsansatzes zu berücksichtigen.

Um eine klarere Struktur des Prozesses zu erhalten, wurde zunächst das Ziel des Sicherheitsnachweises in den Vordergrund gerückt. Der UK-Defence-Standard [1] definiert: Ein Sicherheitsnachweis ist eine strukturierte Argumentation, unterstützt von einem Satz von Beweisen, der einen zwingenden, verständlichen und gültigen Nachweis umfasst, dass ein System sicher in einer gegebenen Anwendung und einer gegebenen Umgebung funktioniert.

Ähnlich beschreibt es Odd Nordland, Notified Body, SINTEF in Norwegen: “The Safety Case is a line of argumentation and not just a collection of facts.”

Zur Erläuterung lässt sich der Vergleich mit einem Gerichtsprozess herstellen: Der Anwalt des Mandaten muss nicht nur alle Fakten sammeln. Seine wichtigste Aufgabe ist es, eine Argumentation aufzubauen, deren Ziel es ist, den Richter vom Sachverhalt zu überzeugen. Die Beweise – also Fakten – sind nur Mittel zum Zweck. Übertragen auf einen Sicherheitsnachweisprozess muss hier ein Ersteller des Sicherheitsnachweises einen Gutachter oder eine Behörde von der Sicherheit des Systems überzeugen. Dazu verwendet er die Argumentation und angehängte Beweise – in diesem Fall die Dokumente, die im Entwicklungsprozess entstehen.

Erarbeitetes Lösungskonzept des Workstreams G

Für das Lösungskonzept wurde die Argumentation innerhalb eines Sicherheitsnachweises, also die Begründung, warum das System die geforderte Sicherheit erfüllt, stärker in den Vordergrund gerückt.
Hierzu wurden der Einsatz der Methode Goal Structuring Notation (GSN) [2][3] sowie der Einsatz eines GSN-

Tools und eines Dokumentenmanagementsystems vorgeschlagen (siehe Bild 2).

Die Methode GSN

Die Goal Structuring Notation, kurz GSN, wurde von Tim Kelly an der Universität von York entwickelt. Sie ist ein Standard für die grafische Darstellung der Definition und Dokumentation von Sicherheitsnachweisen. GSNs zeigen, wie Sicherheitsziele sich in Sicherheitsanforderungen herunterbrechen lassen, die durch Nachweise (Lösungen) belegbar sind. Sie machen Aussagen über die eingesetzten Strategien und erklären dabei im Rahmen eines gegebenen Kontextes die Hintergründe (Annahmen und Begründungen). Die zur Anwendung kommenden grafischen Symbole und deren Bedeutung sind in Tabelle 1 beschrieben.

An oberster Stelle der Argumentationskette zur Sicherheit eines Systems steht das Ziel „Das System ist sicher“. In den folgenden Arbeitsschritten werden Sub-Ziele definiert, die zur Erreichung des Hauptziels erfüllt werden müssen. Darüber hinaus werden die jeweilige Strategie und die Umgebungsbedingungen, die dabei zur Anwendung kommen, dargestellt (Beispiel: Festlegen von SIL-Level für einzelne Komponenten eines Stellwerks).
An der Wurzel eines jeden (Sub-)Ziels befindet sich immer eine Lösung, d. h. ein konkretes Dokument oder ein Nachweis, der die Erfüllung des Ziels oder der getroffenen Annahme belegt (Beispiele: Berechnung über die Ausfallwahrscheinlichkeit einer Komponente, Nachweis über die Qualifikation eines mit der Aufgabe betrauten Mitarbeiters).

GSN-Tool

Im Workstream G wurde ein GSN-Tool (Bild 3) entwickelt, das die Benutzeroberfläche für die Strukturierung des Sicherheitsnachweises zur Verfügung stellt. An jedes Element der „Goal Structure“ können Dokumente geknüpft werden, die sich in einem Dokumentenmanagementsystem befinden. Durch einen Klick auf den Dokumentnamen wird es direkt aus dem Dokumentenmanagementsystem geöffnet. So ist ein unmittelbarer und strukturierter Zugriff auf alle Nachweise problemlos möglich. Elemente der „Goal Structure“ können je nach Status der Dokumente eingefärbt werden. Auf diese Weise können z. B. Informationen über den Projektfortschritt abgeleitet werden. Über eine CMIS Schnittstelle ist es möglich diese Informationen aus dem Dokumentenmanagementsystem abzurufen.
Das entwickelte Tool steht allen INESS-Partnern kostenlos zur Verfügung und kann gemäß der Firmenrichtlinien und -prozesse erweitert und angepasst werden, da es Open-source-Software ist.

Dokumentenmanagementsystem (DMS)

Zur strukturierten Ablage der Dokumente des Sicherheitsnachweisprozesses eines Projektes wurden zwei Tools zum Dokumentenmanagement erprobt.

Nach einem Evaluationsprozess von frei verfügbaren open-Source-Dokumentenmanagementsystemen wurde „Alfresco“ [4] als am besten Geeignete ausgewählt. Zusätzlich wurde SharePoint von Microsoft untersucht, da davon auszugehen ist, dass es eine weite Verbreitung hat. Beide Systeme haben die von Workstream G spezifizierten Funktionen und besitzen die offen spezifizierte Kommunikationsschnittstelle CMIS (Content Management Interoperability Services) [5]. CMIS wurde erst vor kurzem definiert, um ein einheitliches Format für die Kommunikationen zwischen verschiedenen Prozessen von Content Management Systemen festzulegen. Auf diese Weise kann jedes DMS, das CMIS unterstützt, an das GSN-Tool angebunden werden.

Die Dokumente, die im CENELC-Entwicklungsprozess entstehen, bleiben nach den Vorgaben der Norm unverändert. Eine Ablage erfolgt in einem der Dokumentenmanagementsysteme. So ist die gewohnte und etablierte Arbeitsumgebung inklusive Konfigurationsmanagement sicher gestellt. Für neue Projekte bedeutet dies wesentlich weniger Aufwand, weil vorhandene Strukturen übernommen werden können. Dies gilt sowohl für die Hersteller, also auch für Gutachter, Bahnen und nationale Sicherheitsbehörden.

Anwendung an realen Projekten

Um die Vorteile der erarbeiteten Lösung nachzuweisen, wurde die GSN-Methode zusammen mit den vorgeschlagenen Tools in zwei realen Projekten angewendet.

Funkwerk IT setzte für die erarbeitete Lösung ein Entwicklungsprojekt bei den ÖBB ein. Dabei wurde ein fertiges Projekt mit der GSN-Methode strukturiert. Die Aufteilung des Systems in Teilsysteme und die Argumentation, an welcher Stelle welcher Sicherheitslevel SIL erforderlich ist, hat den Erstellern und Prüfern verdeutlicht, welche Komponenten Sicherheitsverantwortung tragen und mit welchen Dokumenten diese belegt werden muss. Auch die Vollständigkeit der Argumentation konnte erweitert werden, weil der Nachweis einfach nachvollziehbar war und so Lücken schneller aufgedeckt werden konnten. Der Entwurf der Argumentation als Grafik mit GSN-Objekten und beispielhaft einigen Dokumenten wurde dem Gutachter und ÖBB präsentiert und gemeinsam diskutiert. Alle Beteiligten waren der Auffassung, dass die Darstellung mit GSN die Übersichtlichkeit deutlich verbessert. Die Anbindung an das Dokumentenmanagementsystem und die dadurch sofort erreichbaren Dokumente als Belege sind darüber hinaus ein klares Plus.

BBR setzte die GSN-Methode in einer Hardware-Entwicklung ein. Aufgabe war die Änderung einer vorhandenen Baugruppe. Mit Hilfe von GSN konnten die Funktionen strukturiert und sogar auf der Baugruppe lokalisiert werden. So war es für den Ersteller einfach, den Prüfer von der Sicherheit der Änderung zu überzeugen und nachzuweisen, dass nur die beschriebenen Teile betroffen waren.

Es war für die Beteiligten bemerkenswert, dass mit einer derart einfachen Methode die Übersicht über die Sicherheitsfunktionen des Systems so stark verbessert werden konnte.

Zusammenfassung

Der Workstream G des INESS-Projektes befasste sich mit der Dokumentation und Anwendung von Sicherheitsnachweisen. Das Ergebnis wurde von Fachleuten aus mehreren Nationen mit unterschiedlichen Hintergründen ausgearbeitet und erscheint so in hohem Maße anwendbar. Der Einsatz der GSN-Methode in Verbindung mit dem entwickelten GNS-Tool und einem Dokumentenmanagementsystem kann die Verständlichkeit über Grenzen hinweg erleichtern und so einen Beitrag leisten, die Aufwände für die Sicherheitsnachweisführung zu senken.

Summary

INESS: Tool Support for the Safety Case Process

The Europe-wide research project INESS (Integrated European Signalling System) aims at reducing the procurement costs of interlockings by introducing a set of clear, standardised specifications with cross-border validity. This article describes the results of the INESS-Workstream „Safety Case“, led by Funkwerk IT and TU Braunschweig. Within the workstream the safety case process was analysed, a tool support specified and a prototype implemented.

Referenzen:

[1] UK Defence Standard 00-56 Issue 4

[2] T. P. Kelly: Arguing Safety – A Systematic Approach to Safety Case Management, DPhil Thesis YCST99-05, Department of Computer Science, University of York, UK, 1998.

[3] Tim Kelly and Rob Weaver: The Goal Structuring Notation – A Safety Argument Notation, Department of Computer Science and Department of Management Studies, University of York, UK.

[4] www.alfresco.com

[5] www.oasis-open.org/committees/cmis/

Abbildungen:

Autoren:

Dipl.-Ing. Carsten Trog

Funkwerk Information Technologies GmbH

Anschrift: Edisonstraße 3, D-24145 Kiel

E-Mail: carsten.trog@funkwerk-it.com

Dipl.-Ing. Geltmar von Buxhoeveden

TU Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik

Anschrift: Langer Kamp 8, D-38106 Braunschweig

E-Mail: buxhoeveden@iva.ing.tu-bs.de