Umbruch in der Signaltechnik – Positive Erfahrungen bei der Weiterentwicklung der RBÜT

Christoph Rade / Christian Blechinger

Die sicherungstechnische Grundlage der Signaltechnik in Deutschland hat sich verändert. Der Übergang von der nationalen Richtlinie Mü8004 zu den europäischen CENELEC-Normen ist weitgehend vollzogen. Die Anwendung der CENELEC-Normen ist im Wesentlichen auf die Entwicklung neuer Systeme beschränkt. Dieser Beitrag zeigt Möglichkeiten auf, positive Impulse der neuen Normen auch bei Weiterentwicklungen bestehender Anlagentechniken sinnvoll zu nutzen. Beispielhaft wird der Nutzen bei Sicherheitsbetrachtungen sowie Verifikation und Validation betrachtet.

1 Einleitung

Die Entwicklung der Rechnergesteuerten Bahnübergangssicherungstechnik RBÜT begann mit der Basisfunktionalität für die Überwachungsarten ÜS und Hp. Die Zulassung der Anlagentechnik durch das Eisenbahn-Bundesamt erfolgte 1999 auf Grundlage der EBA-Richtlinie Mü8004. Die RBÜT ist kontinuierlich weiterentwickelt worden. Die Erweiterung der Anlagenfunktionalität beinhaltet unter anderem die Überwachungsart Fü, diverse Schaltfälle und Anbindungen von Straßenverkehrssignal- und Gefahrenraumfreimeldeanlagen. Die diesbezüglichen Zulassungen erfolgten weiterhin auf Grundlage der Mü8004. Aktuell steht die Unterstützung der Überwachungsart ÜSOE vor der Zulassung.

Dipl.-Ing. Christoph Rade
Leiter der Entwicklung im Bereich Signaltechnik bei der Firma Pintsch Bamag.
Anschrift: Pintsch Bamag Antriebs- und Verkehrstechnik GmbH, Hünxer Straße 149, D-46537 Oberhausen.
E-Mail: c.rade@pintschbamag.de

Dipl.-Ing. Christian Blechinger
Bei der ipw Ingenieurgesellschaft als Projektleiter in den Bereichen Prüfung Signalanlagen und Bahnübergangssicherungstechnik sowie Erstellung von Sicherheitsnachweisen tätig.
Anschrift: ipw Ingenieurgesellschaft, Breite Straße 25-26, D-38100 Braunschweig.
E-Mail: c.blechinger@ipw.de

2 Umbruch Mü8004 nach CENELEC

Mit Einführung der CENELEC-Normen werden diese zunehmend zum Maßstab für die Führung von Sicherheitsnachweisen. Da die Normen nur auf neu zu entwickelnde Systeme anwendbar sind, bleibt die Mü8004 formell Grundlage für die Weiterentwicklungen an der RBÜT. Eine Wiederholung des Entwicklungsprozesses zur CENELEC-konformen Dokumentation wäre weder wirtschaftlich noch sinnvoll. Um dennoch einen Übergang zum CENELEC-Verfahren zu erreichen, sind und werden die Entwicklungsprozesse schrittweise den erweiterten Anforderungen angepasst. Anfängliche Befürchtungen bezüglich erhöhter Dokumentationsaufwendungen haben sich bestätigt. Im Folgenden werden - am Beispiel systematischer, risikoorientierter Sicherheitsbetrachtungen und auditierbarer Aufzeichnungen im Rahmen von Verifikation und Validation - positive Erfahrungen beim Vorgehen nach CENELEC aufgezeigt.

3 Sicherheitsanalyse

Die Sicherheitsanalyse liefert einen Satz an Sicherheitsanforderungen für das betrachtete System. Die geforderte Sicherheit des Systems ist bei Einhaltung der Sicherheitsanforderungen gewährleistet. Eine systematische, risikoorientierte Sicherheitsanalyse liefert ein Satz von Sicherheitsanforderungen, der den sicherheitstechnischen Aufwand minimal hält. Unter diesem Aspekt wurden die eingeführten, regelbasierten Sicherheitskonzepte hinterfragt und alternative Sicherungsverfahren untersucht.
Im Rahmen der Weiterentwicklung der RBÜT wurden einzelne Anwendungsfunktionen einer Sicherheitsanalyse unterzogen. Grundlage einer Sicherheitsanalyse ist die Risikoanalyse, die Sicherheitsziele und die zugehörigen tolerierbaren Gefährdungsraten festlegt. Eine Risikoanalyse des Betreibers, die Betrachtungseinheiten und deren tolerierbare Gefährdungsraten vorgibt, lag nicht vor. Deshalb wurde eine Risikobetrachtung auf Grundlage einer System-Anforderungsspezifikation (ohne Berücksichtigung von Sicherungsfunktionen) durchgeführt. Die System-Anforderungsspezifikation legt die Grenzen des Systems und die auszuführenden Funktionen fest. Die Gefährdungsidentifikation ist durch eine Ausfallauswirkungsanalyse erfolgt. Die Anwendung der Methode FMEA (Ausfallauswirkungsanalyse) war für die Teilmodelle angemessen, da die betrachteten Funktionen von geringer Komplexität sind. Zur Risikoanalyse wurden den Ergebnissen der Gefährdungsidentifikation Kritikalitätsstufen gemäß der Methode FMECA (Ausfalleffektanalyse) zugeordnet. Für die Sicherheitsziele wurden keine Gefährdungsraten berechnet, wohl aber die Tolerierbarkeit klassifiziert nach:

1. *kritisch* – das Ereignis kann zu einer Gefährdung führen,
2. *relevant* – der Weiterbetrieb der Anlage kann zu einer Gefährdung führen,
3. *nicht relevant* – der sichere Betrieb der Anlage ist nicht gefährdet oder eine Gefährdung hinreichend unwahrscheinlich.

Da die Sicherheitsziele nicht quantitativ festgelegt sind, erfolgte die Klassifizierung konservativ, also im Zweifel eher „kritisch“ oder „relevant“. Die Gefährdungsanalyse legt die Sicherungsfunktionen fest und ordnet diese den Sicherheitszielen der Risikoanalyse zu. In der Gefährdungsanalyse wurden allen Ereignissen mit der Klassifizierung „kritisch“ oder „relevant“ Sicherungsfunktionen zugeordnet. Die hinzugefügten Sicherungsfunktionen können Ursache für weitere Risiken sein. Somit führt ein iteratives Vorgehen zu einer umfassenden Gefährdungsanalyse. Abschließend erfolgte der Nachweis der Erfüllung der Sicherheitsziele, indem sich für alle Ereignisse der FMECA bei der gewählten Implementierung unter Anwendung der gewählten Sicherungsfunktionen die Klassifizierung „nicht relevant“ ergibt.
Durch konsequente Anwendung einer risikoorientierten Sicherheitsbetrachtung konnten angepasste Sicherungsfunktionen entwickelt werden. Zum Beispiel bei Ausfall von Komponenten an einer eigensicheren Einschaltstelle wurden verminderte Schließzeiten für den Kraftfahrzeugverkehr und eine erhöhte Verfügbarkeit der Bahnübergangssicherungsanlage (BÜSA) erreicht.

4 Prüfung der Anwendungssoftware

Die RBÜT-Programmsoftware besteht aus dem Laufzeitsystem (Betriebssystem) und der Anwendungssoftware. Für das Laufzeitsystem existiert ein eigener Sicherheitsnachweis. Die Anwendungssoftware der RBÜT ist in drei Funktionseinheiten aufgeteilt:

1. Das Laufzeitinterface stellt die Schnittstelle zum Laufzeitsystem (Betriebssystem) dar. Es übernimmt die Initialisierung der Module der Anwendung und den zyklischen Aufruf der Dienste (zum Beispiel: Behandlung von Laufzeitfehlern, Timerbearbeitung) und der Schnittstellen.
2. Die Anwendung beinhaltet die eigentliche Funktionalität für den zu steuernden Bahnübergang und verwendet für die Kommunikation die Dienste des Laufzeitinterfaces und der Diagnose.
3. Die Diagnose stellt die nicht-sicheren Dienste zur Anwendungs- und Programmablaufdiagnose zur Verfügung, verarbeitet die Diagnosedaten und reicht sie an externe Diagnoseeinrichtungen weiter.

Grundlage für die Entwicklung und Prüfung der o.g. Überwachungsarten ist die Spezifikation der RBÜT-Anwendungssoftware. Die Überwachungsarten wurden - zeitlich gestaffelt - in mehreren Stufen implementiert. Somit wurde auch die Spezifikation schrittweise erweitert und für die jeweilige Entwicklungsstufe dem Eisenbahn-Bundesamt zur Genehmigung vorgelegt.
Grundlage des Mitte der 90er-Jahre begonnenen Entwicklungs- und Prüfprozesses war die Mü8004. Darüber hinaus hat sich der Hersteller für die Spezifikation der RBÜT-Anwendungssoftware an den Anforderungen der neuen europäischen Normen für Bahnanwendungen orientiert, so dass diese in weiten Bereichen einer EN 50128-konformen Software-Anforderungsspezifikation entspricht.
Demgemäß waren die Verifikation und Validation der Anwendungssoftware wesentlicher Bestandteil der sicherungstechnischen Prüfung.

4.1 Verifikation der Softwaremodule

Als Zwischenschritt zwischen der Spezifikation der RBÜT-Anwendungssoftware und der eigentlichen Implementierung des Codes wurde herstellerseitig ein Software-Entwurf erstellt. Diese Vorgehensweise wird auch in der EN 50128 für den Software-Entwurf und die Implementierung gefordert. Die Modellierung erfolgte auf Grundlage der Methoden *Strukturierte Analyse* (SA) nach DeMarco mit der Real-time-Erweiterung (RT) nach Pirbhai/Hatley sowie *Strukturiertes Design* (SD) nach Yourdon/Constantine. Das Ergebnis der Modellierung ist ein System hierarchischer Prozesse, die miteinander kommunizieren und in dem alle Prozesse als *Endliche Automaten* vorliegen. Die Automaten werden durch Zustandsübergangsdiagramme dargestellt. Dadurch entsteht eine starke Entkopplung der Prozesse, was die Modultests wesentlich erleichtert. Auf der Basis des Modells wurde der Sourcecode konventionell entwickelt.
Der Software-Entwurf dient gleichzeitig als Grundlage für die Erstellung der White-Box-Tests. In den White-Box-Tests kann anhand der Diagramme der SA/SD eine vollständige, widerspruchsfreie und korrekte Ausführung der spezifizierten Funktionen nachgewiesen werden. Aufgrund der defensiven Programmierung kann eine Code-Abdeckung nicht zu 100 % erreicht werden. Für nicht abgedeckte Zweige wurde mittels Code-Inspektion die Korrektheit nachgewiesen. Diese Modultests sind ebenfalls in der EN 50128 für den Software-Entwurf und die Implementierung gefordert. Die Ausführung der Modultests erfolgt automatisiert mittels Modultestdateien, die neben der Stimulans bereits die Soll-Reaktionen enthalten. Innerhalb der Modultestumgebung werden der Testablauf und die Reaktionen protokolliert und ausgewertet.

4.2 Validation der Anwendungssoftware

Für die Validierung der Anwendungssoftware wurde konform zur EN 50128 auf die Spezifikation der RBÜT-Anwendungssoftware zurückgegriffen. Der für die RBÜT aufgestellte Testfallkatalog enthält mittlerweile über 2.500 Testfälle, auch dieser Katalog wurde im Laufe der Jahre für die verschiedenen Überwachungsarten erweitert. Die Überwachungsarten sowie die spezifischen Ausprägungen einer BÜSA

Bild 1: RBÜT-Testmaschine

können mittels Konfigurationssets individuell eingestellt werden.
Aus dem Testfallkatalog wurden Testfalldateien erstellt, die neben der Stimulans bereits die Soll-Reaktionen enthalten. Die Bearbeitung dieser Testfalldateien erfolgt automatisiert durch die RBÜT-Testmaschine (*Bild 1*). Die RBÜT-Testmaschine stellt die Testumgebung für die Funktionstests

der Anwendung RBÜT dar und besteht aus einer RBÜT-Steuereinrichtung zuzüglich einer Ansteuerungs- und Auswerteeinheit. Die RBÜT-Steuereinrichtung enthält die zu validierende Programmsoftware. Die Ansteuerungseinheit liefert die Eingaben an die RBÜT, die Auswerteeinheit protokolliert alle Ausgaben der RBÜT. Anhand der in den Testfällen bereits enthaltenen Soll-Reaktionen kann auch die Auswertung automatisiert durchgeführt werden. Sowohl die Abarbeitung der Testfälle inklusive dem Laden unterschiedlicher Konfigurationssets als auch die Auswertung der protokollierten Daten erfolgt vollständig automatisiert. Vor der Abarbeitung der Testfalldateien wird die Testmaschine an ihren Schnittstellen validiert, um zu verhindern, dass ein Fehler in der Anwendungssoftware von einem Fehler in der Testmaschine überdeckt wird. Die Validation geschieht mit speziellen Testfällen zusammen mit einer speziellen Programmsoftware, die nicht mit der zu prüfenden Software identisch ist.

4.3 Dokumentation der Prüfergebnisse

Die Ergebnisse der Validierung der Anwendungssoftware werden in einem Prüfbericht zum Funktionsnachweis zusammengefasst. Dieser Prüfbericht beinhaltet damit einen Validationsbericht gemäß der EN 50128.

5 Zusammenfassung

Der Aufwand für die Durchführung von Risikoanalysen wird mit abgestuften Sicherheitszielen für die Anwendungsfunktionen belohnt. Das Ziel ist die ausreichende Dimensionierung von Sicherheit, das heißt Verhinderung zu schwach ausgelegter Sicherungsfunktionen und Vermeidung kostspieliger Überdimensionierungen. Eine gute Risikoanalyse zeigt offen und nachvollziehbar, wie man zu den Sicherheitszielen gelangt ist, und kann einfach auf neue oder modifizierte Funktionen angepasst werden.
Die auditierbaren Aufzeichnungen der Verifikation und Validation ermöglichen eine leichte Nachvollziehbarkeit und durch die Automatisierung eine einfache Reproduzierbarkeit der Testergebnisse. Somit kann der größte Teil der Tests innerhalb weniger Tage vollständig und mit gleichbleibend hoher Qualität wiederholt werden. Bei einer Änderung der Programmsoftware sind nur die betroffenen Tests in dem Maße anzupassen, in dem sich die Software geändert hat.
Mit der Weiterentwicklung der RBÜT wurde ein pragmatischer Weg beschritten, um das klassische Sicherheitsnachweisverfahren mit den bahnspezifischen europäischen Normen in Verbindung zu bringen.

Literatur

[1] Braband, J.: Methoden zur Sicherheitsanalyse und ihre praktische Anwendung. SIGNAL+ DRAHT, 2002, Heft 1+2

[2] Peters H.: Risikoanalysen im Rahmen der EN 50126/9. Abstract of conference: Application of the international standard IEC 61508, 29.-30. Jan 2003

SUMMARY

Revolution in Signalling – Positive Experiences in Further Development of RBÜT

The basis of technical safety in signalling in Germany has changed. The transition from the national guideline Mü8004 to European CENELEC-Standards is largely complete. The application of CENELEC-Standards has essentially been limited to development of new systems. This article points out opportunities to use the new standards as inspiration for further developments of existing facility technologies. Benefits in the areas of safety analysis as well as verification and validation are used as examples.