Die erfolgreiche SIL-Projektierung

Von Dip.-Informatiker Bernd Pessara und
Dipl.-Marketingwirtin (WAK) Dana Schiffer

Ausgangslage – Schritt für Schritt zum Ziel – Das Safety Instrumented System – Unbefristet begutachtet

1. Ausgangslage

Sicherheit ist im Bahnbereich ist ein zentrales Thema. Eine erfolgreiche SIL-Projektierung setzt bei Kunden und Lieferanten ein fundiertes Wissen voraus, denn die Anforderungen sind umfangreich. Als Produzent von Sensoren, Fahrdatenrekordern, Anzeigern und Multi-Funktions-Terminals steht für DEUTA-WERKE die Sicherheit von Menschen im Fokus der Produktentwicklung. In dem folgenden Bericht bieten wir einen Einblick in die Welt einer erfolgreichen SIL-Projektierung.

Der Bereich der „funktionalen Sicherheit" beschäftigt sich mit technischen Lösungen, die eine sicherheitsgerichtete Funktion ausüben, um Schaden von Mensch und Umwelt abzuwenden. D. h. Risiken werden ermittelt und mit geeigneten Schutzmaßnahmen reduziert. Diese sicherheitsgerichtete Funktion muss auch dann noch verfügbar sein, wenn aufgrund eines Fehlers die normale Funktionalität des Gerätes bzw. der Anlage nicht mehr möglich ist. Beispielhaft ist hier die Sicherheitsfahrschaltung (SIFA) in Triebfahrzeugen genannt.

Fehlt aufgrund einer Handlungsunfähigkeit der regelmäßige Impuls des Triebfahrzeugführers an die SIFA-Taste oder das SIFA-Pedal, verhindert die Sicherheitsfahrschaltung mit einer Zwangsbremsung die Weiterfahrt des Zuges.

Die Funktionale Sicherheit einer Komponente ist immer ein Teil der Gesamtanlagensicherheit. Sie hängt von der korrekten Funktion sicherheitsbezogener Systeme zur Risikoreduzierung ab. Betrachtet werden dabei die Hardwarekomponenten, die Softwareanteile sowie die verwendeten Entwicklungs- und Fertigungsprozesse.

Für jeden einzelnen Branchensektor (Maschinenbau, Prozessindustrie, Kraftfahrzeuge etc.) gibt es spezielle Sicherheitsnormen. Im Bereich der Bahnanwendungen gelten unter anderem die CENELEC-Normen DIN EN 50126, DIN EN 50128 und DIN EN 50129. Diese Sektornormen basieren auf der DIN EN 61508 und wurden auf das spezifische Produktspektrum und seine Gefährdungen angepasst. Die IEC-Basisnorm für funktionale Sicherheit wurde bereits 1998 als ein weltweit gültiger Standard verabschiedet.

2. Schritt für Schritt zum Ziel

Für die Hersteller eines Produktes beginnt die SIL-Projektierung mit einer analytischen Phase, die sich in die Bereiche Konzept, Definition des Geltungsbereiches, einer umfassenden Risikoanalyse und der Festlegung der notwendigen Safety Integrity Level für die unterschiedlichen Sicherheitsfunktionen gliedert. Wegbereitend für die erfolgreiche SIL-Projektierung sind eine ausführliche Gefährdungsanalyse und ein Anforderungskatalog des Kunden.

Sicherheitsmanager und Gutachter begleiten von Beginn an den Entwicklungsprozess.

Die hausinternen Sicherheitsmanager achten darauf, dass die notwendigen Maßnahmen und Methoden zur Erreichung der funktionalen Sicherheit eingehalten werden. Sie begleiten den gesamten Entwicklungsprozess inklusive der Dokumente und Design Reviews bis hin zur Produkteinführung. Mit qualifiziertem Fachwissen sorgen sie dafür, dass Hard- und Software normgerecht dem aktuellen Stand der Technik und der erforderlichen Sicherheitsstufe (SIL) entsprechen. Jeder Entwicklungsschritt wird verifiziert.

Nicht immer ist eine Produktneuentwicklung zur Erreichung des Safety Integrity Levels für ein Produkt notwendig. Mit der Bewertung von betriebsbewährten Produkten kann auch ein älteres Produkt-Fabrikat innerhalb eines Projektes eine SIL-Qualifizierung erhalten. Ein Produkt gilt als betriebsbewährt, wenn eine dokumentierte Bewertung darlegt, dass sich das Produkt aufgrund seiner bisherigen Verwendung nachweislich für den Einsatz in einem sicherheitstechnischen System eignet.

3. Das Safety Instrumented System

Gebündelt in einem Safety Instrumented System (SIS) sichern SIL-Produkte gefährliche Prozesse. Ein Safety Instrumented System gliedert sich in die Bereiche Sensoren, Steuerungen und Aktoren (Bild 1).

Um einen Safety Integrity Level zu erreichen, muss das gesamte SIS die Forderungen für die systematischen Fehler (Hardware und Software) und die zufälligen Fehler (Hardware) erfüllen. Die Fehlersicherheit eines Safety Instrumented Systems gliedert sich in Level 1 – 4, abhängig von der Eintrittswahrscheinlichkeit eines gefährlichen Ereignisses und den Auswirkungen dieses Ereignisses (Bild 2). Diese Einstufungen werden in der IEC 61508 beschrieben.

Entscheidend für die erfolgreiche Entwicklung einer SIL-Komponente ist die Integration des Gutachters in der frühen Planungs- und Konzeptphase bei der Produktentwicklung. So können Konzeptfehler und daraus resultierende Mehrkosten und Verzögerungen der Entwicklung vermieden werden.

In den Konzepten müssen entsprechende Strukturen, z. B. diversitäre Redundanz, dynamische Interfaces, galvanische Trennung, Diagnosefunktionalität etc., implementiert werden, um mögliche Ausfälle zu detektieren und bei Fehlern das System in den sicheren Zustand überführen zu können.

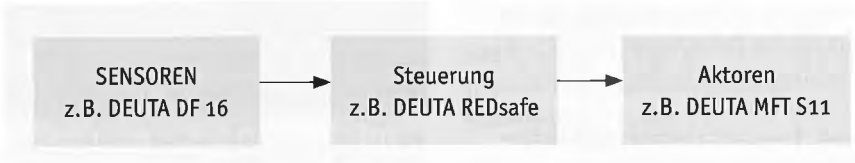

Bild 1: Gliederung des Safety Instrumented Systems

Bild 2: Beispiel für eine Steuerung im SIS – die DEUTA REDBOX Safe+

4. Unbefristet begutachtet

Die Fahrzeughersteller benötigen ein Sicherheitsgutachten für das gesamte Schienenfahrzeug. Das Safety Instrumented System ist ein Teil des Gutachtens. DEUTA hat partnerschaftlich mit seinen Kunden eine marktgerichtete System-Projektstrategie erarbeitet und eine passende zertifizierte Produktpalette entwickelt. Die Kunden werden mit Risikoanalysen, Festlegungen der notwendigen Safety Integrity Level, Systementwürfen mit Hilfe von betriebsbewährten oder neu zu entwickelnden Komponenten, Integrationstests und den notwendigen Systemdokumentation unterstützt. Bei bereits begutachteten Produkten kann nach kundenspezifischen Anpassungen eine Änderungsbegutachtung erfolgen, wodurch sich weitere wesentliche Zeit- und Kosteneinsparungen ergeben.

Ein SIL-Gutachten ist grundsätzlich unbefristet gültig. Erst Änderungen der verwendeten Komponenten, der Funktionalität (Software) oder des Systems machen eine neue Begutachtung bzw. eine Änderungsbegutachtung notwendig.

Die funktionale Sicherheit des Systems muss während des gesamten Lebenszyklus gewährleistet sein.

Ein aktives Obsoleszenz-Management im Rahmen einer konsequenten Produktzyklus-Strategie ist die beste Voraussetzung für die Langlebigkeit einer SIL-Komponente und das korrespondierende Gutachten.

Validierung und Inbetriebnahme setzen die Schlusspunkte einer SIL-Projektierung. In diesen abschließenden Schritten wird das finale Produkt auf Basis der Spezifikationen validiert. Bei DEUTA wird die Produktvalidierung im hausinternen akkreditierten Prüflabor durchgeführt.

Die eingesetzten Maßnahmen und Methoden werden im technischen Sicherheitsbericht zusammengefasst. In diesem Dokument wird auch die Berechnung der Gefährdungsrate dokumentiert. Die resultierende Gefährdungsrate muss unter dem Grenzwert liegen, der abhängig von dem angestrebten SIL ist. Der Sicherheitsbericht enthält die technischen Anwendungsbedingungen mit den entscheidenden Hinweisen für den sicheren Einsatz des Produktes. Die anschließende kontrollierte Inbetriebnahme im Feld stellt final sicher, dass die SIL-Projektierung erfolgreich durchgeführt wurde.

U4: Spatenstich zu den Elbbrücken

Mit dem feierlichen Spatenstich am 21. Juni 2013 begannen offiziell die Bauarbeiten für die Verlängerung der neuen Hamburger U-Bahn-Linie U4 bis zu den Elbbrücken. Die Bauarbeiten werden im Jahr 2018 abgeschlossen sein. Dann soll die U4 auch die neu entstehenden Quartiere der östlichen HafenCity an das Hamburger U-Bahn-Netz anbinden und einen Übergang zur S-Bahn bieten.

Olaf Scholz, Erster Bürgermeister der Freien und Hansestadt Hamburg: „Hamburg wächst durch neue Verbindungen zusammen. Bei diesem Prozess setzen wir ganz klar auf öffentliche Verkehrsmittel. Die U4 erfüllt die Anforderungen, die das moderne urbane Leben an ein leistungsfähiges Nahverkehrsangebot stellt: kurze Zugangszeiten, kurze Fahrzeiten, hohe Verfügbarkeit und hoher Beförderungskomfort – und natürlich eine gute Umweltverträglichkeit."

Enak Ferlemann, Parlamentarischer Staatssekretär beim Bundesministerium für Verkehr, Bau und Stadtentwicklung: „Die Weiterführung der U4 ist der richtige Schritt. Damit sich die HafenCity auch im östlichen Bereich zu einem attraktiven und lebendigen Stadtteil entwickelt, ist eine gute Vernetzung mit dem öffentlichen Nahverkehr wichtig."

Günter Elste, Vorstandsvorsitzender der HOCHBAHN: „Die Anbindung an ein leistungsfähiges Schnellbahnsystem ist für neu entstehende Stadtquartiere von hoher Bedeutung. Gerade hier spürt man den Trend „weg vom privaten Pkw" hin zu passgenauer Mobilität mit dem ÖPNV als Rückgrat. Wichtig für das nun startende Bauprojekt ist, dass wir – wie beim ersten U4-Abschnitt – die Infrastruktur fertigstellen werden, bevor die Bauprojekte an der Oberfläche starten."

Die 1,3 Kilometer lange Strecke führt die U-Bahn-Anbindung der HafenCity bis zu den Elbbrücken fort und bietet für die dort entstehenden Wohn- und Arbeitsquartiere eine leistungsfähige und attraktive Anbindung an die Hamburger Innenstadt. In den Quartieren Baakenhafen und Elbbrücken sollen 2.800 Wohnungen und Arbeitsplätze für 20.000 Menschen entstehen. Die HOCHBAHN rechnet mit mindestens 18.000 Fahrgästen pro Tag. Diese Zahl dürfte mit zunehmenden Pendlerströmen in der Zukunft und dem Anschluss der S-Bahn an die Haltestelle Elbbrücken noch einmal ansteigen.

An dem feierlichen Spatenstich nahmen auch Verkehrssenator Frank Horch,