Aspekte des Sicherheitsnachweises zum Einsatz rechnergestützter Leittechnik in kerntechnischen Anlagen

Freddy Seidel

Fachbereich Sicherheit in der Kerntechnik
Bundesamt für Strahlenschutz
Willy-Brandt-Straße 5
38206 Salzgitter
fseidel@bfs.de

Abstract: Im Nachweisverfahren zum Einsatz rechnergestützter Sicherheitsleittechnik in Kernkraftwerken müssen systemtechnische und leittechnische Anforderungen sowie Anforderungen an die Softwareentwicklung berücksichtigt werden. Für Leittechnikfunktionen mit höchster Sicherheitsbedeutung (Reaktorschutz) ist dabei insbesondere nachzuweisen, dass der systematische Ausfall der Komponenten eines Leittechnikteilsystems – etwa infolge eines Softwarefehlers - vom Gesamtsystem beherrscht wird. Auf Aspekte des Sicherheitsnachweises wie Software-Fehlerpostulate, Bewertung von Software-Diversität und –Komplexität sowie Kriterien zur Akzeptanz der Betriebserfahrung bei früheren Applikationen wird eingegangen.

1 Einleitung

Bei der Leittechnikmodernisierung in Kernkraftwerken (KKW) wird oft ein konservativer Ansatz verfolgt, nach dem die rechnergestützte Leittechnik sukzessive, beginnend bei betrieblichen Funktionen sowie Funktionen mit abgestufter Sicherheitsbedeutung eingesetzt wird, während die festverdrahtete Leittechnik die sicherheitskritischen Funktionen des Reaktorschutzes übernimmt.

Bei einer Um- und Nachrüstung im Bereich des Sicherheitssystems muss der Antragsteller nachweisen, dass die neu implementierten Systeme und Komponenten die spezifizierten Eigenschaften hinsichtlich Funktionalität und Zuverlässigkeit besitzen. Außerdem ist nachzuweisen, dass nicht modifizierte Anlagenteile und deren Funktionen durch die neuen Einrichtungen nicht unzulässig beeinträchtigt werden. Die Nachweiskriterien und –methoden für den sicherheitskritischen Einsatz der rechnergestützten Leittechnik sowie Leitlinien, die Anforderungen an vorgefertigte rechnergestützte Einrichtungen enthalten, werden derzeit formuliert.

2 Aspekte des Sicherheitsnachweises

2.1 Regelwerk

Für den Einsatz rechnergestützter Sicherheitsleittechnik enthält das deutsche Kerntechnische Regelwerk nur übergeordnete Anforderungen. Die Detailanforderungen können branchenspezifischen DIN-IEC Standards entnommen werden. Diese basieren auf internationalen Standards der International Electrotechnical Commission (IEC), die vom entsprechenden Arbeitsgremium der Deutschen Elektrotechnischen Kommission (DKE) im DIN hinsichtlich der Kompatibilität mit deutschen Sicherheitsanforderungen überprüft und in deutscher Fassung herausgegeben werden.

Inwieweit auch branchen-unspezifische IEC-Standards für Nachweisverfahren in der Kerntechnik angewendet werden dürfen, ist noch zu klären. So sind rechnergestützte Leittechniksysteme für Standardfunktionen (z.B. für Hebezeuge) oft nach dem Standard IEC 61508 qualifiziert, wobei ein probabilistischer Ansatz zur Einstufung der sicherheitstechnischen Bedeutung (in sogen. *safety integrity levels*) vorgegeben ist. Da das deutsche Sicherheitskonzept für KKW jedoch vorrangig deterministische Kriterien vorsieht, könnte die Anwendbarkeit von IEC 61508 auch künftig auf Einzelsysteme und Komponenten mit abgestufter Sicherheitsbedeutung beschränkt bleiben.

2.2 Top-down-Näherung und Kategorisierung der Leittechnikfunktionen

Die übergeordneten Schutzziele (Reaktivitätskontrolle, Brennelementkühlung, Einschluss radioaktiver Stoffe und Begrenzung der Strahlenexposition) werden bis zur Zuordnung der Leittechnikfunktionen zu Komponenten untersetzt. Während die anlagentechnischen Sicherheitsfunktionen (z.B. Notkühlung bei Kühlmittelverlust) den Sicherheitsebenen (in diesem Beispiel dem gestörten Betrieb oder Störfall) zugeordnet werden, sind die einzelnen Leittechnikfunktionen – als Hilfsfunktionen - nach deren sicherheitstechnischer Bedeutung für die entsprechende Sicherheitsfunktion zu kategorisieren. Die Sicherheitsebenen werden sowohl quantitativ durch die Wertebereiche der Anlagenzustandsparameter (z.B. gestaffelte Ansprechwerte der Leittechnik für Kühlmitteldruck, -temperatur oder Neutronenflussdichte) als auch - für den Ereignisfall - durch deterministische Annahmen über die Verfügbarkeit (Ausfall) betrieblicher oder sicherheitstechnisch bedeutsamer Funktionen (z.B. Leistungsregelung und -begrenzung) definiert.

Aus der Kategorisierung der Leittechnikfunktionen werden abgestufte Anforderungen an die Qualifizierung und Nachweisführung abgeleitet, wobei für rechnergestützte Systeme mit hoher Sicherheitsbedeutung gefordert wird, dass die Software und Hardware strukturiert und stufenweise nach einem Verfahrensmodell zu entwickeln sind (z.B. Lebenszyklusmodell mit stufenweiser Verifikation und Validierung – V&V).

2.3 Fehlerpostulate für Software

Weil nach dem derzeitigen Stand des Software-Engineerings die Fehlerfreiheit für komplexe Systeme (hier verteilte Rechnersysteme) nicht nachgewiesen werden kann, ist beim Sicherheitsnachweis für rechnergestützte Systeme insbesondere ein systematisches Funktionsversagen infolge eines Auslegungsfehlers zu unterstellen.

Der Sicherheitsnachweis kann wesentlich auf ein in die Tiefe gestaffeltes System von Maßnahmen gegen das Totalversagen von Leittechnikfunktionen gestützt werden; z.B. bestehend aus Maßnahmen zur Fehlervermeidung (Qualitätssicherung, konstruktive Maßnahmen wie Redundanz), analytischen Maßnahmen (V&V) und Maßnahmen gegen Fehlerausbreitung, wie Diversität, Fehlertoleranz und sicherheitsgerichtetes Ausfallverhalten. Nach den in Deutschland geltenden Prinzipien der Kerntechnik sind die Ausfallpostulate deterministisch zu unterstellen und auch die Gegenmaßnahmen deterministisch vorzusehen.

2.4 Sicherheitsnachweis auf Grund von mehreren Standbeinen

Bezogen auf analytische Maßnahmen zur Qualitätssicherung kann die Nachweisführung eingeschränkt sein, wenn z.B. die Entwicklungsdokumentation nicht oder nur eingeschränkt verfügbar ist (Softwarequalifizierung ist nur eingeschränkt nachvollziehbar), der Quellcode nicht verfügbar ist (Code-Analysen sind nicht ausführbar), der Phasenraum für Werte der Eingangssignale sehr groß ist (Testabdeckung ist nicht hinreichend nachweisbar) oder wenn die Systemfunktionen, die durch die Leittechnik unterstützt werden sollen, ein Anlagenverhalten auslösen, dass sich in der Rückwirkung auf die Anforderungen an das Leittechniksystem nur ungenau oder unvollständig simulieren lässt (i.d.R. sind *closed-loop* Tests aus Sicherheitsgründen in der Anlage nicht ausführbar).

In all diesen Fällen ist ein Nachweiskonzept auf der Basis mehrerer „Standbeine“ (*multiple leg approach*) erforderlich. Beispiele für zusätzliche Standbeine sind die Berücksichtigung der Betriebserfahrung aus vergleichbaren Anwendungsfällen, die Anwendung speziell entwickelter Simulationstools zur Überprüfung des spezifizierten Leittechnik-Funktionsverhaltens und ggf. die Ergänzung der deterministischen Nachweisführung durch Nachweise anhand probabilistischer Kriterien.

2.5 Diversität versus Komplexität

Wird Gerätediversität mit unterschiedlicher Software als wesentliche Auslegungsmaßnahme gegen systematisches Funktionsversagen gewählt, führt dies zu erhöhter Komplexität des Softwaresystems und damit zu höheren Anforderungen an die analytische Qualitätssicherung (statische Analysen und Tests hinsichtlich Kompatibilität und Priorität der Teilsysteme untereinander; Nachweis zur unabhängigen Entwicklung der Softwareversionen).

Für den Einsatz in deutschen KKW wird das Konzept der Funktionalen Diversität bevorzugt, begleitet durch Maßnahmen zur räumlichen, funktionalen und energetischen Trennung der Redundanzen, s. VDI/VDE 3527.

2.6 Kriterien zur Berücksichtigung der Betriebserfahrung

Für eine Reihe branchen-unabhängig entwickelter und vorqualifizierter Leittechnikkomponenten, liegen vielfältige Anwendungserfahrungen vor. Außerdem sind vormals anwendungsspezifisch entwickelte Leittechniksysteme mittlerweile auf der Basis von Plattformen so weiterentwickelt worden, dass auch sie flexibel einsetzbar sind.

Die Betriebserfahrung mit vorgefertigten Komponenten kann in späteren Nachweisverfahren nur dann berücksichtigt werden, wenn vorgegebene Auswahlkriterien erfüllt sind. Als Kriterien werden derzeit ein nachvollziehbares Konfigurationsmanagement, Nachvollziehbarkeit der Informationen aus der Betriebserfahrung, der Nachweis, dass die Plattformentwicklung eine stabile Phase erreicht hat, sowie die Bestätigung diskutiert, dass die Betriebserfahrung für ein relevantes Anforderungsprofil gesammelt wurde.

Bei der Entwicklung von Leittechniksystemen auf einer Plattform werden Anforderungen an die Auslegung und Qualifizierung i.d.R. deterministisch vorgegeben; sie bleiben bei der Weiterentwicklung invariant. Bei Auswertung der Betriebserfahrung sollte dann Fall für Fall untersucht werden, ob diese Invarianten bei den erfahrenen Ereignissen verletzt worden sind.

Die Verwendung der Betrieberfahrung als Nachweis für probabilistische Kriterien ist insbesondere für Sicherheitssysteme problematisch, die auf Anforderung funktionieren sollen. Hier ist die Zahl der Anforderungsfälle zu gering, um statistisch signifikante Betriebsdaten ableiten zu können. Allenfalls für kontinuierlich (zyklisch) ablaufende Betriebsystemfunktionen wie Datenaustausch oder Selbsttest können nach angemessener Betriebszeit genügend Daten gesammelt werden.

Inwieweit statistische Tests geeignet sind, um probabilistische Kriterien für komplexe häufig oder kontinuierlich angeforderte Leittechnikanwendungen (z.B. sicherheitsrelevante Regelungsfunktionen) nachweisen zu können, wird weiterhin untersucht. Dazu ist nachzuweisen, dass eine ausreichende Testabdeckung erreicht ist und dass das Testprofil repräsentativ für das Anforderungsprofil im späteren Betrieb ist.

Für vorgefertigte Komponenten können die Nachweisanforderungen nach der sicherheitstechnischen Bedeutung der zu erfüllenden Leittechnikfunktion, der Komplexität der Komponente sowie der Verfügbarkeit von Informationen aus dem Entwicklungs- und Qualifizierungsprozess abgestuft werden [Pa03]. Die Akzeptanz dieser Methode ist allerdings von der Definition der Software-Komplexität und von der Methode zur Bestimmung und sicherheitstechnischen Bewertung der Komplexität abhängig.

2.7 Strukturierung der Nachweisführung

Die Fachregeln enthalten konkrete ausführungsspezifische Detailanforderungen, die beim Nachweis im Kontext zu weiteren Anforderungen zu betrachten sind. So erscheint es zweckmäßig, für die Nachweisführung eine strukturierte Prozedur mit Detailverweisen auf das benutzte Regelwerk vorzugeben [Co01].

Eine solche Strukturierung kann natürlich nicht die detailliert zu führenden quantitativen oder qualitativen Nachweise zu Einzelbehauptungen ersetzen. Vielmehr ist sie eine semi-formale Methode, um komplexe mehrstufige Nachweisverfahren nachvollziehbar auf Vollständigkeit und Widerspruchsfreiheit zu überprüfen.

3. Zusammenfassung – Bezug zur Informatik

Wird Softwarediversität als Maßnahme zur Beherrschung des systematischen Funktionsversagens gewählt, müssen die Unabhängigkeit der diversitären Softwarelösungen untereinander sowie das widerspruchsfreie Funktionieren im Anforderungsfall nachgewiesen werden.

Das Verfahren zum Nachweis der Softwaresicherheit kann anhand von Informationen über die Softwarekomplexität ausgerichtet werden. Dies bedingt, dass geeignete Methoden zur Analyse sowie Metriken zur Quantifizierung der Softwarekomplexität weiterentwickelt und erprobt werden.

Die Anforderungsspezifikation lässt sich derzeit nur für einfache Systeme (geringer Funktionsumfang) streng formal und damit nachweisbar logisch exakt ableiten. Die praktische Anwendbarkeit von semi-formalen Nachweisprozeduren, bei denen systematisch und hierarchisch die Qualifizierungsbehauptungen mit entsprechenden Argumenten und Beweisen verknüpft werden, muss für reale Anwendungsfälle noch demonstriert werden.

Statistisches Testen erscheint derzeit nur bedingt geeignet, um für Sicherheitsfunktionen, die erst bei Anforderung ausgelöst werden, quantitative Zuverlässigkeitsanforderungen nachweisen zu können. Die künftige Methodenentwicklung wird zu beobachten sein.

Bei der Verwendung von Betriebserfahrungen für den Sicherheitsnachweis sind Akzeptanzkriterien vorzugeben und zu erfüllen.

Literaturverzeichnis

[Co01] Courtois, P.-J.: Semantic structures and logic properties of computer-based system dependability cases, Nuclear Engineering and Design 203 (2001) 87-106

[Pa03] Pavey, D.J.: CEMSIS - Cost Effective Modernisation of Systems Important to Safety, Work Package 6, FISA-2003, Luxembourg, November 2003