Qualifizierung integrierter Werkzeugumgebungen für die Erstellung sicherheitsrelevanter Software in Kernkraftwerken

Horst Miedl, Josef Märtz

Abteilung Qualifizierung
Institut für Sicherheitstechnologie (ISTec) GmbH
Forschungsgelände
85748 Garching b. München
Horst.Miedl@istec.grs.de
Josef.Märtz@istec.grs.de

Abstrakt: In Kernkraftwerken wird zunehmend analoge Leittechnik durch rechnerbasierte digitale Leittechniksysteme ersetzt. Um für rechnerbasierte digitale Leittechnik die erforderliche Betriebssicherheit bei akzeptablen Entwicklungs- und Qualifizierungskosten zu erreichen, werden verstärkt integrierte Werkzeugumgebungen eingesetzt. Die integrierten Werkzeugumgebungen sind zum Teil für die Entwicklung von Sicherheitstechnik qualifiziert und für nichtnukleare industrielle Anwendungen zertifiziert, deren Qualifikation für den nuklearen Einsatz ist jedoch noch nachzuweisen.

Das Papier stellt ein Bewertungsschema vor, das eine tragfähige Qualitätsaussage zu verschiedenen integrierten Werkzeugumgebungen unter Berücksichtigung der Sicherheitskategorie der zu erstellenden anwendungsspezifischen digitalen Sicherheitsleittechnik erlaubt. Das Bewertungsschema zielt auf eine "Vorqualifizierung" integrierter Werkzeugumgebungen, weitgehend losgelöst von den damit zu realisierenden Sicherheitsfunktionen. Damit wird der Sicherheitsnachweis der Anwendungssoftware des Zielsystems unterstützt und entlastet. Ohne Vorqualifizierung müssten die für die Sicherheit des Zielsystems relevanten Dienste der integrierten Werkzeuge jeweils von Grund auf neu qualifiziert werden.

1 Einführung

In Kernkraftwerken wird zunehmend analoge Leittechnik durch rechnerbasierte digitale Leittechniksysteme ersetzt. Der Einsatz dieser Systeme bietet die Möglichkeit einer umfassenden Informationsaufbereitung für das Schichtpersonal sowie verbesserte Selbstüberwachungs- und Diagnosefunktionen und kann damit zur Erhöhung der Reaktorsicherheit beitragen.

Um für rechnerbasierte digitale Leittechnik die erforderliche Betriebssicherheit bei akzeptablen Entwicklungs- und Qualifizierungskosten zu erreichen, werden verstärkt integrierte Werkzeugumgebungen eingesetzt. Für die Entwicklung komplexer Leittechniksysteme für kerntechnische Anlagen, die Funktionen der Sicherheitskategorien B und C nach DIN IEC 61226 /DIN05/ ausführen, werden auch kommerzielle integrierte Werkzeugumgebungen verwendet, die ursprünglich nicht für den nuklearen Einsatz konzipiert waren. Da der Einsatz von Sicherheitsleittechnik besonderen Sicherheitsanforderungen unterworfen ist, muss die Qualifikation kommerzieller integrierter Werkzeugumgebungen für die Entwicklung von Software für den nuklearen Einsatz nachgewiesen werden.

Das vorliegende Papier stellt ein Bewertungsschema vor, das eine tragfähige Qualitätsaussage zu verschiedenen integrierten Werkzeugumgebungen unter Berücksichtigung der Sicherheitskategorie der zu erstellenden anwendungsspezifischen digitalen Sicherheitsleittechnik erlaubt. Das Bewertungsschema basiert auf der Analyse und Klassifikation von Diensten, welche die von der integrierten Werkzeugumgebung bereitgestellten Funktionalitäten in Form von Softwarepaketen (z. B. Softwarepakete für Spezifikation, Codegenerierung, usw.) repräsentieren.

Das Bewertungsschema zielt auf eine "Vorqualifizierung" integrierter Werkzeugumgebungen, weitgehend losgelöst von den damit zu realisierenden Sicherheitsfunktionen. Damit wird der Sicherheitsnachweis der Anwendungssoftware des Zielsystems unterstützt und entlastet. Ohne Vorqualifizierung müssten die für die Sicherheit des Zielsystems relevanten Dienste der integrierten Werkzeuge jeweils von Grund auf neu qualifiziert werden.

2 Bewertungsschema

Dieser Abschnitt erläutert die Tätigkeiten und den Rahmen zur Bewertung integrierter Werkzeugumgebungen. Dies soll dem Prüfer die Möglichkeit geben, die Qualifizierung objektiv, nachvollziehbar und somit auch wiederholbar durchzuführen. Grundlage der Qualifizierung bilden die Dienste, welche die von der integrierten Werkzeugumgebung bereitgestellten Funktionalitäten in Form von Softwarepaketen (z. B. Softwarepakete für Spezifikation, Codegenerierung, usw.) repräsentieren. Die Bewertung der Eignung integrierter Werkzeugumgebungen für den Einsatz in der digitalen Sicherheitsleittechnik nuklearer Anlagen basiert auf einem abgestuften Verfahren (siehe Abbildung 1).

In einem ersten Schritt wird die Befolgung allgemeiner Anforderungen an die Gestaltung integrierter Werkzeugumgebungen analysiert, wobei das Ziel dieser Analyse die Feststellung der prinzipiellen Einsetzbarkeit der integrierten Werkzeugumgebung in der vorgesehenen Sicherheitskategorie zum frühestmöglichen Zeitpunkt ist.

Angelehnt an die Erfahrungen mit speziell für die Sicherheitssysteme nuklearer Anlagen entwickelten digitalen Leittechniksystemen wurden allgemeine Anforderungen an die Gestaltung integrierter Werkzeugumgebungen aufgestellt. Es ist jedoch nicht nur auf die zahlenmäßige Abdeckung der Anforderungen durch die Dienste der integrierten Werkzeugumgebung zu achten, sondern insbesondere auf deren qualitative Erfüllung. Ein wesentlicher Aspekt ist die Kohärenz der Dienste, d. h. deren Kommunikationsfähigkeit und Durchgängigkeit in Bezug auf den Softwarelebenszyklus.

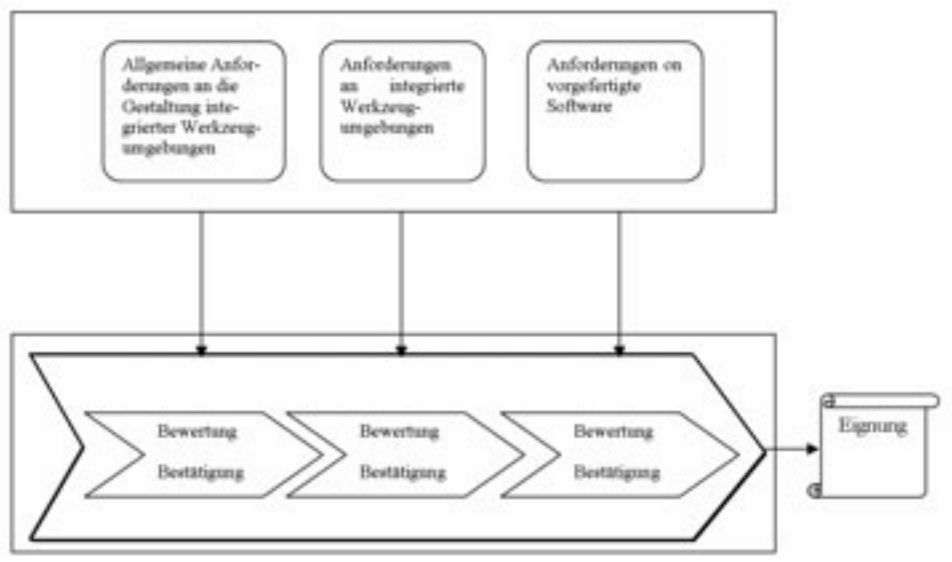

Abbildung 1: Bewertungsschema

In der folgenden Tabelle 3.1 sind auszugsweise allgemeine Anforderungen an die Gestaltung integrierter Werkzeugumgebungen aufgelistet und beschrieben:

Tabelle: Anforderungen an die Gestaltung integrierter Werkzeugumgebungen (Auszug)

Nr.	Anforderung	Beschreibung
1	Softwareentwicklung nach Lebenszyklus	Die Entwicklung der Anwendungsprogramme soll nach einem Softwarelebenszyklus erfolgen, der in klar abgegrenzte Phasen unterteilt ist. Jede Phase sollte mit qualitätssichernden Maßnahmen unterstützt werden. Es sollten Mittel für die Verifizierung der Phasenübergänge zur Verfügung stehen.

Nr.	Anforderung	Beschreibung
2	Konfigurationsmanagement	Es sollen Dienste zur Erfassung und Kontrolle der zur Erstellung des Zielsystems erforderlichen Bestandteile verfügbar sein.
3	Softwarepflege	Die Durchführung regelmäßiger Prüfungen und Änderungen am Zielsystem sollen unterstützt werden.
4	Formalisierte Entwurfsmethoden	Die Entwurfsmethoden sollten formalisiert und für alle Projektbeteiligte verständlich sein.
5	Automatische Codegenerierung	Die Erstellung des Codes der Anwendungsprogramme erfordert Dienste zur automatisierten Codegenerierung.
6	Einschränkungen bei „manueller“ Software (z. B. Einhaltung von Programmierrichtlinien, usw.)	„Manuell“ implementierter Anwendungs-programmcode ist zu vermeiden. Falls erforderlich, ist der Code in übersichtliche, vollständig testbare Module zu strukturieren. Soweit möglich sollen die Module sequentiell arbeiten.
7	Automatisierte Verifizierungswerkzeuge	Es sollten Dienste zur automatisierten Verifizierung aller Softwarekomponenten zur Verfügung stehen.
8	Einschränkungen beim Betriebssystem (z. B. statisch, usw.)	Betriebssystemkomponenten des Zielsystems sollten überschaubar und bewährt sein. Dynamische Verwaltung von Ressourcen ist abzulehnen.
9	Deterministisches Programmverhalten	Die Prozesse des Zielsystems sollen zyklisch abgearbeitet werden. Unterbrechungen sind zu minimieren, um ein deterministisches Programmverhalten zu erreichen. Genügend Reserven sind einzuplanen für Selbsttests und die Stapelverarbeitung.

Sollte die Analyse der allgemeinen Anforderungen mit positivem Ergebnis abgeschlossen sein, so müssen die Dienste der integrierten Werkzeugumgebung detailliert und in entsprechender Prüftiefe analysiert, eventuelle Defizite festgestellt und kompensierende Maßnahmen bewertet werden. Diese Qualifikation der Dienste erfolgt in den folgenden beiden Hauptschritten.

Darüber hinaus bestimmt die Sicherheitskategorie des Zielsystems, welches mit der integrierten Werkzeugumgebung erstellt werden soll, die Anforderungen an die integrierte Werkzeugumgebung. Der Standard DIN IEC 61226 /DIN05/ stellt Kriterien auf zur Zuordnung leittechnischer Funktionen zu Kategorien, die deren sicherheitstechnische Bedeutung bestimmen.

In Abhängigkeit von der Sicherheitskategorie des Zielsystems, welches mit der integrierten Werkzeugumgebung erstellt werden soll, liefert beispielsweise der Standard DIN IEC 62138 /DIN04/ Anforderungen an die Auswahl und die Einsatzmöglichkeit integrierter Werkzeugumgebungen. Im zweiten Hauptschritt werden die Dienste an diesen Anforderungen gemessen und entsprechend bewertet.

Nach erfolgreicher Qualifikation werden in einem abschließenden Schritt die Dienste der integrierten Werkzeugumgebung, die als vorgefertigte Software die Qualität des Zielsystems beeinflussen, abhängig von ihrer Sicherheitsbedeutung detailliert analysiert. Zur Bewertung der Befähigung wird ein systematisches Vorgehen festgelegt zur Gewichtung der Sicherheitsbedeutung der Dienste der integrierten Werkzeugumgebungen. Die Dienste werden eingeteilt im Hinblick auf deren Einfluss auf die Qualität des Zielsystems. Davon abhängig finden Anforderungen an vorgefertigte Software Anwendung, wie sie z. B. im Standard DIN IEC 62138 festgelegt sind.

3 Zusammenfassung

Es wurde ein wissenschaftlich fundiertes Bewertungsschema entwickelt, in welches die Bewertung der einzelnen Dienste der integrierten Werkzeugumgebung - unter Beachtung der Sicherheitsrelevanz des Zielsystems - einfließt. Das Bewertungsschema erlaubt eine umfassende Qualifizierung integrierter Werkzeugumgebungen hinsichtlich ihrer Eignung für den Einsatz in sicherheitsrelevanten Bereichen der Kerntechnik.

Das Bewertungsschema zielt auf eine "Vorqualifizierung" integrierter Werkzeugumgebungen, weitgehend losgelöst von den damit zu realisierenden Sicherheitsfunktionen. Damit wird der Sicherheitsnachweis der Anwendungssoftware des Zielsystems unterstützt und entlastet. Ohne Vorqualifizierung müssten die für die Sicherheit des Zielsystems relevanten Dienste der integrierten Werkzeuge jeweils von Grund auf neu qualifiziert werden.

Literaturverzeichnis

[DIN05] DIN IEC 61226: Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Kategorisierung leittechnischer Funktionen, VDE 0491-1, September 2005.

[DIN04] DIN IEC 62138: Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C, VDE 0491-3-3, September 2004.

[IST07] Miedl, H. et.al.: Qualifizierung integrierter Werkzeugumgebungen zur Entwicklung rechner-basierter Systeme in KKW, ISTec-A-1285, August 2007.