Sichere Automatisierungssysteme mit Hilfe qualitativer Modellierung und quantitativer Risikobewertung

UWE BIEGERT

Institut für Automatisierungs- und Softwaretechnik
Universität Stuttgart

biegert@ias.uni-stuttgart.de

Zusammenfassung

Für die Sicherheitsanalyse von Prozessautomatisierungssystemen ist es notwendig, alle Systembestandteile zu betrachten. Im Beitrag wird ein Modell vorgestellt, bei dem der technische Prozess, die Automatisierungssoftware und menschliche Bedieneingriffe qualitativ beschrieben werden. Aus den einzelnen Modellen und deren Wechselbeziehungen werden Situationen berechnet, die das mögliche Verhalten des Prozessautomatisierungssystems beschreiben. Im Beitrag wird gezeigt, wie eine Risikobewertung der berechneten Situationen nach VDI/VDE 3542 realisiert werden kann. Mit Hilfe der Quantifizierung des Risikos können konkrete Aussagen bezüglich des Grenzrisikos eines Prozessautomatisierungssystems gemacht werden.

1 Einleitung

Im Bereich der Prozessautomatisierung wird der Automatisierungssoftware immer mehr Verantwortung übertragen. Sie hat nicht nur die Aufgabe, komplexe technische Prozesse zu automatisieren sondern muss ebenfalls sicherheitskritische Situationen des Systems verhindern, die unmittelbar für Mensch und Umwelt eine Gefahr darstellen würden.

Um die Sicherheit eines Prozessautomatisierungssystems zu untersuchen, kann auf viele klassische Methoden zurückgegriffen werden. So wird in Deutschland für den Kfz-Bereich häufig das Verfahren FMEA eingesetzt, während für verfahrenstechnische Prozesse das PAAG - Verfahren verwendet wird. Die Automatisierungssoftware kann mit Hilfe der Fehlerbaumanalyse auf Fehler untersucht werden. Im akademischen Bereich werden verstärkt formale Methoden betrachtet, mit denen Sicherheitsanforderungen mathematisch nach gewiesen werden. Menschliche Bedieneingriffe werden z.B. mit der Action Error Analyse auf einzelne Operationen heruntergebrochen und deren Auswirkungen auf das System analysiert. Die meisten klassischen Verfahren für die Sicherheitsanalyse sind auf einen Teilbereich des Prozessautomatisierungssystems spezialisiert. Die Analyse des Wechselspiels vom technischen Prozesses, der Automatisierungssoftware und den menschlichen Bedieneingriffen wird vernachlässigt. Dabei gehen viele Unfälle und Katastrophen auf Mehrfachfehler zurück, deren Auswirkungen durch die eingeschränkte Betrachtungsweise bei der Analyse unterschätzt bzw. falsch interpretiert wurden. Beispielsweise können defekte Bauelemente das

reguläre Verhalten der Automatisierungssoftware entscheidend beeinflussen. Werden zusätzlich falsche Bedieneingriffe gemacht, so stößt die Brainstorming-Analyse vieler klassischer Methoden schnell an ihre Grenze.

Am Institut für Automatisierungs- und Softwaretechnik wurde daher ein modellbasierter Ansatz für die Sicherheitsanalyse von Prozessautomatisierungssystemen entwickelt. Hierbei werden die drei Teilbereiche und die Struktur eines Prozessautomatisierungssystems mit Hilfe der qualitativen Modellierungsmethode SQMA[1] beschrieben. Dabei werden ebenfalls mögliche Defekte von Bauelementen oder falsche Bedienhandlungen mit berücksichtigt. Basierend auf diesen Modellen und der Struktur kann der Computer die Wechselbeziehung der Bestandteile auswerten und mögliche sicherheitskritische Systemsituationen berechnen. Anhand dieser berechneten Situationen muss der Experte entscheiden, ob zusätzliche Sicherheitsmaßnahmen notwendig sind oder gegebenenfalls begründen warum nicht. Zur Entscheidungsfindung existieren quantitative Bewertungsansätze für das zu erwartende Risiko. Diese werden nun in den folgenden Abschnitten vorgestellt und diskutiert.

2 Grundlagen

Das primäre Ziel einer Sicherheitsanalyse ist es, Aussagen über die Sicherheit[2] des Systems zu machen. Eine absolute Sicherheit ohne jegliches Risiko gibt es in technischen Systemen nicht [1]. Deshalb wird nach DIN VDE 31000, Teil 2, die Sicherheit in Abhängigkeit des Risikos definiert, siehe Abbildung 1. Ein System ist sicher, falls das Risiko aller Einzelvorgänge kleiner ist als ein Grenzrisiko. Das Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustands. Wird dieses Grenzrisiko überschritten, so wird diesem Bereich der Begriff "Gefahr" zugeordnet.

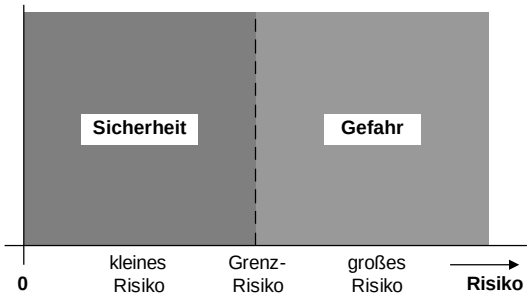

Abbildung 1. Zur Definition der Begriffe Sicherheit und Gefahr [1]

[1] Situationsbasierte Qualitative Modellierung und Analyse [1], [2]

[2] Sicherheit im Sinne des englischen Begriffes "Safety", nicht zu verwechseln mit "Security"

Ein weiteres Ziel der Sicherheitsanalyse ist es, das Grenzrisiko (R_v) eines Systems zu bestimmen und Aussagen über das Risiko von Teilvorgängen zu machen, siehe (1). Nach VDI/VDE 3542 (Sicherheitstechnische Begriffe für Automatisierungssysteme) setzt sich das Risiko eines Teilvorganges (Ri) aus der Wahrscheinlichkeit oder Häufigkeit (Hi) des Eintritts einer Fehlfunktion oder eines Defekts und des zu erwarteten Schadenausmaßes (Si) zusammen, siehe (2). Es muss gezeigt werden, dass jeder Risikowert eines Teilvorgangs kleiner oder gleich dem Grenzrisiko ist, also

$$Ri \leq Rv \quad \text{, für i = 1.. n} \qquad (1)$$

$$Hi \cdot Si \leq Hv \cdot Sv \text{ , für i = 1..n} \qquad (2)$$

Das Risiko kann bei einem großen Schadenausmaß und kleiner Fehlerwahrscheinlichkeit demzufolge gleich sein, wie bei einem geringen Schadenausmaß und großer Fehlerwahrscheinlichkeit. In vielen Fällen ist eine quantitative Angabe nicht möglich, sodass Risiko in diesem Sinne eher qualitativ als quantitativ zu verstehen ist [4]. DIN 50126 gibt den qualitativen Zusammenhang zwischen der Häufigkeit eines Gefahrenfalls und dem erwarteten Schadenausmaß wieder (definierte Bewertungsstufen: vernachlässigbar, tolerabel, unerwünscht und intolerabel). Die quantitative Risikobewertung dient innerhalb einer Analyse als Vergleichsmaß, um bestimmte Vorgänge hinsichtlich ihres Gefahrenpotential zu bewerten.

Beim technischen Prozess beruhen Angaben bezüglich der (sicherheitsbezogenen) Ausfallrate auf Erfahrungswissen, Laborversuche oder auch Schätzungen. Ebenfalls wird versucht, menschliches Versagen bzw. die Wahrscheinlichkeit für menschliche Fehleingriffe zu ermitteln. Das von Swain entwickelte Verfahren THERP enthält 27 Tabellen mit Fehlerwahrscheinlichkeiten für menschliches Verhalten [3]. Hingegen machen Angaben über die Fehlerwahrscheinlichkeit bei Software keinen Sinn, da Software nicht verschleißen kann bzw. von der Software selbst unmittelbar kein Risiko zu erwarten ist. Softwarefehler (insbesondere Entwurfsfehler) wirken sich direkt bzw. indirekt durch falsche Informationen an den Menschen auf den technischen Prozess aus.

Um eine Risikobewertung für die modellbasierte Sicherheitsanalyse zu integrieren, wird von der ursprünglichen Definition des Risikos ausgegangen.

3 Modellbasierte Sicherheitsanalyse

Bei der modellbasierten Sicherheitsanalyse werden die Bestandteile des Prozessautomatisierungssystems ausgehend von der vorhandenen Systembeschreibung in Form von Situationen und Transitionen modelliert [5]. Beim technischen Prozess geben die Situationen das physikalische Verhalten wieder. Dabei werden Ausfälle von Bauelementen berücksichtigt. Die Situationen des qualitativen Modells der Automatisierungssoftware werden direkt aus dem Entwurf ermittelt. Gegenwärtig unterstützt das Verfahren die Methode UML-RT. Dabei stellen die Situationen und Transitionen das Verhalten des Automatisierungssystems dar. Das qualitative Modell der

menschlichen Bedieneingriffe enthält richtige und falsche Eingriffe in das System. Aus den Modellen ermittelt der Rechner das mögliche Systemverhalten für den Normalbetrieb sowie für den fehlerhaften Betrieb des Prozessautomatisierungssystems.

	Technischer Prozess			Automatisierungssoftware		Mensch	Status
	Zulaufventil	Tank	Ablaufventil	AnlagenController	DialogManager	Bedieneingriffe	
..	..	..	..	..	..	..	..
Sx	geöffnet	gefüllt, Zulauf	geschlossen	Füllen	Eingaben sperren	Prozess starten	bestimmungs-gemäß
Sy	geöffnet, blockiert	gefüllt, Zulauf	geschlossen	Soll-Niveau erreicht, Zulaufventil schließen	Eingaben sperren	Türe öffnen	unerwünscht
Sz	geöffnet blockiert	gefüllt, Zulauf, Überlauf	geschlossen	Soll-Niveau erreicht, Zulaufventil schließen	Eingaben sperren	keine Eingriffe	intolerabel
..	..	..	..	..	..	..	..

Tabelle 1. Systemsituationen eines Prozessautomatisierungssystems

Die Tabelle 1 zeigt drei verschiedene Situationen eines Systems. Der Tabellenkopf enthält dabei die Bezeichnungen der Systemelemente. Die Situation Sx stellt einen bestimmungsgemäßen Betrieb des Prozessautomatisierungssystems dar. Sie zeigt einen Füllvorgang: die Automatisierungssoftware hat die Aufgabe, den Zufluss in einen Behälter zu regeln und kann dazu das Zulauf- und Abflussventil des Behälters ansteuern. Im Unterschied zu Zustandsautomaten sind in einer Situation Ursache und Wirkung gleichzeitig dargestellt. Die weiteren Situationen zeigen das mögliche Systemverhalten für blockierte Ventile. Jede dieser Situationen hat für die Sicherheitsanalyse eine andere Bedeutung und ist dementsprechend qualitativ bewertet.

Mit einer zusätzlichen quantitativen Bewertung des Risikos lässt sich die Aussagekraft der nichtbestimmungsgemäßen Systemsituationen verbessern. Hierzu muss die Auftrittswahrscheinlichkeit der in den Situationen beschriebenen Fehlern und im Schadenfall dessen Ausmaß betrachtet werden.

Die qualitative Modellierung von möglichen Fehlern der einzelnen Systemkomponenten wird um die Angabe der Wahrscheinlichkeit der Fehler erweitert. Diese Werte können aus den Datenblättern der Bauelemente entnommen oder geschätzt werden. Einen grundlegenden, normierten Maßstab für die Wahrscheinlichkeiten existiert nicht. Wichtig ist nur, dass ein definierter Maßstab innerhalb einer Sicherheitsanalyse konsequent anzuwenden ist, um die Vergleichbarkeit verschiedener Situationen zu gewährleisten. Bei der Auftrittwahrscheinlichkeit handelt es sich um eine bedingte Wahrscheinlichkeitsangabe, die unabhängig von der Zeit ist (stationäre Wahrscheinlichkeitsangaben). Gefährliche Vorgänge in Systemkomponenten oder Teilsystemen werden durch einen Wert für das Schadenausmaß klassifiziert, diese Werte liegen zwischen 1 (kein Schadenausmaß) und 10 (hoher Schadenausmaß).

Zur Berechnung des Risikos wird die Gleichung (2) herangezogen. Das Risiko einer nichtbestimmungsgemäßen Systemsituation setzt sich somit aus dem Produkt aller

Auftrittwahrscheinlichkeiten der beschriebenen Fehler und der Summe des Schadenausmaßes zusammen.

Mit diesen Angaben lässt sich für jede nichtbestimmungsgemäße bzw. sicherheitskritische Systemsituation das Risiko nach (3) ermitteln. Der Parameter k steht für die Nummer der Situation und n für die Anzahl der vorhandenen Systemelemente. Je höher die Werte für R(k), desto höher das Risiko der Systemsituation.

$$R(k) = \left(100 \cdot \prod_{i=1}^{n} Pi(k)\right) \cdot \left(\sum_{i=1}^{n} Si(k)\right) \qquad (3)$$

Für das Beispiel aus Tabelle 1 wurden folgende Werte angenommen:

Die Auftrittswahrscheinlichkeit für ein blockiertes Ventil im offenen Zustand wurde mit P= 0,05 angenommen. Das Schadenausmaß für einen Überlauf des Tanks ist von der Art der Flüssigkeit abhängig. Das Schadenausmaß wurde mit dem Wert 4 berücksichtigt. Die berechneten Werte für das Risiko der nichtbestimmungsgemäßen Systemsituationen aus Tabelle 1 sind in der letzten Spalte der nachstehenden Tabelle angegeben.

	Technischer Prozess			Automatisierungssoftware		Mensch	Status	Risiko
	Zulaufventil	Tank	Ablaufventil	AnlagenController	DialogManager	Bedieneingriffe		
..	..	..	..	..	..	..	..	..
Sz	geöffnet blockiert, P = 0,05	gefüllt, Zulauf, Überlauf, S=4	geschlossen	Soll-Niveau erreicht, Zulaufventil schließen	Eingaben sperren	keine Eingriffe	intolerabel	20
Sy	geöffnet, blockiert, P = 0,05	gefüllt, Zulauf	geschlossen	Soll-Niveau erreicht, Zulaufventil schließen	Eingaben sperren	Prozess abbrechen	unerwünscht	5
Sx	geöffnet	gefüllt, Zulauf	geschlossen	Füllen	Eingaben sperren	Prozess starten	bestimmungs-gemäß	-
..	..	..	..	..	..	..	..	..

Tabelle 2: Systemsituationen nach ihrem Risiko bewertet.

Im Allgemeinen enthält das qualitative Modell eines Prozessautomatisierungssystems mehrere hunderte Systemsituationen und Komponenten. Anhand der eingeführten Risikobewertung können die Systemsituation einfach untereinander verglichen und entsprechend des Risikos sortiert werden. Damit kann die Systemsituation, die das größte Risiko beim Betreiben des Prozessautomatisierungssystems repräsentiert, ermittelt werden.

Die modellbasierte Sicherheitsanalyse erlaubt die Bestimmung der Auswirkung von beliebig vielen Mehrfachfehlern auf das Systemverhalten. Mit Hilfe der quantitativen Risikobewertung kann das Auftreten und die Auswirkungen von Mehrfachfehler gegenüber der qualitativen Bewertung konkreter analysiert werden, da hier die Auftrittswahrscheinlichkeit zusätzlich mit in das Ergebnis einfließt.

Der Experte muss schließlich die berechneten Situationen auswerten und gegebenenfalls entscheiden, ob zusätzliche Sicherheitsfunktionen notwendig sind. Diese Sicherheitsfunktionen haben die Aufgabe, die mit hohem Risiko behafteten

Systemsituationen zu vermeiden. Die Situation Sz in Tabelle 2 kann verhindert werden, indem z.B. der Entwurf der Automatisierungssoftware um eine Sicherheitsfunktion ergänzt wird, die grundsätzlich beim Überschreiten eines bestimmten Schwellwerts des Füllstands das Ablaufventil öffnet.

4 Zusammenfassung

Die modellbasierte Sicherheitsanalyse erlaubt die Betrachtung aller Bestandteile eines Prozessautomatisierungssystems. Dabei werden mögliche Systemsituationen hinsichtlich ihrer Relevanz für die Systemsicherheit qualitativ bewertet. Diese Bewertung wurde zusätzlich mit einer quantitativen Risikobewertung ergänzt, die sich nach VDI/VDE 3542 aus der Auftrittswahrscheinlichkeit und dem Schadenausmaß zusammensetzt. Voraussetzung für die quantitative Risikobewertung ist die konsequente Anwendung eines einheitlichen Maßstabes für die Auftrittswahrscheinlichkeit und des Schadenausmaßes. Die Quantifizierung des Risikos dient in erster Linie für den Vergleich von verschiedenen Systemsituationen eines Prozessautomatisierungssystems. Die Auswirkungen von Mehrfachfehlern können gegenüber der qualitativen Risikobewertung konkreter analysiert werden, da die Auftretenswahrscheinlichkeit berücksichtigt wird. Das eigentliche Ziel der quantitativen Risikobewertung liegt in der Unterstützung des Experten bei der Entscheidungsfindung, ob das Grenzrisiko des Prozessautomatisierungssystems überschritten wird und damit zusätzliche Sicherheitsfunktionen notwendig sind.

5 Literatur

[1] R. Lauber, P. Göhner, *Prozessautomatisierung*, Band 1 und 2, 3.Auflage, Springer-Verlag Berlin Heidelberg New York 1999

[2] Leveson, Nancy G.: *SAFEWARE - System Saftey and Computers*, Addison-Wesley 1995

[3] Heiner Bubb (TU-München), Menschliche Zuverlässigkeit, ecomed-Verlag, 1992

[4] Litz, Lothar; Grundlagen der sicherheitsgerichteten Automatiseirungstechnik, at 2/98, Seite 56-57

[5] Biegert, Uwe; *Computer-supported Safety Analysis for Computer-controlled Systems*, MMAR 2000, Sixth International Conference on Methods and Models in Automation and Robotics.