Landesumweltamt Nordrhein-Westfalen

Kurzbericht zum
Forschungsvorhaben 56/03

Qualifizierung von Bussystemen und deren Komponenten in der Anlagensicherheit der Chemie-Industrie

von

Dipl.-Ing. Klaus Kemp

Dipl.-Ing. Thomas Steffens

Dipl.-Ing. Gernot Klaes

TÜV Industrie Service GmbH
Automation, Software und Informationstechnologie (ASI)

Inhaltsverzeichnis **Seite**

Qualifizierung von Bus-Systemen und deren Komponenten in der Anlagensicherheit

1 Einleitung

Bei dem vorliegenden Kurzbericht handelt es sich um eine inhaltliche Kurzform des Hauptberichtes des Forschungsvorhaben 56/03. Der Kurzbericht soll einen Überblick über die Forschungstätigkeit und deren Ergebnisse liefern.

In einem vorangegangenen Forschungsvorhaben mit dem Thema „Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie“ sollte geklärt werden, ob Bussysteme für sicherheitsrelevante Aufgaben im Sinne der **12.BImSchV** (Störfall-Verordnung) in verfahrenstechnischen Anlagen verwendet werden dürfen.

Hierbei wurde schwerpunktmäßig eine Betrachtung durchgeführt, ob und unter welchen Bedingungen es möglich ist, bei dem gegenwärtig fortgeschrittenen Stand der Signalübertragungstechnik, die Übertragung von Signalen einer Schutzeinrichtung mittels eines Bussystems **gemeinsam** mit den Signalen der Betriebs- und Überwachungseinrichtungen, ohne Verlust von Zuverlässigkeit, Verfügbarkeit und Funktionalität und ohne Zunahme des Risikos in der Verfahrenstechnik durchzuführen, d. h. auf mindestens gleichem sicherheitstechnischen Niveau wie bei Punkt-zu-Punkt verdrahteten Sicherheitskomponenten.

Für die damalige Betrachtung wurde der anwendungsunabhängige Basisstandard IEC 61508 herangezogen, da einerseits dieser Standard eine Technologie zum Gegenstand hat, die auch bei Bussystemen verwendet wird und andererseits dieser Standard eine Trendwende in der sicherheitstechnischen Welt darstellt, wobei immer mehr Anwendungsstandards auf diesen Basisstandard verweisen, wenn es um die Betrachtung der dort beschriebene Technologie geht.

Bezogen auf die Prozessindustrie, der die Chemie-Industrie auch angehört, etabliert sich zur Zeit der Anwendungsstandard IEC 61511. Dieser Standard beschreibt die Anforderungen für die Funktionale Sicherheit von sicherheitstechnischen Systemen in der Prozessindustrie und weist sehr enge Bezüge zum Basisstandard IEC 61508 auf.

Das Ergebnis dieses vorangegangenen Forschungsvorhaben war, dass unter bestimmten Bedingungen die gemeinsame Übertragung von sicherheitsrelevanten und nicht sicherheitsrelevanten Daten grundsätzlich möglich ist, dass es aber zum Zeitpunkt des Forschungsvorhabens noch keine zertifizierten Bussysteme gegeben hat.

Das hier behandelte weiterführende Forschungsvorhaben „Qualifizierung von Bussystemen und deren Komponenten in der Anlagensicherheit“ soll, basierend auf den Ergebnissen des vorangegangenen Forschungsvorhabens „Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie“ Behördenmitarbeiter unmittelbar in die Lage versetzen, ein in einem der **12.BImSchV** unterliegendem Betriebsbereich eingesetztes sicherheitsgerichtetes Bussystem bewerten zu können.
Hierbei sollen die Bereiche Planung, Installation, Betrieb, Wartung und Instandhaltung sowie Reparatur und somit der gesamte Lebenszyklus des Systems betrachtet werden und spezifische Merkmale herausgearbeitet werden, die ein Bussystem und dessen Komponenten auf jeden Fall aufweisen müssen, und die Merkmale, die ein System auf keinen Fall aufweisen darf, um den sicherheitstechnischen Anforderungen in der Prozessindustrie, bzw. Chemie-Industrie zu genügen.

2 Sicherheitstechnische Festlegungen

Unter sicherheitstechnischen Festlegungen werden hier nicht nur die normativen Festlegungen verstanden, sondern auch Empfehlungen aus Erfahrungsberichten von Interessengemeinschaften und Arbeitsgremien. Die sicherheitstechnischen Festlegungen beschreiben den aktuellen **Stand der Sicherheitstechnik**. Aufgrund des technischen Fortschrittes unterliegen diese sicherheitstechnischen Festlegungen einem fortlaufenden Änderungsprozess.

Die zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall Verordnung **12.BImSchV**) fordert im §3 „Anforderungen zur Verhinderung von Störfällen“ im Abschnitt 4, dass die Beschaffenheit und der Betrieb der Anlagen des Betriebsbereiches dem **Stand der Sicherheitstechnik** entsprechen müssen.

Die Anforderungen aus der **12.BImSchV** für sicherheitsrelevante Anlagenteile gelten selbstverständlich auch für zukünftig einzusetzende Bussysteme in der Verfahrenstechnik. Welche spezifischen Anforderungen diese Bussysteme zu erfüllen haben ist in dieser Verordnung nur indirekt durch den Verweis auf den **Stand der Sicherheitstechnik** zu erfahren.

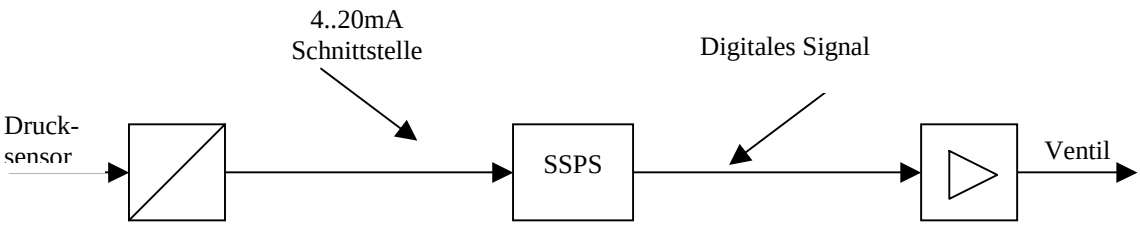
Die in der **12.BImSchV** beschriebenen Anforderungen lassen sich in ähnlicher Form in der **IEC 61508** wiederfinden. Da aber ein Bussystem die Technologie verwendet, die der IEC 61508 zugrunde liegt, gelten die dort beschriebenen Anforderungen gleichermaßen für Bussysteme, die in einer Sicherheitskette verwendet werden.

In der Anwendungsnorm **IEC 61511-1** werden die Anforderungen an die Funktionale Sicherheit in der Prozessindustrie beschrieben. Die IEC 61511-1 lehnt sich direkt an die IEC 61508 an und setzt deren Anforderungen auf das Anwendungsgebiet der Prozessindustrie, unter Berücksichtigung anwendungsspezifischer Anforderungen, um.

3 Sicherheitstechnische Konzepte in Verbindung mit Bussystemen

Bevor in die konkrete Betrachtung der Bussysteme eingestiegen wird ist es erforderlich den Begriff „Buskomponenten“ im Rahmen dieses Projektes zu definieren.

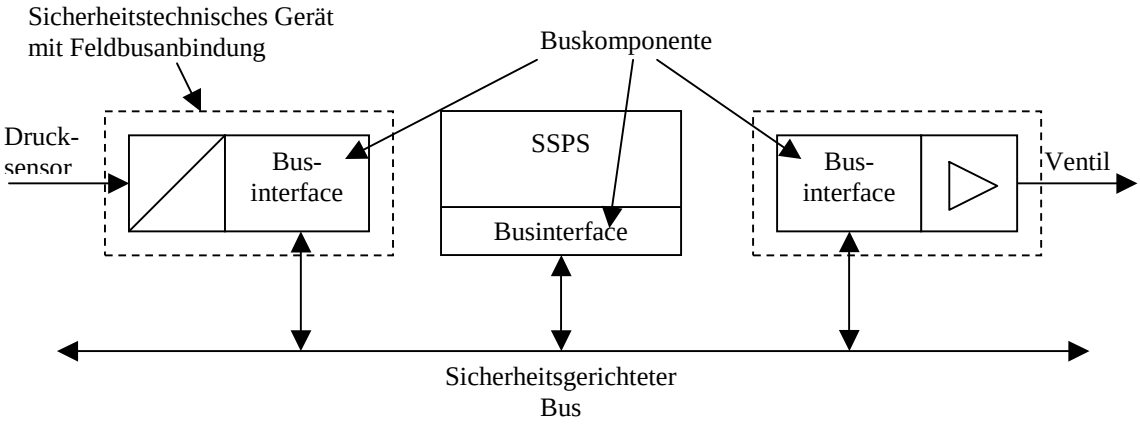
Bei der konventionellen Technik wird zunächst eine physikalische Größe mit Hilfe eines Umsetzers in eine standardisierte elektrische Größe z. B. 4.. 20 mA umgesetzt und diese einer Überwachungseinheit (z. B. SSPS) zugeführt. Diese Überwachungseinheit löste die Schutzfunktion bei Überschreitung eines Grenzwertes beispielsweise durch Ansteuerung eines Ventils aus, wie in der folgenden Skizze gezeigt ist.



Bei der Realisierung dieser Funktion mit einem Bussystemen wird dem Umsetzer ein weiterer Baustein, ein Businterface, nachgeschaltet und dem Ventil vorgeschaltet. Dieses setzt die technische Größe des Umsetzers als digitalen Wert in ein festspezifiziertes Kommunikationsprotokoll um. Die Überwachungseinheit muss wiederum in der Lage sein, diese Protokoll zu verstehen, um die im Protokoll enthaltenen relevanten Informationen entsprechend verarbeiten zu können. In gleicher Art und Weise erfolgt die Übertragung der relevanten Informationen von der Überwachungseinheit zum Aktor.

Im weiteren Verlauf dieses Forschungsvorhabens wird dieses Businterface als Buskomponente bezeichnet.

Aufgabe einer Buskomponente ist die sichere Umsetzung der Informationen in ein definiertes Protokoll und deren sichere Übertragung. Alle anderen an der Sicherheitsfunktion beteiligten Komponenten sind keine Buskomponenten.



3.1 PLT-Systeme

Feldbusse sind im allgemeinen nichts Neues in der Prozessleittechnik (PLT). Sie tauschen Informationen zwischen Sensoren/Aktoren und prozessnahen Komponenten (PNK) aus. Remote I/O Komponenten (sich im Feld befindende I/O Komponenten) sammeln Informationen von Aktoren/Sensoren über standardisierte Strom- und Spannungsschnittstellen und übermitteln diese über Feldbusse an die prozessnahen Komponenten, beispielsweise eine SPS.

Dieser Einsatz bezieht sich jedoch auf Anwendungen, in denen nicht sicherheitsrelevante Informationen über Bussysteme ausgetauscht werden.
Sicherheitsrelevante Aufgaben und Verknüpfungen werden in der Regel in bewährter Technik, z. B. konventioneller Verdrahtung in Hardware, realisiert.

Gemäß IEC 61511 muss beim Einsatz von Bussystemen für sicherheitsrelevante Aufgaben grundsätzlich mindestens das gleiche Sicherheitsniveau wie bei Schutzsystemen in herkömmlicher Technik erreicht werden. Der Trend der sich auf dem Markt abzeichnet ist die Übermittlung betrieblicher und sicherheitsgerichteter Daten mittels eines Bussystem, welches als ein hybrides, offenes Bussystem bezeichnet wird.

Hierfür wurden die allgemeinen Busspezifikationen um Maßnahmen und Verfahren erweitert, die es ohne Verlust an Zuverlässigkeit, Verfügbarkeit und Funktionalität und ohne Zunahme des Risikos erlauben, Betriebsinformationen und sicherheitsrelevante Informationen mit definierter Datenintegrität gemeinsam zu übertragen.

4 Sicherheit und Verfügbarkeit

4.1 Allgemeines

In der chemischen Industrie ist es wichtig, dass die dort eingesetzten Systeme nicht nur sicher, sondern auch in einem hohen Maße verfügbar sind. Die Forderung nach einer hohen Systemverfügbarkeit entstammt nicht einzig und allein wirtschaftlichen Gesichtspunkten, sondern auch sicherheitstechnischen Gesichtspunkten, da die Betriebsphasen des Einschaltens und des Abschaltens einer Anlage in der chemischen Industrie mit erhöhten Gefahren verbunden sein können.

Die technischen Maßnahmen zur Risikoreduzierung durch eine Schutzeinrichtungen sind derart auszulegen, dass sie die ihnen übertragene Sicherheitsverantwortung unter definierten Bedingungen erfüllen. Umwelteinflüsse und Fehler sind zu beherrschen und dürfen nicht zu einem Verlust der Sicherheitsfunktion führen.

Die Ursachen für Fehler können Störungen oder Ausfälle sein. In der Praxis sind dies überwiegend umweltbedingte Störungen (z. B. EMV), die Fehlfunktionen hervorrufen und die Schutzfunktion ungewollt auslösen können. Diese Störungen können kurzfristig oder dauerhafter auf die Komponenten einwirken. Hierbei wird zwischen sporadischen und dauerhaften Fehlern unterschieden.

4.2 Maßnahmen zur Erhöhung der Verfügbarkeit

Alle beteiligten Komponenten eines Sicherheitssystems müssen eine entsprechende EMV-Robustheit besitzen. Der Nachweis ist die Konformitätserklärung des Komponentenherstellers. Anwendungs- und Produktnormen stellen darüber hinaus spezifische Anforderungen.

Insbesondere bei Bussystemen spielt die richtige Verlegung der Busleitung eine entscheidende Rolle. Diese liegt im Feld und ist allen möglichen Einflüssen und Einkopplungen ausgesetzt. Alle zu treffenden Installationsmaßnahmen sind in dem zum Bussystem zugehörigen Sicherheitshandbuch des Herstellers zu beschreiben.

Neben den oben genannten Maßnahmen lassen sich auch zusätzliche Maßnahmen in der Software implementieren, die verhindern, dass ein System bei einer kurzzeitigen Störung die Sicherheitsfunktion ausführt. Entsprechende Filtermaßnahmen erfordern einen zusätzlichen zeitlichen Aufwand. Daher sind diese Verfahren nur dann zulässig, wenn dadurch die resultierende Übertragungszeit die Prozesssicherungszeit nicht überschreitet.

Nach einem Arbeitspapier der ISA S84 Working Group 1 (WG1) darf ein sicherheitsgerichteter Bus für die Übertragung von sicherheitsrelevanten Nachrichten nicht mehr als die halbe Prozesssicherungszeit, bezogen auf die schnellste Sicherheitsfunktion, beanspruchen.

Eine dauerhafte Funktionsstörung durch mechanische Einflüsse kann nicht mit EMV- oder softwaretechnischen Maßnahmen, sondern nur mit Redundanz begegnet werden.
Neben der elektrischen Eignung einer Busleitung für ein gewähltes Bussystem, ist dessen mechanische und stoffresistente Eignung für die jeweilige Umgebung zu beachten.

5 Anforderung an die Konfiguration und Parametrierung

Bei der Parametrierung eines Sicherheitssystems mit bustauglichen Komponenten sind umfangreiche Einstellungen vorzunehmen. Diese Einstellungen werden mit Hilfe von speziellen Software-Programmen durchgeführt, die es dem Anwender ermöglichen, das Bussystem entsprechend der Anwendung zu konfigurieren und Kenngrößen zu parametrieren.

Unter der **Konfiguration** eines Busses wird u. a. die Festlegung der Topologie verstanden. Die **Parametrierung** eines Busses legt beispielsweise Grundlegende Buskenngrößen fest.

5.1 Zugangskontrolle

Das Ausmaß einer falschen Konfiguration oder Parametrierung eines Bussystems für sicherheitsgerichtete Anwendungen kann Schäden mit nicht absehbaren Folgen haben. Nach **12.BImSchV** ist die Konfiguration vor Eingriffen Unbefugter zu schützen. Daher kommt der autorisierten, sachkundigen Person, welche die Konfiguration durchführt oder ändert, eine zentrale Sicherheitsverantwortung zu.

Personen, die ein Bussystem konfigurieren und parametrieren, müssen für diese Aufgabe ausreichend qualifiziert sein. Dies muss durch geeignete Schulungsmaßnahmen sichergestellt werden.

Darüber hinaus fordert die IEC 61511-1 im Abschnitt 11.7.2 eine Zugangskontrolle für die Instandhaltungs- und Engineering-Schnittstellen bezüglich bestimmter Funktionen.

5.2 Konfigurierung/Parametrierung

Die Tätigkeit des Konfigurierens und Parametrierens wird in der Regel mit Hilfe eines PC durchgeführt, dessen Hardware und zugehörige Software als ungeprüft und nicht fehlersicher im Sinne einer Norm angesehen werden muss. Es muss aber sichergestellt sein, dass die ins Zielsystem geladenen Daten dort auf Plausibilität und Integrität überprüft und anschließend zur Validation durch den Bediener wieder auf den PC geladen werden.

Die Änderung einer Konfiguration im laufenden Betrieb („Online-Betrieb“) einer Anlage kann möglich sein. Allerdings ist zu beachten, dass während des Einspielens einer neuen Konfiguration die entsprechende Komponente nicht mehr unbedingt in der Lage ist, ihre Sicherheitsaufgabe zu erfüllen.

Die Konfigurationssoftware sollte Bestandteil der Prüfung und Zertifizierung sein, um sicher zu stellen, dass die sicherheitsrelevanten Abläufe folgerichtig umgesetzt worden sind. Darüber hinaus sollte dieser Prozess im Sicherheitshandbuch festgelegt sein.

5.3 Historienaufzeichnung

Unter der Historienaufzeichnung ist hier die Aufzeichnung vergangener Konfigurationen, Parameter, Fehler (Error Log) oder Ereignisse (Event Log) zu verstehen, welche im Zielsystem (bei jedem Teilnehmern eines Sicherheitsbusses) hinterlegt sind. Alte Konfigurationen und Parameter werden vom Hersteller aus haftungsrechtlichen Gründen hinterlegt, um im Falle eines Versagens der Schutzeinrichtung aufklären zu können, ob ein Ausfall der Schutzeinrichtung auf eine Fehlkonfiguration zurück zuführen ist. Eine Fehler- oder Ereignisliste dient dazu, vergangene Abläufe zu analysieren.

Nicht zu verwechseln ist die Historienaufzeichnung mit der nach IEC 61511-1 Abschnitt 17 geforderten **dokumentierten** Änderungsverfolgung. Die dokumentierte Änderungsverfolgung muss durch den Anwender im Zusammenhang mit den Anforderungen an das Management zur Funktionalen Sicherheit erfolgen.

5.4 Diagnosewerkzeuge

Neben der Möglichkeit einen Bus oder dessen Busteilnehmer zu konfigurieren oder zu parametrieren, besteht häufig zusätzlich die Möglichkeit der Busdiagnose. Die entsprechenden Diagnosewerkzeuge sind aufgrund ihrer Aufgabe „online“ mit dem Bussystem verbunden und „hören“ den Datenverkehr ab. Diagnosewerkzeuge haben in der Regel keinerlei sicherheitstechnische Relevanz, können aber dazu beitragen Systeme bezüglich ihrer Verfügbarkeit zu optimieren. Der Nachweis der Rückwirkungsfreiheit zum sicherheitsrelevanten System ist zu erbringen.

6 Sicherheitsbetrachtungen nach IEC 61508 bzw. IEC 61511

6.1 Anwendungsbereich von Bussystemen

Die hier zu betrachtenden sicherheitsgerichteten Bussysteme, haben die Aufgabe, Daten, **unabhängig** von deren Herkunft oder Bedeutung, entsprechend des geforderten Sicherheits-Integritätslevels, sicher von der Informationsquelle zur Informationssenke zu übertragen. Die Anforderungen an das Bussystem hängen also nicht von der Art der Daten ab.

Für den Anwendungsbereich des Bussystems selbst spielt es keine Rolle, ob die von ihm zu transportierenden Daten innerhalb einer Prozessanlage, einem Labor, einer Vielzweckanlage, einer Produktion (Konti, Batch, Semibatch) oder einem Lager (Einstoff, Vielstoff) ausgetauscht bzw. übertragen werden. Es muss lediglich sicherstellen, dass diese Daten entsprechend dem Sicherheits-Integritätslevel übertragen werden.

6.2 Anforderungen an die Beurteilung der Funktionalen Sicherheit

6.2.1 Unabhängigkeitsgrad bei der Beurteilung der Funktionalen Sicherheit

Die IEC 61508-1 Tabelle 5 beschreibt den erforderlichen minimalen Unabhängigkeitsgrad für die Beurteilung der funktionalen Sicherheit in Abhängigkeit vom Sicherheits-Integritätslevel. Bis SIL 3 ist es jedem Unternehmen selbst überlassen selbst festzustellen, wer die Beurteilung durchzuführen hat.

Die IEC 61511-1 legt keine weiteren Anforderungen an den Grad der Unabhängigkeit bei der Beurteilung der Funktionalen Sicherheit fest.

Bei einer Beurteilung der Funktionalen Sicherheit durch den Hersteller selbst besteht die Gefahr, dass das subjektive Betrachtungen in die Beurteilung einfließen. Daher wird im Rahmen dieses Forschungsvorhabens die Zertifizierung eines Bussystems von einer unabhängigen Stelle empfohlen.

6.3 Anforderungen an die Dokumentation

Der Teil 1, Kapitel 5 der IEC 61508 beschäftigt sich mit den Anforderungen an die Dokumentation, welche für den gesamten Sicherheitslebenszyklus zu erstellen ist. Für die Lebenszyklusphase Installation/Errichtung, Betrieb, Wartung werden dem Anwender in der Regel drei Dokumente zur Verfügung gestellt:

- Einbauanleitung („Beipackzettel“),
- Betriebsanleitung, Sicherheitshandbuch
- Bussystemhandbuch

Diese Dokumente sind Bestandteil der sicherheitstechnischen Begutachtung.

6.4 Maßnahmen zur Fehlervermeidung

Die IEC 61508 fordert die Erbringung des Nachweises über die Durchführung von Maßnahmen zur Fehlervermeidung über den gesamten Lebenszyklus des Sicherheitssystem. Der Umfang der durchzuführenden Maßnahmen ist abhängig vom angestrebten SIL. Die durchgeführten Maßnahmen sind entsprechend orientiert am Lebenszyklus zu dokumentieren.

Hierbei müssen insbesondere die Phasen Planung, Installation, Betrieb, Wartung, Modifikation, sowie Außerbetriebnahme betrachtet werden.

Bestandteil dieser Dokumente sollten Checklisten der Komponentenhersteller sein, aus denen hervorgeht, wie eine erfolgreiche Verifikation der spezifizierten Sicherheitsfunktionen durchgeführt werden kann.

6.5 Sicherheitstechnische Kenngrößen

Die Nennung von sicherheitstechnische Kenngrößen (HFT, SFF, PFD, PFH, Proof-Testintervall) in Produkt- oder Systemhandbüchern ist insbesondere für die Personen erforderlich, welche eine Sicherheitskette und deren Komponenten hinsichtlich des angestrebten SIL beurteilen.

Neben den genannten sicherheitstechnischen Kenngrößen sind auch die im Sicherheitshandbuch beschriebenen Restriktion zu beachten. Darüber hinaus haben diese Kenngrößen eine produktbeschreibende Funktion.

6.5.1 Rechnerische Ermittlung der sicherheitstechnischen Kenngrößen

Die IEC 61508 unterscheidet zwei Bewertungsverfahren, um eine Aussage über die Eignung einer Sicherheitseinrichtung zu treffen. Es müssen immer beide Bewertungsverfahren durchgeführt werden.

1. Bewertungsverfahren:

Das erste Verfahren hat die Hardware Fault Toleranz (HFT) und die Safe Failure Fraction (SFF) zum Gegenstand. Hier wird nach dem Grundsatz verfahren, dass ein einfach gestaltetes System (einkanalig) eine Diagnose mit sehr hoher Wirksamkeit besitzen muss, um Fehler im System zu erkennen.

Hingegen reicht bei einem aufwendig gestaltetem System (mehrkanalig) eine Diagnose mit einer geringeren Wirksamkeit, da hier mehrere Kanäle unabhängig voneinander die Schutzfunktion auslösen können.

Die Struktur eines Sicherheitssystems (ein oder mehrkanalig) drückt sich in der HFT aus. Diese, in Verbindung mit dem als Ziel gesetzten SIL, ergibt die zu erreichende SFF, die wesentlich durch die Wirksamkeit der Diagnose bestimmt wird.

2. Bewertungsverfahren

Das zweite Bewertungsverfahren besteht in der Berechnung der Ausfallwahrscheinlichkeiten PFD, PFH, und basiert auf den Daten der FMEA.
Als Berechnungsverfahren sind die Anwendung von Zuverlässigkeitsblockdiagrammen oder Markov - Modellen gebräuchlich.

Die Wahrscheinlichkeit eines gefährlichen Ausfalls ist nach dem Einschalten eines geprüften Systems sehr klein. Mit fortlaufender Betriebszeit steigt die Ausfallwahrscheinlichkeit eines Sicherheitssystems bei Anforderung an. Überschreitet dieser Wert einen zulässigen Grenzwert, so muss ein Proof-Test durchgeführt werden.

Theoretisch wäre das System durch einen solchen vollständigen Proof-Test für eine unbegrenzte Zeit einsetzbar. Dagegen spricht allerdings, dass die Ausfallraten bei den Berechnungen als konstant angenommen werden, was in der Praxis nicht zutrifft. Die Konstanz der Ausfallraten der Komponenten ist nur für einen Zeitraum von 8 bis 12 Jahren gegeben.

6.5.2 Ableitung sicherheitstechnischen Kenngrößen aus Felddaten

Inwieweit sich aus Felddaten Rückschlüsse auf einzelne Komponenten oder auf die Sicherheit eines Bussystem ziehen lassen ist abhängig von der Detailtiefe einer solchen Statistik. Liegen Felddaten detailliert vor, so können diese das Vertrauen in die Eignung eines Bussystems erhöhen. In den Standards wird hierbei vom Nachweis über den Ansatz der Betriebsbewährung gesprochen.

7 Zusammenfassung

Für die sicherheitsgerichtete Kommunikation ist es zwingend erforderlich, dass die in IEC 61508 genannten Fehler durch die implementierten Maßnahmen zur Fehlerbeherrschung erkannt werden und eine geeignete Reaktion erfolgt. Auch die eingesetzten Buskomponenten müssen, wie jede Teilkomponente der Sicherheitskette, entsprechend des angestrebten SIL qualifiziert sein.

Jedoch ist für den Einsatz von sicherheitsgerichteten Bussystemen und deren Komponenten in der chemischen Industrie nicht einzig und alleine ausreichend, dass diese Systeme von einer unabhängigen Stelle zertifiziert sind, vielmehr kommt es darauf an, die in der begleitenden Dokumentation beschriebenen **Schnittstelleninformation** herauszuarbeiten und die Hinweise aus den Sicherheitshandbüchern der einzelnen Hersteller entsprechend der speziellen Anforderungen der Anwendung richtig umzusetzen. Basierend auf diesen Information müssen Pläne zur Verifikation und Validierung des Gesamtsystems erstellt werden, um den betroffenen Lebenszyklusphasen der Anlage, Installation, Betrieb, Wartung, Modifikation und Außerbetriebnahme, gerecht zu werden.

Die prinzipiellen Aspekte der Anwendung von Bussystemen (ähnlich wie die Prinzipien bei der Sicherung von Anlagen mit Mitteln der Prozessleittechnik) in der Anlagensicherheit der Chemie Industrie sollten dem Behördenprüfer vertraut sein.

Als wesentliches Ergebnis enthält der Hauptbericht eine Checkliste, die eine allgemeine Hilfestellung bei der Bewertung liefert. Diese Checkliste erhebt nicht den Anspruch einer einfachen ja/nein Analyse, sondern dient vielmehr dazu, die komplexe Kommunikationstechnik transparenter zu machen und einen sicherheitstechnischen Gesamteindruck zu bekommen.

Darüber hinaus hilft sie gezielte Fragen an den Betreiber und ggf. an den Hersteller zu formulieren.

Die Schnittstelleninformationen in Verbindung mit der Checkliste gestatten eine Bewertung zu einem in der Anlagensicherheit der chemischen Industrie angewandten Bus-Systems.

Indexverzeichnis

Normen und Literaturverzeichnis

12.BImSchV

IEC 61508

IEC 61511

VDI/VDE 3687

VDI/VDE 2180

NAMUR-Empfehlung NE 74

NAMUR-Empfehlung NE 93

NAMUR-Empfehlung NE 97

Grundsatzpapier GS - ET - 26

Fachartikel „EMV - gerechte Projektierungshilfen“, ETZ Heft 1-2/1999

Reinert, Schaefer; „Sichere Bussysteme für die Automation“,
ISBN 3-7785-2797-5