Landesumweltamt Nordrhein-Westfalen

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

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.

Im weiteren Verlauf werden sicherheitstechnische Festlegungen genannt, die für dieses Forschungsvorhaben relevant sind und somit entweder Anforderungen für die verfahrenstechnische Industrie beschreiben oder aus denen Anforderungen für die Bewertung von Bussystemen für die sicherheitsrelevante Kommunikation abgeleitet werden können.

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. Unter anderem fordert diese Verordnung, dass die Betriebsbereiche mit ausreichenden Warn-, Alarm- und Sicherheitseinrichtungen auszurüsten sind und dass bewährte sicherheitstechnische Konzepte, wie z. B. Redundanz, Diversität, Verwendung von zuverlässigen Komponenten, anzuwenden sind. Darüber hinaus sind sicherheitsrelevante Teile des Betriebsbereiches vor Eingriffen Unbefugter zu schützen. Des weiteren beschreibt die **12.BImSchV** im §6 „Ergänzende Anforderungen“ im Abschnitt 1 Anforderungen für die Errichtung, den Betrieb, die Wartung und Reparatur von sicherheitsrelevanten Anlagenteilen. In diesem Abschnitt werden Anforderungen beschrieben, die zum Einen der Vermeidung von Fehlern und zum Anderen der Verifizierung des Sicherheitssystem dienen.

Der Betreiber hat hierfür Unterlagen zur Verfügung zu stellen, die beschreiben, wie die Anforderungen umgesetzt werden können, z. B. Prüfvorschrift für Funktionstest. Auch im Zusammenhang mit einem **Sicherheitsmanagementsystem** fordert die **12.BImSchV** eine nahezu lückenlose Dokumentation der einzelnen Phasen der Lebenszyklen und eine eindeutige Zuordnung der Verantwortungsbereiche.
Die genannten Anforderungen lassen sich in ähnlicher Form in der IEC 61508 wiederfinden.
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 Basisnorm **IEC 61508** beschreibt die Anforderungen an E/E/PES Sicherheitssysteme (elektrische/elektronische/programmierbare elektronische Systeme). Hierbei werden allen Komponenten einer Sicherheitskette betrachtet, die für die erfolgreiche Ausführung der definierten Sicherheitsfunktionn erforderlich sind. Es wird der gesamte Lebenszyklus des Sicherheitssystem und der daran beteiligten Komponenten, beginnend bei der Konzeptphase bis hin zur Außerbetriebnahme, betrachtet. Darüber hinaus fordert die IEC 61508 die Durchführung des Management der Funktionalen Sicherheit für jede einzelne Lebenszyklusphase, in deren Verlauf lückenlos die Vorgehensweise und der Nachweis zur Funktionalen Sicherheit dokumentiert werden muss. Es werden je nach angestrebten Safety Integrity Level (SIL) für die Hardware und Software niedrige, mittlere oder höhere Anforderungen an die Umsetzung von Maßnahmen zur Fehlerbeherrschung und Durchführung von Maßnahmen zur Fehlervermeidung gestellt.

Da 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.

Darüber hinaus werden in der IEC 61508-2 explizit im Abschnitt 7.4.8 Anforderungen an die Datenkommunikation beschrieben. Bei der Kommunikation müssen die zu unterstellenden Fehler: Wiederholungen, Verlust, Einfügung, falsche Abfolge, Verfälschung, Verzögerung und Masquerade berücksichtigt und beherrscht werden. Für diese unterstellten Fehler muss eine Abschätzung der Restfehlerwahrscheinlichkeit durchgeführt und diese Wahrscheinlichkeit bei der Abschätzung des Ausfallgrenzwertes für eine Sicherheitsfunktion berücksichtig werden. Für die Berechnung der Restfehlerwahrscheinlichkeit wird auf die EN 50159 verwiesen.

Ein Arbeitskreis der ISA (The Instrumentation, Systems and Automation Society) diskutiert Detailfragen dieser Anforderungen, z. B. hinsichtlich des Verhaltens bei Verzögerung von Daten in netzwerkverbindenden Informationseinrichtungen (z. B. Routern oder Bridges) und die Anforderungen an Konfigurationswerkzeuge und deren Zugangskontrollmechanismen.

Die Anwendungsnorm **IEC 61511-1** beschreibt die Anforderungen an die Funktionale Sicherheit in der Prozessindustrie. Die IEC 61511-1 lehnt sich an die IEC 61508 an und setzt deren Anforderungen auf das Anwendungsgebiet der Prozessindustrie, unter Berücksichtigung anwendungsspezifischer Anforderungen, um. Dieser Standard richtet sich nicht an die Hersteller der Komponenten, sondern an die Anwender der nach IEC 61508 hergestellten Komponenten.
Gleichermaßen wie in der IEC 61508 betrachtet die IEC 61511-1 die gesamte Sicherheitskette.

Die Kommunikation, die hierbei auch durch eine Bussystem realisiert werden kann, wird als ein Bestandteil dieser Kette betrachtet. Daher gelten die Anforderungen gleichermaßen für Bussysteme in der Prozessindustrie.

Dieser Standard erlaubt den Einsatz eines Bussystem unter der Bedingung, dass dessen Gesamtsicherheit den Zuverlässigkeitsanforderungen der von ihm bedienten sicherheitstechnischen Funktion entspricht. Der Nachweis der Eignung des Bussystems erfolgt auf Basis der IEC 61508.

Die Richtlinie **VDI/VDE 3687** hat sich, ähnlich dem hier vorliegenden Forschungsvorhaben, dem Thema „Auswahl von Feldbussystemen durch Bewertung ihrer Leistungseigenschaften für industrielle Anwendungsbereiche“ gewidmet. Allerdings bezieht sich diese Richtlinie nur auf nicht sicherheitsgerichtete Feldbussysteme. Neben umfassenden Anforderungstabellen und Beispielen aus der Fertigungs-, Prozess-, Gebäude-, Ver- und Entsorgungstechnik sowie ausführlichen Checklisten werden Tabellen mit den Leistungsmerkmalen der einzelnen Systeme dargestellt.
Aus diesen Tabellen können Erkenntnisse für das aktuelle Forschungsvorhaben gezogen werden, wobei die Angaben hinsichtlich der sicherheitstechnischen Relevanz bzw. ihrer Eignung genauer zu bewerten oder zu erweitern sind.

Die Richtlinie **VDI/VDE 2180** beschäftigt sich mit der Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT). Blatt 2 dieser Richtlinie nennt, bezogen auf das aktuelle Forschungsvorhaben, grundsätzliche Auswahlkriterien einer PLT-Schutzeinrichtung. Da diese Schutzeinrichtung auch aus einer (S)SPS (Sichere Speicher Programmierbare Steuerung) bestehen kann und diese in der Regel über eine Feldkommunikation verfügt, können die grundsätzlichen Auswahlkriterien der Richtlinie auch auf Sicherheitsbussysteme abgebildet werden.

Im Blatt 5 der Richtlinie wird auf den Einsatz von sicherheitsgerichteten speicherprogrammierbaren Steuerungen (SSPS) eingegangen.

Die hier genannten Anforderungen beziehen sich nicht nur auf die Hardware, sondern erstrecken sich auch auf die Dokumentation, Konfigurierung/ Parametrierung und Wartung der Steuerung. Alle Anforderungen lassen sich ebenso auf Einrichtungen für die Übertragung von sicherheitsgerichteten Daten übertragen. Eine Überarbeitung dieser Richtlinie ist in Arbeit, so dass eine Annährung an die internationalen Standards IEC 61508 und IEC 61511 zukünftig zu erwarten ist bzw. wünschenswert wäre.

Die **NAMUR-Empfehlung NE 31** referenziert die DIN V 19250. Diese wiederum wird in 2004 zurückgezogen. Wesentliche Elemente dieser Norm sind jedoch in die IEC 61508 eingeflossen.

Die **NAMUR-Empfehlung NE 74** nennt globale und spezielle Anforderungen an Feldbussysteme, deren Komponenten und (Software-) Werkzeuge sowie die Voraussetzungen, welche erfüllt sein müssen, damit diese in der Prozess-technik einsetzbar sind.

Die **NAMUR-Empfehlung NE 93** beschreibt eine Vorgehensweise zur Schaffung einer einheitlichen Grundlage, um mit Hilfe von Felddaten die sicherheitstechnischen Kenngrößen PFD/PFH zu ermitteln.

Die **NAMUR-Empfehlung NE 97** behandelt das Thema „Feldbusse für Sicherungsaufgaben“ und geht daher als themenverwandte Erkenntnisquelle besonders in das aktuelle Forschungsvorhaben mit ein.
Hier wird beschrieben, für welche Komponenten ein Zertifizierungsverfahren sinnvoll ist und für welche die Betriebsbewährung ausreicht.

Neben den Bussystemen und deren Konfigurations- und Parametrierwerkzeugen wird auch die Remote I/O-Technik betrachtet. Das Thema Anlagenverfügbarkeit ist ebenso Bestandteil dieser Empfehlung.

Im **Grundsatzpapier GS - ET - 26** des BIA (Berufsgenossenschaftliches Institut für Arbeitsicherheit) wird auf die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“ eingegangen. Es bildet die Grundlage für die Beurteilung von sicherheitsgerichteten Busprotokollen (Safety Layer) im allgemeinen.

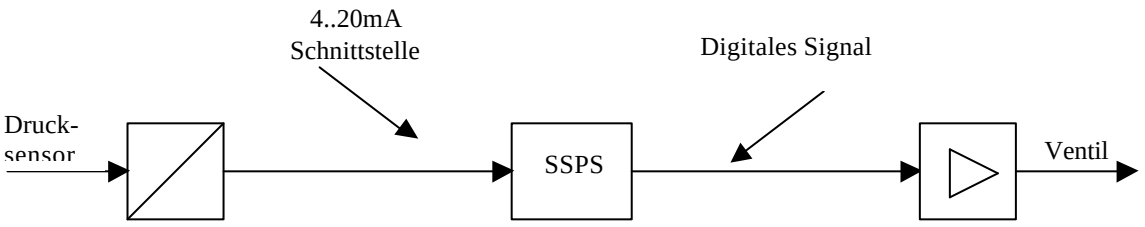
Neben den oben genannten Quellen und sicherheitstechnischen Festlegungen gibt es eine Reihe von **mitgeltenden Standards**. Diese betreffen z. B. die elektrische Sicherheit, Umwelteignung (Klima/Temperatur, mech. Festigkeit, EMV usw.) oder den Einsatz im Ex-Bereich. Die entsprechenden Anforderungen sind oft in produktspezifischen Normen (Produktnormen) oder anwendungsspezifischen Normen zusammengefasst. Sind Produktnormen für ein Produkt nicht oder noch nicht verfügbar, so gelten die übergeordneten Produktfamiliennormen.

Publikationen wie Fachartikel in Fachzeitschriften dienen der Wiedergabe des Standes der Technik und runden die Erkenntnisquellen für das aktuelle Forschungsvorhaben ab.

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.

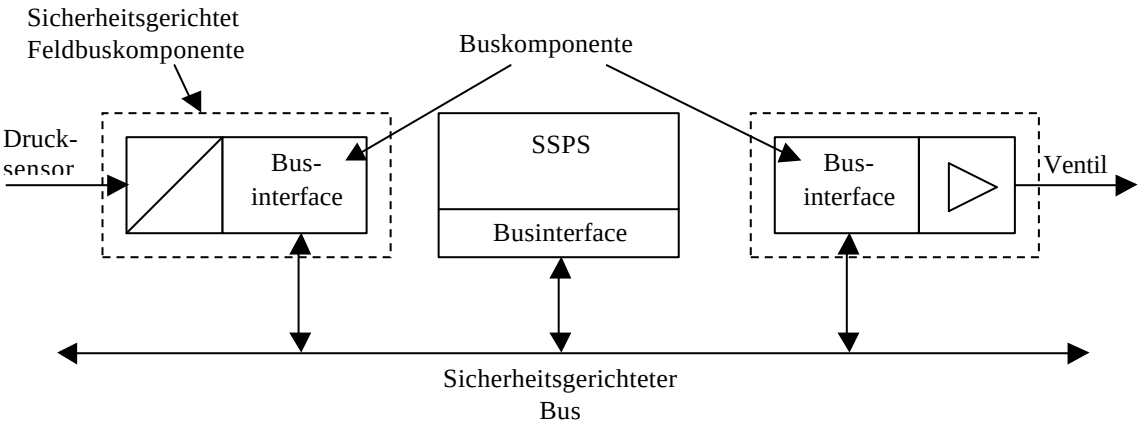
Bei der konventionellen Technik wird zunächst eine physikalische Größe mit Hilfe eines Umsetzers in eine standardisierte elektrische Größe z. B. 4.. 20 mA umgesetzt und diese einer Überwachungseinheit (z. B. SSPS) zugeführt. Diese Überwachungseinheit löste die Schutzfunktion bei Überschreitung eines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



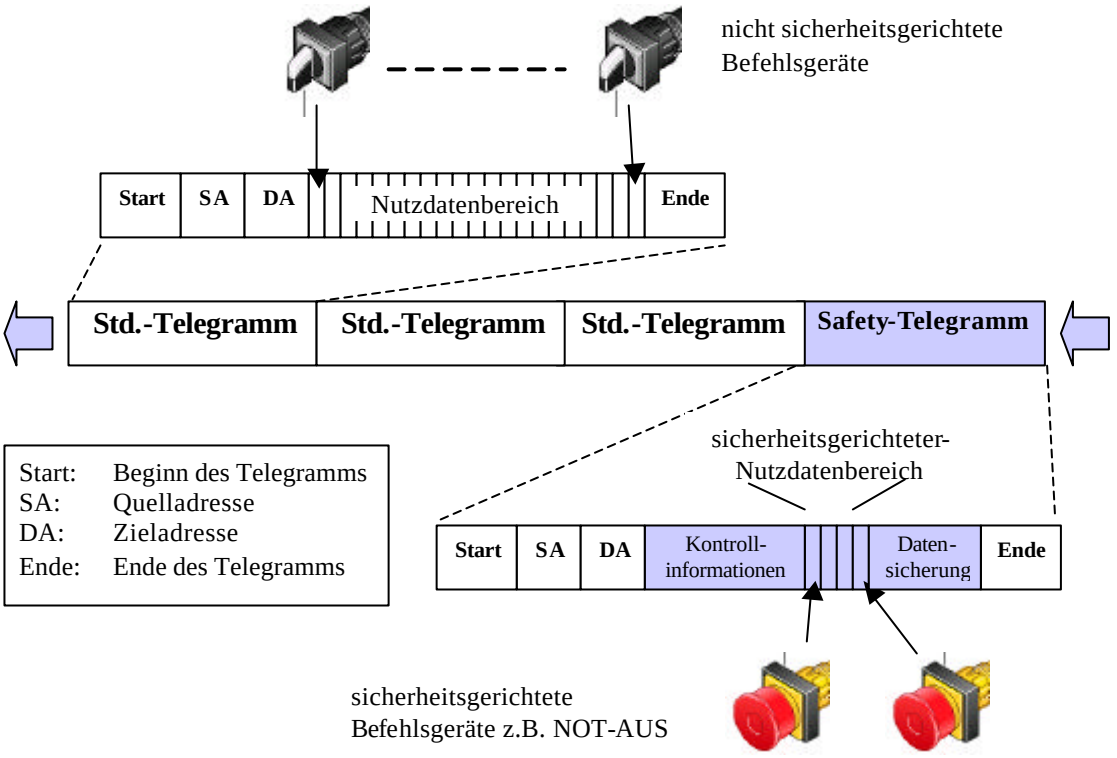
Bei der Realisierung dieser Funktion mit einem Bussystemen wird dem Umsetzer ein weiterer Baustein, ein Businterface, nachgeschaltet und dem Ventil vorgeschaltet. Dieses setzt die technische Größe des Umsetzers als digitalen Wert in ein festspezifiziertes Kommunikationsprotokoll ein. Die Überwachungseinheit 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.



Die Umsetzung der sicherheitsgerichteten Informationen in ein definiertes, sicheres Protokoll zeigt das nachfolgende Beispiel:



Wie zu erkennen ist, wird der Nutzdatenbereich eines Standardtelegramms in der Regel von sicherheitsgerichteten Nutzdaten und deren Kontroll- und Datensicherungsmaßnahmen belegt.

Hieraus ergibt sich, dass die zuübertragende Datenmenge eines sicherheitsgerichteten Protokolls immer kleiner ist als bei nicht sicherheitsgerichteten Protokollen.

3.1 Herkömmliche 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 sammeln Informationen von Aktoren/Sensoren, welche sich im Feld befinden über standardisierte Strom- und Spannungsschnittstellen und übermitteln diese über Feldbusse an die Prozessnahen Komponenten, beispielsweise SPS.

Dieser Einsatz bezeiht 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. Das Vertrauen aufgrund vorliegender Erfahrungen in diese bewährte Technik für sicherheitsrelevante Aufgaben ist zur Zeit noch größer als in Bussysteme, die für nicht sicherheitsrelevante Anwendungen entwickelt worden sind.
Beim Einsatz von Bussystemen für sicherheitsrelevante Aufgaben muss grundsätzlich mindestens das gleiche Sicherheitsniveau wie bei Schutzsystemen in herkömmlicher Technik erreicht werden. Dies entspricht auch einer Anforderung aus der IEC 61511 hinsichtlicht des Einsatzes von Bussystemen für sicherheitsrelevante Kommunikation. Ein Bussystem, das die oben genannte Forderung nach mindestens gleichem Sicherheitsniveau gegenüber herkömmlicher Sicherheitstechnik erfüllt, wird als Sicherheitsbussystem bezeichnet.

3.2 Proprietäre Sicherheitsbussysteme

Unter einem proprietären Bussystem versteht man ein Bussystem, welches von einem Hersteller für eine bestimmte Anwendung definiert und entwickelt wurde und die Verwendung von Geräten anderer Hersteller mitunter ausschließt. Proprietäre Bussysteme sind anwendungsspezifisch optimiert hinsichtlich Teilnehmeranzahl, Datenmenge, Übertragungsrate, Reaktionszeit, Verkabelung oder Anschlusstechnik.

Maßnahmen gegen Umwelteinflüsse (Temperatur, EMV) sind ebenfalls anwendungsspezifisch implementiert.

Proprietäre Bussysteme werden in der Regel nur von jeweils einem Hersteller angeboten. Dieser bietet neben den Buskomponenten auch Unterstützung bei der Projektierung, Inbetriebnahme und Wartung an. Diese „One-Hand-Solutions“ haben für den Anwender den Vorteil einer umfassenden Unterstützung durch einen Hersteller.

An proprietäre Bussysteme, die als Sicherheitsbussysteme eingesetzt werden, sind die gleichen sicherheitstechnischen Anforderungen zu stellen wie an offene Sicherheitsbussysteme in denen Komponenten verschiedener Hersteller verwendet werden können.

3.3 Mischsysteme (Hybride offene Bussysteme)

Hybride Bussysteme, d. h. Bussysteme für die Übermittlung sowohl betrieblicher als auch sicherheitsgerichteter Daten, sind der Trend welcher sich auf dem Markt für offene Bussysteme abzeichnet.

Kennzeichen eines offenen Bussystems ist, dass es von vielen unabhängigen Anbietern in Form von verfügbaren Komponenten oder Know-How getragen wird. Anbieter und Anwender eines offenen Bussystems sind in Clubs, Interessengemeinschaften oder Nutzerorganisationen organisiert.

Aufgaben dieser Interessengemeinschaften sind die Standardisierung des Bussystems in Anwendungsbereichen, die Einleitung und Definition von technologischen Weiterentwicklungen und die Überwachung der Konformität von Buskomponenten.

Bezogen auf den Bereich der Sicherheitsbussysteme wurden vor Jahren entsprechende Aktivitäten der Interessenverbände gestartet.

Die allgemeinen Busspezifikationen wurden 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.

Die Vorteile einer solche Lösung sind:

- Konformitätsbestätigung der Funktionalität durch die Organisation
- Kompatibilität der Komponenten untereinander
- Großes Sortiment von Sicherheitskomponenten durch viele Anbieter
- Nutzung der bisherigen Infrastruktur
- Großes Erfahrungspotenzial über das Bussystem

4 Sicherheit und Verfügbarkeit

4.1 Allgemeines

Ein System wird als ausreichend sicher bezeichnet, wenn das verbleibende Risiko für Mensch und Umwelt kleiner ist als das Grenzrisiko (von der Gesellschaft für das System tolerierte Risiko). Sicherheit wird erreicht, indem durch technische und organisatorische Maßnahmen das Risiko, welches von einem System ausgeht unterhalb des Grenzrisikos reduziert wird.

Gerade 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. Darüber hinaus verleiten häufig unverfügbare Systeme dazu, die entsprechenden Schutzeinrichtungen zu manipulieren.

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, die Fehlfunktionen hervorrufen und die Schutzfunktion ungewollt auslösen können. Diese Störungen können kurzfristig oder dauerhafter auf die Komponenten einwirken.

Beispiele für Störungen mit kurzzeitiger Einwirkungsdauer sind:

- Ein- und Ausschaltspitzen beim Schalten von Motoren, Leuchtmitteln oder kapazitiven Lasten
- Büschelimpulse (Burst) infolge von geschalteten Induktivitäten (Schützen)
- Elektrostatische Entladungen (ESD) an Maschinen oder durch Bediener
- Energiereiche Entladungen (SURGE) infolge von Blitzeinwirkung

Beispiele für Störungen mit dauerhafter Einwirkungsdauer sind:

- Verwendung von Funkgeräten (z. B. Handy´s, Wakie-Talkie´s)
- gemeinsame Verlegung von Starkstromleitungen, Motorzuleitungen von Frequenzumrichtern und Signalleitungen (Busleitungen)
- Mechanische Überbelastung der Busleitung, welche zur Unterbrechung (Abriss) oder Kurzschluss (Überfahren mit Fahrzeugen, Quetschung) der Leitungen führt

Bezogen auf Bussysteme können durch diese Störungen einzelne oder ganze Folgen von Datenbits verfälsch werden. Die Erkennung eines Verlustes der Datenintegrität erfolgt mit den im Forschungsvorhaben 35/00 genannten Maßnahmen.

Scheinbar verhalten sich Sicherheit und Verfügbarkeit diametral zueinander.

4.2 Maßnahmen zur Erhöhung der Verfügbarkeit

Jeder der voran beschriebenen Störungen auf die Buskomponenten kann in ausreichendem Maße mit geeigneten Maßnahmen begegnet werden.

4.2.1 Maßnahmen zur Vermeidung von sporadischen Fehlern

Die Ursache für diese Art von Fehlern ist im wesentlichen in dem Einfluss von elektromagnetischen Störungen zu finden. Aus diesem Grund müssen alle beteiligten Komponenten eine entsprechende EMV-Robustheit für deren relevanten Einsatz besitzen.

Der mindest zu erbringende Nachweis ist die Konformitätserklärung des Komponentenherstellers, dass sein Produkt den Anforderungen des Gesetzes zur Elektromagnetischen Verträglichkeit entspricht. Anwendungs- und Produktnormen stellen darüber hinaus spezifische Anforderungen.

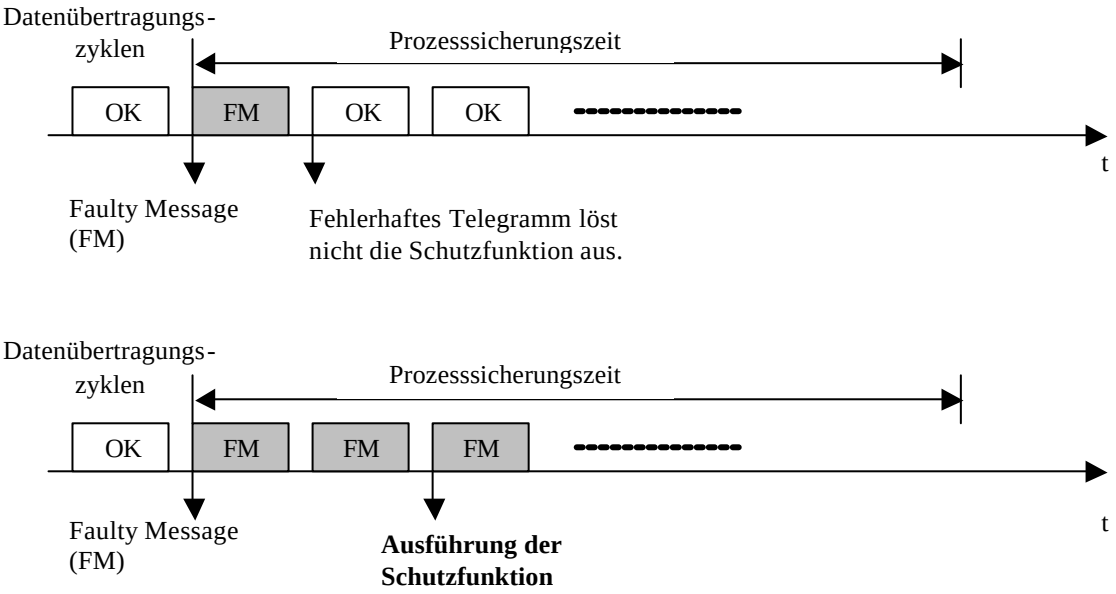
Neben dieser den Komponenten innewohnenden Robustheit gegenüber Störungen, spielt die richtige Verkabelung eine wesentliche Rolle. Der Komponentenhersteller muss Angaben machen, wie seine Geräte anzuschließen sind.

Bei Bussystemen spielt die richtige Verlegung der Busleitung eine entscheidende Rolle. Diese liegt im Feld und ist allen möglichen Einflüssen und Einkopplungen ausgesetzt. Die Wahl der Busleitung hat Einfluss auf die Störfestigkeit. Ein Lichtwellenleiter ist störfester als eine abgeschirmte Leitung und diese wiederum unempfindlicher als eine verdrillte Zweidrahtleitung. Alle zu treffenden Installationsmaßnahmen, die einen störungsfreien Betrieb sicherstellen und zu einer Erhöhung der Busverfügbarkeit führen, sind in dem zum Bussystem zugehörigen Sicherheitshandbuch des Herstellers zu beschreiben.
Darüber hinaus geben die Nutzerorganisationen der verschiedenen Bussysteme dem Anwender Hinweise, wie die Installation durchzuführen ist.

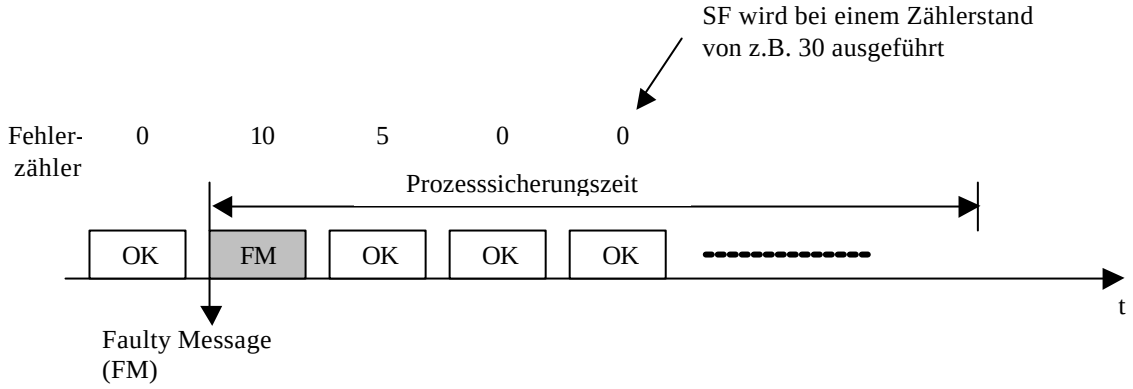
Neben den oben genannten Maßnahmen lassen sich auch zusätzliche Maßnahmen in der Software implementieren, die verhindern, dass ein System bei einer kurzzeitigen Störung die Sicherheitsfunktion ausführt.

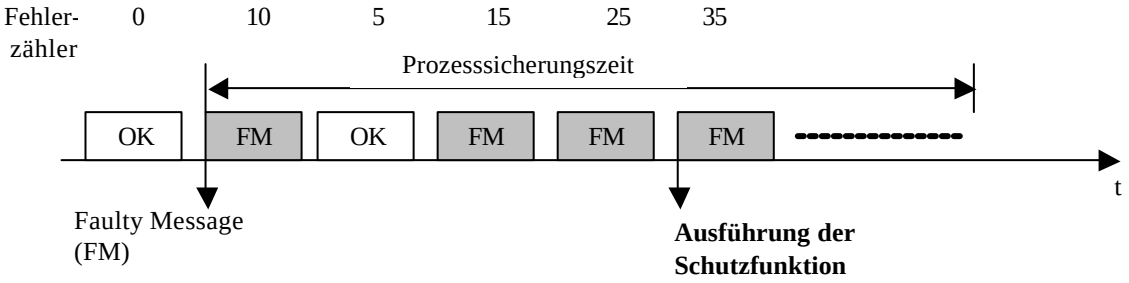
Im Folgenden werden beispielhaft Maßnahmen beschrieben, die zu einer Erhöhung der Verfügbarkeit führen:

1. Ein Datenübertragungsfehler muss über mehrere Übertragungszyklen existent sein, bevor die Sicherheitsfunktion ausgeführt wird.

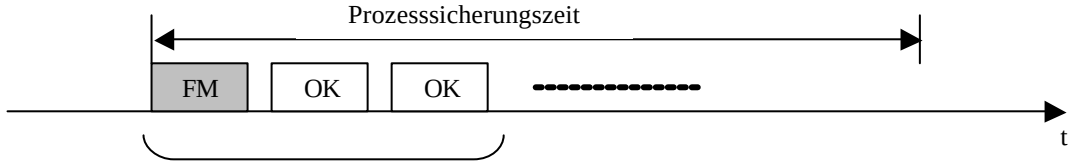


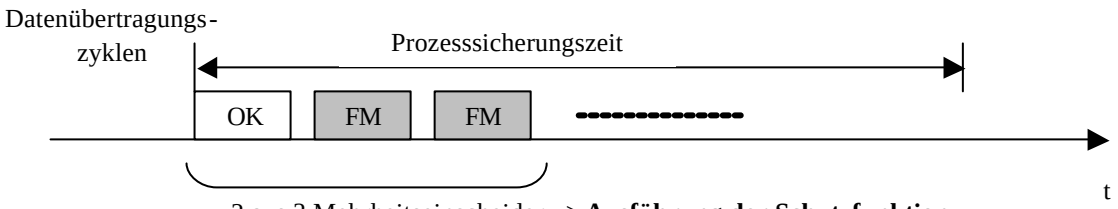
2. Es wird ein Fehlerzähler geführt, der bei Übschreitung eines definierten Wertes die Sicherheitsfunktion auslöst. Jede fehlerhafte Übertragung führt zu einer Erhöhung des Zählerstandes und jede fehlerfreie Übertragung zu einer Reduzierung. Bei diesem Verfahren kann eine Gewichtung der beiden Zustände erfolgen, wobei der fehlerhafte Zustand stärker zu gewichten ist.





3. Die Ergebnisse der Fehlerauswertung eingehender Datentelegramme werden einem Mehrheitsentscheider (Voter) zugeführt, der z. B. eine 2 aus 3 Bewertung durchführt.





Diese und weitere Verfahren sind nur dann zulässig, wenn eine mehrfache Datenübertragung zur Ausführung einer Sicherheitsfunktion bezogen auf die Prozesssicherungszeit toleriert werden kann. Die Prozesssicherungszeit muss also größer sein als die Summe der zur Auslösung der Schutzfunktion notwendigen Datenübertragungszyklen und Verzögerungszeiten der betroffenen Komponenten.

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.

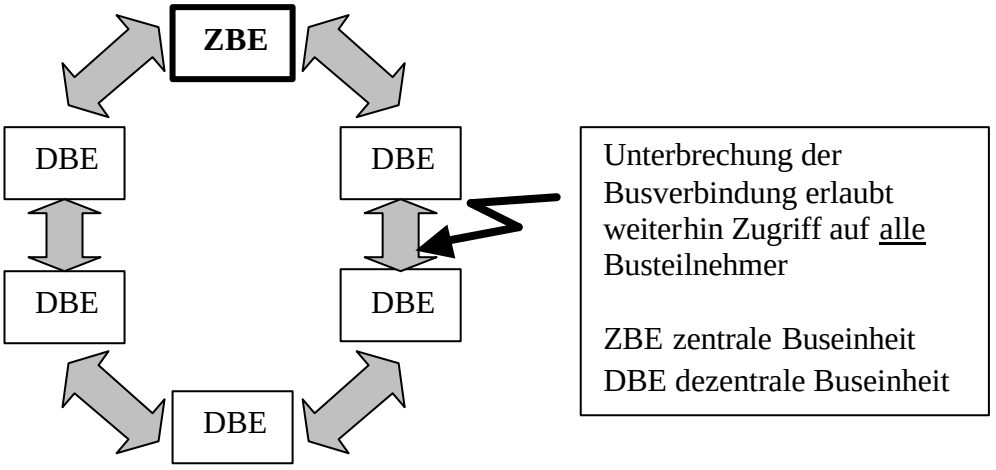
Die hier beispielhaft genannten Maßnahmen zeigen, dass ein einzelner, sporadischer Fehler nicht direkt zum Ausführen der Sicherheitsfunktion führen muss und somit die Verfügbarkeit einer Anlage erhöht werden kann, ohne den Grad der Sicherheit zu mindern.

4.2.2 Maßnahmen zur Vermeidung von dauerhaften Fehlern

Langanhaltende Störeinwirkungen über den Sekundenbereich hinaus durch Funkeinrichtungen, z. B. Mobiltelefone, sind mit den im vorangegangen Kapitel genannten EMV-Maßnahmen zu begegnen.

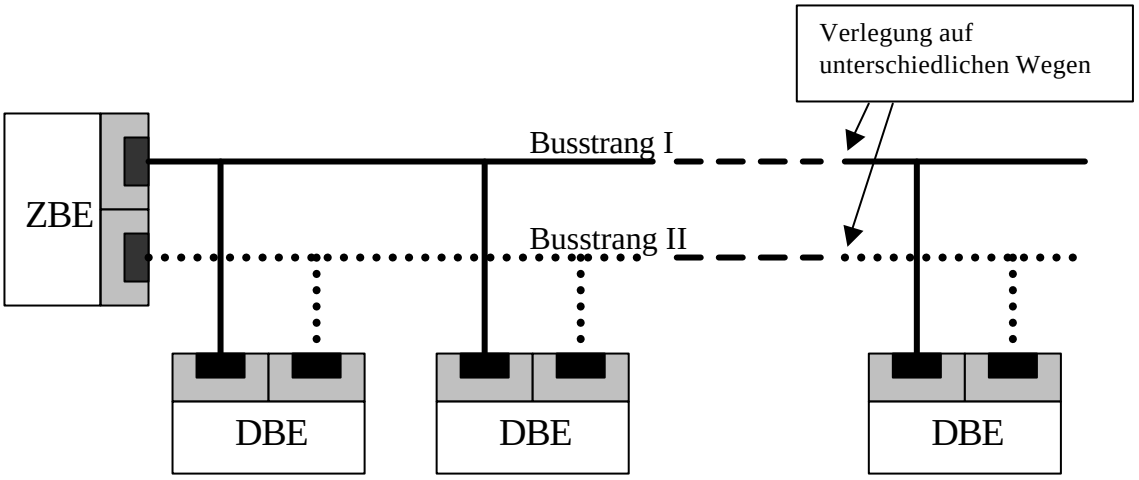
Eine dauerhafte Funktionsstörung durch mechanische Einflüsse kann nicht mit EMV- oder softwaretechnischen Maßnahmen sondern nur mit Redundanz beherrscht werden. Die Art der Redundanz hängt von der Topologie des Bussystems ab.

Bei der **Ringstruktur** eines Bussystems hat jeder Busteilnehmer zwei Wege für die Kommunikation.



Die Unterbrechung einer Strecke führt weder zu einer Beeinträchtigung der Sicherheit noch der unmittelbaren Verfügbarkeit. Der Ausfall einer Verbindung wird erkannt und kann im laufenden Betrieb behoben werden. Diese Bustopologie setzt allerdings voraus, dass das einzusetzende Bussystem als Ringstruktur ausgelegt werden kann.

Bei der **Linien- oder Sternstruktur** liegt keine der Struktur innewohnende Redundanz vor. Hier kann die Redundanz durch eine Verdopplung der gesamten Infrastruktur erreicht werden.



Voraussetzung für einen redundanten Busstrang ist, dass alle Geräte am Bus über eine Anbindung für eine zweite Schnittstelle und eine 2 von 2 Auswerteeinrichtung verfügen oder die Komponenten müssen doppelt vorhanden sein.

Wird mit einer mechanischen Beschädigung der Übertragungskabel gerechnet, sollten die redundanten Buskabel bevorzugt auf unterschiedlichen Kabelwegen geführt werden, damit bei einem Ausfall eines der beiden Kabelwege die Übertragung weiterhin über den zweiten Kanal gewährleistet ist (NAMUR Empfehlung NE 97).

Neben der elektrischen Eignung einer Busleitung für ein gewähltes Bussystem, ist dessen mechanische und die stoffresistente Eignung für die jeweilige Umgebung zu beachten. Eine Verstärkung des Mantels oder das Mitführen eines Entlastungsdrahtes sind hier nur beispielhafte Maßnahmen.

5 Anforderung an die Konfiguration und Parametrierung

5.1 Allgemeines

Bei der konventionellen Ausführung von Sicherheitssystemen beschränkt sich die Parametrierung der einzelnen Komponenten aus wenigen einfachen Einstellungen, die z. B. über Kodierschalter vorgenommen werden können. Bei der Parametrierung eines Sicherheitssystems mit bustauglichen Komponenten sind dagegen eine Vielzahl zusätzlicher Einstellungen vorzunehmen. Darüber hinaus ist auch das Bussystem selbst für den speziellen Einsatz anzupassen.

Diese Einstellungen werden mit Hilfe von speziellen Software-Programmen durchgeführt, die es dem Anwender ermöglichen, das Bussystem zu konfigurieren und Kenngrößen entsprechend der Anwendung zu parametrieren.

Unter der **Konfiguration** eines Busses wird u. a. verstanden:

- Festlegung der Topologie, z. B. Festlegung des Busmasters, Aufteilung eines Bus in verschiedene Stränge / Stichleitungen
- Auswahl und Einbindung der Geräte aus dem Gerätekatalog in die Topologie, z. B. digitale E/A-Baugruppen mit bestimmter Anzahl von Ein- oder Ausgängen, Frequenzumrichter, sichere Steuerung usw.

Die **Parametrierung** eines Busses legt beispielsweise fest:

- Grundlegende Buskenngrößen: Teilnehmeradressen, Übertragungsrate, Intervall mit der sich jeder Teilnehmer beim Busmaster meldet (Heart-Beat)
- Auswahl der einzelnen Gerätefunktionen gemäß der Gerätebeschreibung, wie beispielsweise die Festlegung von Filterzeiten, Grenzwerten oder die Vergabe von Bezeichner (Label) für den jeweilige Messkanal

5.2 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.
Neben dieser organisatorischen Maßnahme muss das Konfigurations- und Parametrierprogramm gegen unbefugte Nutzung geschützt sein. Diese Zugangskontrollen sind in der Regel aufgabenbezogen abgestuft, d. h. beispielsweise, dass die Konfigurationsebene und die Funktion für das Runterladen (Download) der Konfiguration in das Zielsystem durch verschiedene Passwörter getrennt sein muss. Hinweise zur richtigen Umsetzung dieses Zugriffschutzes finden sich in den Sicherheitshandbüchern der Hersteller.

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

5.3 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.

Dabei stellt sich folgende Frage:

Wie erfolgt die Verifikation der sicherheitsrelevanten Konfiguration- und Parameterdaten, welche über ein nicht fehlersicheres Gerät erstellt worden sind, im Zielsystem und wie kann man sicher sein, dass diese Daten den eingegebenen entsprechen?
Die im PC hinterlegten Konfigurations- und Parameterdatensätze müssen mit einer Signatur (CRC) gesichert sein. Das gleiche gilt für die Datenpakete, die vom PC an das Zielsystem (Download) und vom Zielsystem in den PC (Upload) übertragen werden. Auf der empfangenden Seite muss jeweils eine Überprüfung/Verifizierung des Signatur erfolgen.

Neben den Plausibilitätsüberprüfung der Konfigurationsdaten im PC, müssen die Daten auch im Zielsystem auf Plausibilität und Zulässigkeit für die jeweilige Hardware überprüft werden. Erst bei positiver Überprüfung dürfen die Daten als gültig übernommen werden.
Die vom Zielsystem nach einem Download eines neuen/geänderten Konfigurationsdatensatzes erhaltenen Daten werden verifiziert und zurück an den PC geschickt und dort softwaremäßig auf Gleichheit mit den ursprünglich eingegebenen Daten verglichen. Bei Ungleichheit erfolgt eine Fehlermeldung.

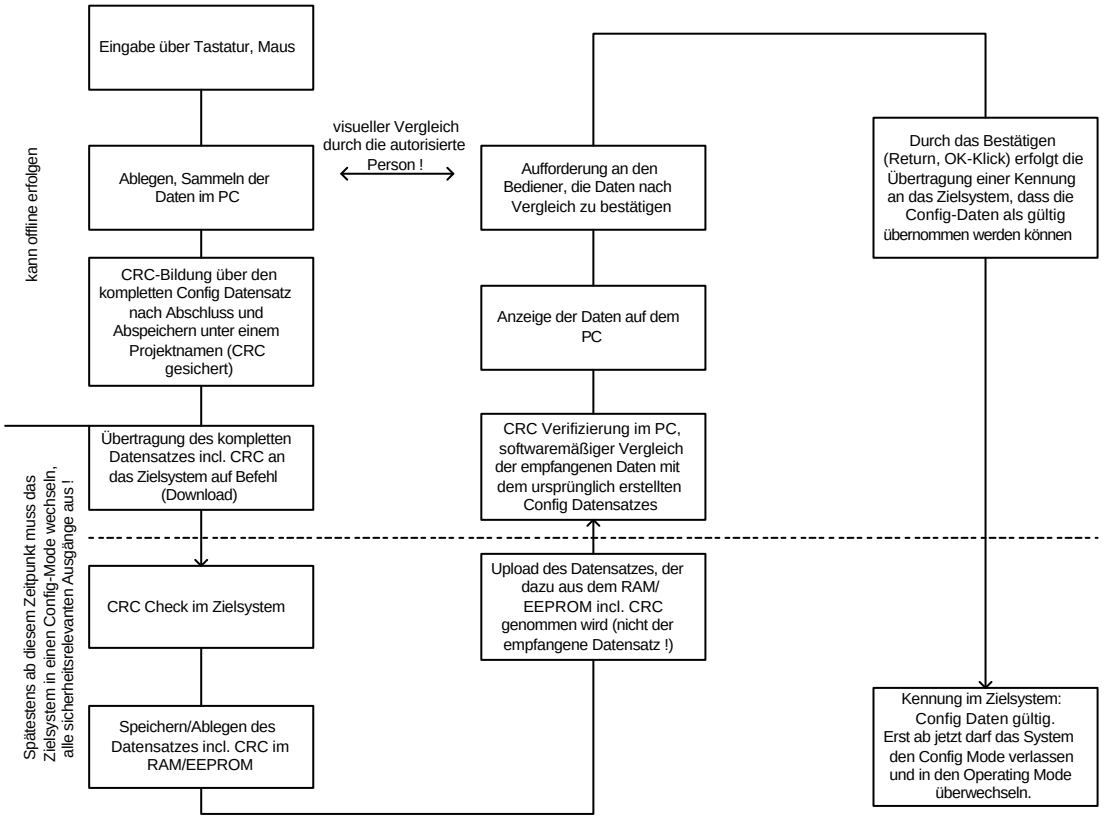
Stellt der softwaremäßige Vergleich der Daten im PC eine Gleichheit der Daten fest, so wird der Bediener anschließend zur Bestätigung der Daten und zur Übernahme aufgefordert. Der Bediener muss nach Abschluss der Konfigurationsprozedur durch einen Hinweis, den er bewusst bestätigen muss, aufgefordert werden, die Sicherheitsfunktionen des Gerätes zu verifizieren.

Es kommt der Person, welche die Konfiguration durchführt, eine zentrale Sicherheitsverantwortung zu.

Sie muss in jedem Fall als „Vergleicher“ zwischen den Daten, die sie am PC eingegeben hat, und den Daten, die sie durch Upload aus dem Zielsystem zurückerhält, fungieren und bewusst die Gültigkeit der Daten bestätigen.

Eine Konfiguration oder das Einstellen von Bus-/Komponentenparametern wird in der Regel im „Offline-Betrieb“, also ohne eine Verbindung zum Zielsystem erstellt und nach Abschluss ins Zielsystem runtergeladen. 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 folgende Abbildung zeigt eine mögliche Prozedur zur Erstellung eines Konfigurationsdatensatzes am PC mit den anschließenden Phasen Download, Upload, Verifizieren und Bestätigen.



Die hier beschriebene Prozedur stellt sicher, dass Daten eines Prozesses von einer autorisierten Person richtig in den sicherheitsrelevanten Teil einer Anlage gelangen und anschließend überprüft werden. Anstrengungen kriminellen Ursprungs, deren Ziel es ist, bewusst Schäden an Mensch oder Umwelt herbei zuführen wurden hier nicht betrachtet.

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

5.4 Historienaufzeichnung

Unter der Historienaufzeichnung ist hier die Aufzeichnung vergangener Konfigurationen, Parameter, Fehler (Error Log) oder Ereignisse (Event Log) zu verstehen, welche im Zielsystem (bei den 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.

Diese Daten haben keine direkte sicherheitstechnische Relevanz. Die Historienaufzeichnung von Konfigurationen oder Parametern ist dem Anwender weder durch die Dokumentation bekannt noch wird sie ihm zugänglich gemacht. Die Historie der Daten ist nur dem Hersteller des Produktes über eine separate, Passwort geschützte Zugangsebene zugänglich. Hingegen sind die Fehler- oder Ereignislisten dem Anwender zugänglich und stellen nützliche Werkzeuge während der Inbetriebnahme und Wartung dar.

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.

5.5 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 ohne in die Funktionen des Systems aktiv einzugreifen.

Diagnosewerkzeug bieten unter anderem folgenden Funktionen:

- Aufbau einer Punkt-zu-Punkt Verbindung vom Diagnosewerkzeug zu einem Teilnehmer, um die physikalische Verbindung zu überprüfen.
- Auslesen der Komponentenparameter
- Lesen von Eingangs- und Ausgangswerten
- Aufzeichnung von fehlerhaften Datenpaketen, Timeouts, Wiederholungen
- Busauslastung

Mit Hilfe der Diagnosewerkzeuge sind unter anderem Rückschlüsse auf die Installationsqualität eines Busses möglich. Eine unerwartet hohe Anzahl von fehlerhaften Datenpaketen kann ihre Ursache beispielsweise in fehlenden Abschlusswiderständen, zu langen Stichleitungen, defekten Leitungen und Anschlusstechnik haben, welches sich in Reduzierung der Verfügbarkeit wiederspiegelt.

Wichtig hierbei ist, dass die verwendeten Diagnosewerkzeuge, da sie ja in der Regel online am Bus sind, sich nicht sicherheitskritisch auswirken können. Hierbei sollte die Frage gestellt werden, ob diese Tools Bestandteil der Prüfung und Zertifizierung waren und der Nachweis der Rückwirkungsfreiheit im Verlauf der Prüfung erbracht worden ist. In der Regel ist die Verwendung der Werkzeuge nur im Zusammenhang mit bei der Prüfung ermittelten Einschränkungen bzw. Bedingungen möglich. Diese Bedingungen und Einschränkungen müssen im zugehörigen Sicherheitshandbuch enthalten sein und die korrekte Umsetzung muss bei der Abnahme des System verifiziert werden.

6 Sicherheitsbetrachtungen nach IEC 61508 bzw. IEC 61511

6.1 Bestimmung des Sicherheits-Integritätslevels (SIL)

Ausgangspunkt einer jeden sicherheitstechnischen Betrachtung ist die Frage: Welches Sicherheitsniveau muss die zu betrachtende Einrichtung erfüllen? Diese Frage wurde bereits im Rahmen des Forschungsvorhabens 35/00 „Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie“ unter Kapitel 3 behandelt und soll daher hier nicht weiter vertieft werden.

Wichtig hierbei ist festzuhalten, dass dem bei der Risikobetrachtung ermittelten Sicherheits-Integritätslevel alle Teile der Sicherheitskette zu entsprechen haben, also auch das Bussystem. 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 das Bussystem 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 sicher 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

Nachdem Maßnahmen und Verfahren zum Erreichen eines geforderten Sicherheits-Integritätslevels spezifiziert worden sind, stellt sich die Frage:

Wer oder welche Institution darf eine Beurteilung über die vorgesehenen und realisierten Maßnahmen abgegeben und das Bussystem nach positiver Beurteilung zertifizieren?

Die IEC 61508-1 Tabelle 5 beschreibt den erforderlichen minimalen Unabhängigkeitsgrad für die Beurteilung der funktionalen Sicherheit in Abhängigkeit vom Sicherheits-Integritätslevel.

Minimaler Unabhängigkeitsgrad	**Sicherheits-Integritätslevel (SIL)**			
	1	**2**	**3**	**4**
Unabhängige Person	++	++1	--	--
Unabhängige Abteilung	O	++2	++1	--
Unabhängige Organisation	O	O	++2	++

++ der festgelegte Unabhängigkeitsgrad ist als Minimum für die bestimmte Auswirkung ... oder den Sicherheits-Integritätslevel ... besonders empfehlenswert ...

-- der festgelegte Unabhängigkeitsgrad wird als nicht ausreichend betrachtet ...

o für den festgelegten Unabhängigkeitsgrad liegt keine Empfehlung für oder gegen seine Verwendung vor.

Kapitel 8.2.13 der IEC 61508-1 gibt dazu folgende Erläuterungen:

„In den Tabellen kann entweder ++1 oder ++2 zutreffen (nicht beides), dies hängt von einer Anzahl von anwendungsspezifischen Faktoren ab. Trifft ++1 zu, ist ++2 nicht als Anforderung zu verstehen, wenn ++2 zutrifft, ist ++1 als -- (nicht empfehlenswert) zu verstehen. Liegt keine anwendungsspezifische Norm vor, müssen die Gründe für die Auswahl von ++1 oder ++2 ausführlich dargelegt werden.

Faktoren, die dazu führen, dass ++2 eher angemessen ist als ++1 sind:

- fehlende Erfahrung mit einem ähnlichen Entwurf;
- höherer Grad der Komplexität;
- höherer Neuigkeitsgrad des Entwurfs;
- höherer Neuigkeitssgrad der Technologie;
- fehlende Normung von Konstruktionsmerkmalen.

Diese Anforderungen an die Unabhängigkeit für die Beurteilung der funktionalen Sicherheit gelten selbstverständlich auch für Bussysteme.
Die IEC 61508 schreibt nur für SIL 4 die Einschaltung einer unabhängigen Organisation für die Beurteilung der Funktionalen Sicherheit vor. Damit ist es jedem Unternehmen selbst überlassen, bei Bussystemen bis SIL3 selbst festzustellen, inwieweit die o. g. Faktoren zutreffen.
Die IEC 61511-1 legt keine weiteren Anforderungen an den Grad der Unabhängigkeit bei der Beurteilung der Funktionalen Sicherheit fest. Sie legt lediglich fest, dass zum Beurteilungsteam mindestens eine erfahrene, kompetente Person gehören muss, die nicht mit dem Entwurf des Projektes befasst war. Da sich aber die IEC 61511-1 mit dem gesamten Sicherheitssystem und die IEC 61508 sich mit den dort zu implementierenden Komponenten befasst, müssen für ein Bussystem die Anforderungen an die Unabhängigkeit gemäß IEC 61508 eingehalten werden. Der Nachweis hierfür ist durch den Hersteller der Komponente zu erbringen.

Neben den normativen Vorgaben gibt es jedoch gute Gründe, ein Bussystem von einer oder mehreren unabhängigen Organisation(en) beurteilen und zertifizieren zu lassen. Solche Gründe sind:

- marktpolitisch unabhängige Beurteilung
- Anerkennung der Ergebnisse durch andere Institutionen
- Anerkennung der Ergebnisse über nationale Grenzen hinaus
- Wettbewerbsvorteile durch Führen eines Prüfzeichens auf dem Produkt
- zunehmende Forderung der Anwender nach einer Zertifizierung durch eine unabhängigen Stelle

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. Unabhängig von den einzelnen Lebenszyklusphasen gilt:

Die Dokumentation muss:

- genau und knapp sein,
- von denjenigen Personen, die sie verwenden müssen, einfach zu verstehen sein,
- den Zweck erfüllen, für den sie erstellt worden ist,
- verfügbar und pflegbar sein.

Für die Lebenszyklusphase Installation/Errichtung, Betrieb, Wartung werden dem Anwender in der Regel drei Dokumente zur Verfügung gestellt:

Einbauanleitung („Beipackzettel“)

Diese Dokumentation wird dem Produkt, z. B. der Buskomponente, in der Verpackung in mehreren Sprachen mitgeliefert und informiert den Anwender über die wichtigsten Produktmerkmale:

- Produktbezeichnung mit Bestellnummer
- Kurzbeschreibung der Funktion
- Allgemeine Anschlusshinweise mit Beispielen
- Technische Daten
- Sicherheitshinweise

Betriebsanleitung, Sicherheitshandbuch

Die Betriebsanleitung und Sicherheitshandbuch können separat oder in einem Dokument zusammengefasst sein. Sie stellen dem Anwender sehr viel detailliertere Information zur Verfügung als die Einbauanleitung. Als Referenzquelle haben sie alle notwendigen Informationen zu liefern, die für die Inbetriebnahme, den laufenden Betrieb, die Fehlerdiagnose und die Fehlerbehebung erforderlich sind.

Betriebsanleitung und Sicherheitshandbuch müssen enthalten:

- Allgemeine Angaben
  - Geltungsbereich
  - Standards
  - Sicherheitstechnische Auflagen
  - Beschreibung der Sicherheitsfunktion
  - Verwendete Abkürzungen und Symbole

- Produktbeschreibung
  - Prinzipielle Arbeitsweise der Komponente
  - Reaktion im Fehlerfall
  - Einsatzbereiche
  - Funktion und Bedeutung von Bedien- und Anzeigeelementen
  - Beschreibung der Schnittstellen
  - Sicherheitszeiten
- Montage und Installation
  - Sicherheitstechnische Randbedingung/ Einschränkungen
  - Befestigungshinweise
  - Anschlussbelegungen
- Applikations- und Konfigurationsbeispiele
  - Busspezifische Einstellungen (Adressen, Busabschlüsse..)
  - Hinweise zur Berechnung der Reaktionszeiten
- Inbetriebnahme
  - Personelle Qualifikationen
  - Einschaltsequenz
  - Hinweise zur Prüfung der Sicherheitsfunktionen (Checkliste)
  - Parametrierung und Konfigurierung
  - Zugangsberechtigung
- Diagnose und Fehlerbehebung
  - Ablage der Diagnosedaten
  - Ablage der Prozessdaten
  - Fehlerliste und deren Behebung
- Technische Daten
  - Elektrische/mechanische/klimatische Umgebungsbedingungen
  - EMV Bedingungen
  - Sicherheitstechnische Kenngrößen (PFD/PFH) und deren Randbedingungen (Proof-Test Intervall)

Bussystemhandbuch

Das Handbuch des Bussystems bezieht sich nicht auf spezielle Buskomponenten. Es beschreibt hingegen allgemeine Randbedingungen die einzuhalten sind, damit ein Bussystem zuverlässig, interkompatibel und spezifikationsgemäß arbeitet.

Das Bussystemhandbuch umfasst:

- Leitungsspezifische Kenngrößen
  - Leitungsbeläge
  - Wellenwiderstand
  - Abhängigkeit Leitungslänge vs. Baudrate
  - Biegeradien
- Busterminierung
- Max. zulässige Buslängen
  - Segment
  - Stichleitung
- Stromversorgungskonzept
- Galvanische Trennung
- Schirmung / Erdung der Busleitung
  - Anbindung
- Verlegungshinweise
- Standardisierte Steckverbindungstechnik und deren Belegung

6.4 Sicherheitskette

Die in den Tabellen 2 und 3 der IEC 61508-1 genannten gefährlichen Versagenswahrscheinlichkeiten bei Anforderungen (PFD) bzw. Wahrscheinlichkeiten eines gefahrbringenden Versagens pro Stunde (PFH) beziehen sich immer auf die komplette Sicherheitsfunktion.

Der Grenzwert für einen bestimmten SIL-Level bezieht sich auf das Zusammenspiel aller Komponenten, die in einer Sicherheitsfunktion verwandt werden. Es schließt die gesamte Kette vom Sensor bis zum Aktor ein.
Aus diesem Grund darf ein einzelnes Gerät oder eine einzelne Komponente, die innerhalb der Sicherheitsfunktion verwand wird, nicht den gesamten zulässigen Grenzwerte von PFD bzw. PFH in Anspruch nehmen.
Die übliche Aufteilung ist wie folgt:

»**35%** »**15%** »**50%**

Diese Anteile sind nicht in der Norm festgeschrieben. In der Praxis hat sich diese Aufteilung aber als sinnvoll erwiesen. Die Aufteilung kann variieren, wird sich aber nicht wesentlich verändern. Bekanntermaßen sind die meisten Ausfälle in den Peripheriebereichen zu beobachten, d.h. im Bereich des Sensors und in der Verdrahtung zwischen Sensor und Verarbeitungseinheit. Der Sensor ist üblicherweise raueren Umgebungsbedingungen ausgesetzt als die Verarbeitungseinheit. Das gleiche gilt auch für den Aktor, also z. B. Ventil, Schütz, Motor, etc.. Die Logik ist meist geschützt in einem Schaltschrank untergebracht und damit weniger harten Umgebungsbedingen ausgesetzt.

Ein Bussystem verbindet Sensoren und Aktoren mit der Logik und ist damit ebenso Teil der Sicherheitskette. Der Anteil von PFD bzw. PFH, welcher ein Bussystem beanspruchen darf, ist ebenso in keiner Norm festgeschrieben. Auch hier gibt es einen Praxiswert, wonach ein Bussystem nicht mehr als ca. 1 % der jeweils zulässigen Grenzwerte für SIL 3 in Anspruch nehmen sollte. In diesem Falle kann der Anteil des Bussystems vernachlässigt werden.

Diese Vernachlässigung ist nur dann zulässig, wenn die für das Bussystem angegebenen Randbedingungen in der Praxis auch eingehalten werden. Hierbei geht wesentlich die Bitfehlerwahrscheinlichkeit, welche die Wahrscheinlichkeit angibt, dass bei der Übertragung einer Nachricht ein Bit verfälscht wird, in die Bestimmung der Versagenswahrscheinlichkeit ein. Die Bitfehlerwahrscheinlichkeit ist abhängig vom Übertragungsmedium.

Bitfehler-wahrscheinlichkeit p	Übertragungsmedium
$> 10^{-3}$	Funkstrecke
10^{-4}	Ungeschirmte Datenleitung
10^{-5}	Geschirmte „twisted Pair“ Telefonleitung
10^{-6} - 10^{-7}	Digitale Telefonleitung der TELEKOM
10^{-9}	Koaxialkabel in lokal begrenzten Anwendungen
10^{-12}	Glasfaserkabel

Eine Änderung des vorgeschriebenen Übertragungsmediums, z. B. von geschirmter auf ungeschirmte Leitung, hat einen gravierenden, negativen Einfluss auf die Versagenswahrscheinlichkeit und ist daher unzulässig.
Welche Leitung verwendet werden darf, muss im Bussystemhandbuch oder Sicherheitshandbuch beschrieben sein.

6.5 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.

Erfahrungsgemäß ist die Phase Modifikation besonders sicherheitskritisch.
Es müssen seitens des Anlagenbetreibers Pläne erstellt werden, wie bei Modifikationen vorzugehen ist. Diese Pläne bedürfen einer sicherheitstechnischen Beurteilung, um festzustellen, ob bei Ausführung dieser geplanten Maßnahmen die erforderliche Funktionale Sicherheit in jedem Moment noch gegeben ist. Bestandteil dieser Pläne sollten Checklisten der Komponentenhersteller sein, aus denen hervorgeht, wie eine erfolgreiche Verifikation der spezifizierten Sicherheitsfunktionen durchgeführt werden kann.
Für die Verifikation des Bussystems ist die Verwendung von busspezifischen Diagnosewerkzeugen hilfreich.

6.6 Sicherheitstechnische Kenngrößen

Die Nennung von sicherheitstechnische Kenngrößen in Produkt- oder Systemhandbüchern dient zum einen dazu alle notwendigen Informationen dem Anwender zur Verfügung zu stellen, die er benötigt, um eine Sicherheitskette zu beurteilen. Darüber hinaus haben diese Kenngrößen eine produktbeschreibende Funktion.

- Die Hardware Fault Tolerance, HFT ist ein Merkmal der sicherheitstechnischen Architektur eines (Teil)-Systems (ein- bzw. mehrkanalig).

- Die Safe Failure Fraction, SFF stellt den quantitative Anteil der sicheren und erkannten gefährlichen Ausfälle dar.

- Die Probability of Failure on Demand, PFD bzw. die Probability of a dangerous failure per hour, PFH geben die quantitativen Werte der Versagenswahrscheinlichkeit der Schutzfunktion eines (Teil-) Systems wieder und ermöglichen eine Beurteilung der Einhaltung der entsprechenden Grenzwerte für die gesamte Sicherheitskette

- Das Proof-Test Intervall gibt die Zeit an, nach der eine Prüfung zur Aufdeckung von unerkannten Fehlern zu erfolgen hat, damit der geforderte Sicherheitsintegritätslevel eingehalten wird.

Damit eine gesamtsicherheitstechnische Betrachtung einer Sicherheitskette erfolgen kann, sind alle genannten Angaben zwingend erforderlich.
Diese Angaben sind insbesondere für die Personen erforderlich, welche eine Beurteilung vornehmen, in wieweit die für die Sicherheitskette gewählten Komponenten entsprechend des angestrebten SIL geeignet sind. Neben den oben genannten sicherheitstechnischen Kenngrößen sind auch die im Sicherheitshandbuch beschriebenen Restriktion zu beachten.

6.6.1 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 HFT und 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.

Beispiel: zweikanaliges System (HFT = 1) bestehend aus einfachen Bauteilen (keine hochintegrierte IC's) deren Ausfallverhalten ausreichend definiert ist (Typ A-Teilsysteme), angestrebter SIL 3.

Tabelle 2 der IEC 61508-2:

Anteil der ungefährlichen Ausfälle (SFF)	**Fehlertoleranz der Hardware (HFT)**		
	0	**1**	**2**
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %		SIL 3	SIL4
90 % - < 99 %	SIL 3	SIL4	SIL4
> 99 %	SIL 3	SIL4	SIL4

Die SFF gibt das Verhältnis der sicheren und erkannten, also diagnostizierten gefährlichen, Ausfälle zu allen Ausfällen wieder.

Die Gleichung verdeutlicht den Zusammenhang.

$$SFF = \frac{l_{SAFE} + l_{Dangerous} \cdot DC}{l_{SUM}}$$

λ_{SAFE}	Rate sicherer Ausfälle
$\lambda_{DANGEROUS}$	Rate gefährlicher Ausfälle
λ_{SUM}	Summe aller Ausfallraten
DC	Diagnostic Coverage (Diagnoseaufdeckungsgrad)

Voraussetzung für die Bestimmung der SFF ist die Ermittlung und Aufteilung der Ausfallraten in sichere, gefährlich erkannte und gefährlich unerkannte Anteile. Diese Aufteilung erfolgt zweckmäßigerweise mit Hilfe einer FMEA und zwar für jedes Teilsystem. Diese FMEA kann auf Funktionsblockebene wie auch auf Komponentenebene erfolgen.

2. Bewertungsverfahren

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

Im Teil 6 der IEC 61508 stellt die Norm für verschiedene Architekturen Formeln sowohl für PFD als auch PFH dar, die auf Zuverlässigkeitsblockdiagrammen basieren. Bei Anwendung dieser Formeln ist jedoch zu berücksichtigen, dass diese nur unter den oder genannten Randbedingungen gelten. Treffen diese Randbedingungen nicht zu, so muss die Gleichung für die Ausfallwahrscheinlichkeit individuell bestimmt werden.

Beispiel: Einfache Berechnung der mittleren Probability of Failure on Demand, PFD_{AV} bei einem einkanaligen System.

$$PFD_{AV} = l_{DU} \cdot \frac{T}{2}$$

Darin ist:

λ_{DU}	Ausfallrate gefährlicher unerkannter Fehler
T	Einsatzzeit (Proof-Test Intervall)
PFD_{AV}	mittlere Ausfallwahrscheinlichkeit

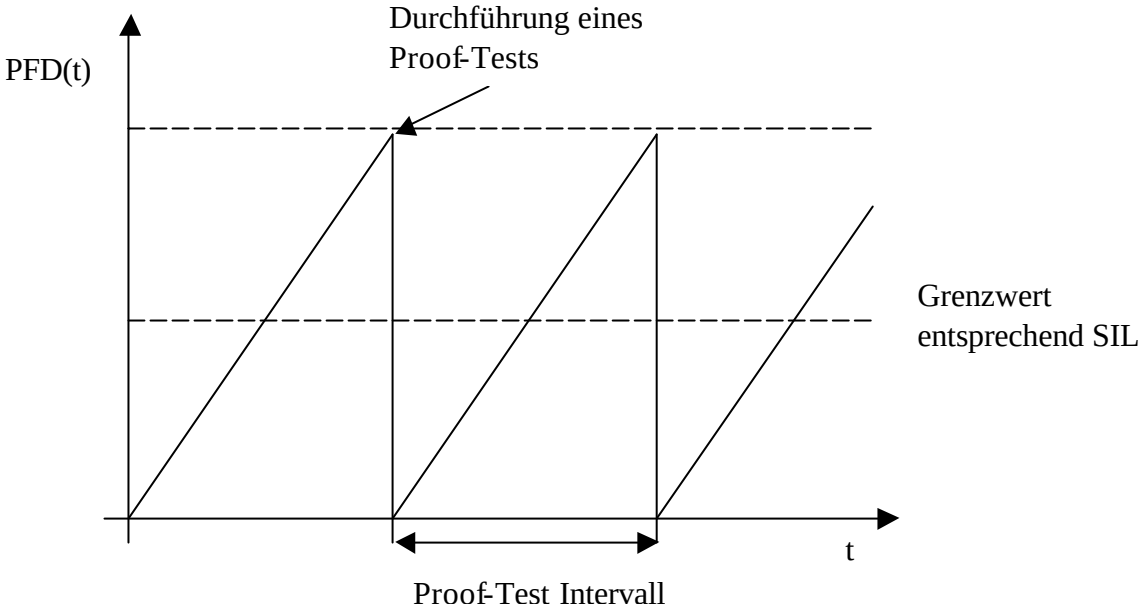
Diese Gleichung gilt unter den folgenden Bedingungen:

- Die Sicherheitsfunktion wird innerhalb der Fehlertoleranzzeit des Prozesses ausgelöst.
- Jeder durch Diagnose erkannte gefährliche Fehler führt innerhalb der Fehlertoleranzzeit des Prozesses zu Auslösung der Sicherheits-funktion.
- Das System ist ein elektronisches Shutdown-System (ESD)
- War der Proof-Test nicht erfolgreich, so muss das System in den sicheren Zustand überführt werden.

Die Bedeutung des Proof-Test Intervalls soll nachfolgend erläutert werden.

Die Wahrscheinlichkeit eines gefährlichen Ausfalls ist nach dem Einschalten eines geprüften Systems sehr klein. Mit fortlaufender Betriebszeit steigt die Wahrscheinlichkeit für kleine Werte von $\lambda_{DU} \cdot t$ angenähert mit $PFD(t) = \lambda_{DU} \cdot t$.

Nach Durchführung des Proof-Tests kann unter den o. g. Bedingungen von einer Wahrscheinlichkeit nahe Null ausgegangen werden. Damit ergibt sich der unten dargestellte zeitliche Verlauf.



Bei vorliegendem λ_{DU} kann im allgemeinen die Einhaltung eines einem SIL zugeordnetem Grenzwertes durch Wahl des Proof-Test Intervalls erreicht werden.

Der Proof-Test muss in der Lage sein, alle durch die Diagnose nicht erkennbaren gefährlichen Fehler aufzudecken. Bei mehrkanaligen Systemen ist der Proof-Test für jeden Kanal einzeln anzuwenden. Bei nicht vollständigem Proof-Test ergibt sich ein ansteigen der mittleren Versagenswahrscheinlichkeit mit der Zeit.
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.

Es lässt sich für jede Komponente in einem System ein Proof-Test Intervall angeben. Sinnvoll ist es, dass die Intervalle aller Komponenten innerhalb der Sicherheitsfunktion in den Revisionszyklus einer Anlage passen. Das Revisionsintervall muss dann kleiner sein als das kleinste Proof-Test Intervall einer Komponente. Damit werden Standzeiten und damit einhergehende Unverfügbarkeiten der Anlage vermieden.

6.6.2 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.

6.6.2.1 Nachweis nach IEC 61508

Die IEC 61508 lässt im Teil 2 die Verwendung von betriebsbewährten („Proven In Use, PIU“) Komponenten in neueren Teilsystemen zu.
Dabei gilt: *“Ein früher entwickeltes Teilsystem darf nur als betriebsbewährt betrachtet werden, wenn es eine klar beschränkte Funktionalität hat und wenn ein angemessener dokumentarischer Nachweis vorliegt, der auf vorheriger Verwendung in einer speziellen Konfiguration des Teilsystems beruht ... und der jede zusätzliche Analyse ... wie erforderlich berücksichtigt. Der dokumentarische Nachweis muss zeigen, dass die Wahrscheinlichkeit irgendeines Ausfalls des Teilsystems.... niedrig genug ist, so dass der erforderliche Sicherheits-Integritätslevel der Sicherheitsfunktion ... erreicht wird.“*

Für den Nachweis über den Ansatz „Proven In Use“ sind umfangreiche Daten erforderlich, die vom Betreiber zur Verfügung gestellt werden müssen. Der Betreiber muss bezüglich der verwendeten Komponenten über ein statistischen Erfassungssystem verfügen.
Eine einfache Komponente kann als ausreichend bewährt angesehen werden, wenn unter anderem folgende Kriterien erfüllt werden:

- Unveränderte Spezifikation
- Einsatz in unterschiedlichen (sicheren und nicht sicheren) Anwendungen
- Betriebsaufzeichnungen über mindestens ein Jahr
- Ausreichend Betriebserfahrung bezogen auf ein bekanntes Anforderungsprofil
- Hinreichend geringe sicherheitsbezogene Ausfälle

Dieser Ansatz ist geeignet, um einen Nachweis zu erbringen, dass die Wahrscheinlichkeit von systematischen Fehlern niedrig genug ist und mit der Kenntnis der sicherheitsbezogenen Ausfälle, dass die gefährliche Versagenswahrscheinlichkeit einen bestimmten SIL erfüllt.

Darüber hinaus sind weitergehende Maßnahmen zur Fehlervermeidung durchzuführen. Für die Identifizierung der zu betrachtenden Komponente müssen weiterhin folgende Informationen zur Verfügung gestellt werden:

- Identifikation des betriebsbewährten Teilsystems (Proven In Use, PIU)
- Beschreibung (Architektur, Funktionsbeschreibung) des PIU Teilsystems
- Informationen über die bisherige Verwendung
- Informationen über die beabsichtigte Verwendung
- Änderungshistorie
- Beschreibung der qualitätssichernden Maßnahmen während der bisherigen und jetzigen Verwendung

6.6.2.2 Nachweis nach NAMUR

Dem Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Einrichtungen in bestehenden Anlagen widmet sich die NAMUR-Empfehlung NE 93. Hier wird dem Anwender ein Formblatt zur einheitlichen numerischen Erfassung von Störungen an die Hand gegeben. Aus der Statistik lassen sich folgende Daten entnehmen:

- Erkennung einer Störung bei Prüfung oder im Betrieb
- Sind nur Diagnoseeinrichtungen betroffen?
- Art des Fehlers: Aktiv oder Passiv?
- Wie ist der Redundanzgrad?
- Blockierung der gesamten Schutzeinrichtung?

Ein Vergleich mit den quantitativen Anforderungen der SILs nach IEC 61508 und den „daraus abgeleiteten Nachweis der Erfüllung der Anforderungen“ schließt sich an. Maßnahmen zur Fehlervermeidung sind nicht Bestandteil dieser Betrachtung.

Die NAMUR-Empfehlung besitzt nicht den Status einer Norm. Daher sind bezüglich des Nachweises einer Betriebsbewährung die Standards IEC 61508 und IEC 61511 heranzuziehen. Die NE 93 dient der fakultativen Benutzung und kann daher nur ergänzend zu den oben genannten Standards verwendet werden.

7 Kriterien für die Verwendung eines Bussystems

Die nachfolgenden Kriterien beziehen sich auf die in der Checkliste des Kapitel 8 genannten Bewertungspunkte. Diese Kriterien sollen dem Anwender der Checkliste weitere Informationen an die Hand geben, um beim Betreiber einer Anlage die Bewertungspunkte gezielt hinterfragen zu können und damit eine Bewertung zu erleichtern.

1. Bewertung der Dokumentation

   Um eine Bewertung der funktionalen Sicherheit für die Lebenszyklusphasen Installation, Validation, Betrieb, Modifikation und Nachrüstung durchführen zu können werden umfangreiche Detailinformationen der Anlage und deren Komponenten benötigt. Darüber hinaus sind Informationen für die erfolgreiche Ausführung der Lebenszyklusphase erforderlich. Das Vorhandensein aller Dokumente, beginnend bei der Anlagenbeschreibung über die Betriebs-, Sicherheits- und Montageanleitungen der einzelnen Komponenten bis hin zu Plänen, um die Sicherheitsfunktionen zu validieren, stellt die Basis für eine umfassende Beurteilung eines Bussystems und deren Komponenten dar.
   Darüber hinaus stellen diese Dokumente ein umfassendes Nachschlagewerk für alle Beteiligten dar, welche an einem Bussystem oder deren Komponenten Arbeiten durchzuführen haben. (Siehe hierzu auch Kapitel 6.3).

2. Bewertung zusätzlicher Anforderungen

   Neben den anwendungsunabhängigen Standards, den sogenannten Basisstandards (z. B. IEC 61508, müssen auch die anwendungsabhängigen Standards, die sich speziell auf eine Anwendung beziehen, berücksichtigt werden.

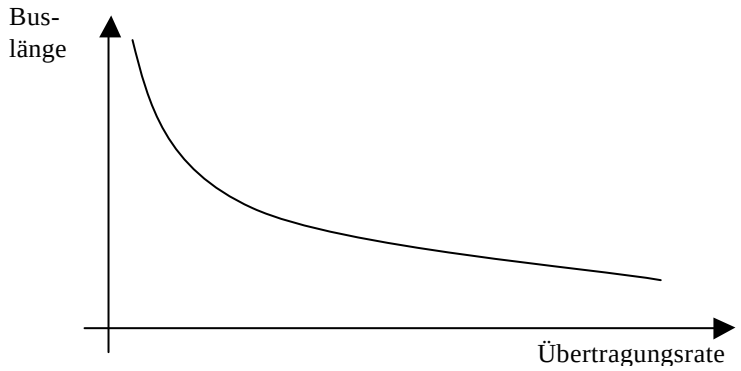
Als Beispiel hierfür seien hier die Standards für Feuerungsanlagen genannt. Anwendungsstandards können Anforderungen definieren, welche die Anforderungen aus den anwendungsunabhängigen Standards ergänzen oder darüber hinausgehende Anforderungen stellen.
Alle Arten von Standards sind in einer Anwendung zu identifizieren und zwingend zu berücksichtigen.

3. Bewertung der Teilnehmeranzahl

In einem Busstrang eines sicherheitsgerichteten Bussystems gehen nicht nur die sicherheitsrelevanten Teilnehmer, sondern auch die nicht sicherheitsrelevanten Teilnehmer in die Gesamtteilnehmeranzahl mit ein. Jeder Busteilnehmer wird über eine im Bussystem einzigartige Adresse, welche vorher ihm zugewiesen wurde, angesprochen. Die Anzahl aller am Bus beteiligten Teilnehmer darf die maximal zulässige, dem Bussystem spezifische, Grenze nicht überschreiten. Die Teilnehmerzahl hat unmittelbaren Einfluss auf die Reaktionszeiten der einzelnen Sicherheitsfunktionen.

4. Bewertung der Übertragungsrate

Die Übertragungsrate gibt an, wie viele Bits pro Zeiteinheit in einem Bussystem übertragen werden. Die max. Übertragungsrate ist abhängig von der elektrischen Spezifikation des Bussystem, vom Übertragungsmedium und von der Länge eines Busstrangs. Je länger ein Busstrang ist, desto niedriger wird die Übertragungsrate. Dieser Zusammenhang verdeutlicht folgendes Bild:



Sinkt die Übertragungsgrate, so erhöht sich gleichzeitig die Buszykluszeit, also die Zeit welche benötigt wird um einen kompletten Datenaustausch auf dem Bus durchzuführen.

5. Bewertung der Reaktionszeiten

Aus den zur Verfügung gestellten Dokumenten müssen die erforderlichen Reaktionszeiten für jede zu realisierende Sicherheitsfunktion herausgearbeitet werden.

Die Reaktionszeit ist abhängig von der Anzahl der Busteilnehmer, Übertragungsrate, Datenmenge und der Verarbeitungszeit eines jeden Busteilnehmers. Das Bussystemhandbuch gibt dem Anwender entsprechende Gleichungen an die Hand, um die busspezifischen Zeiten zu bestimmen.

Es muss verifiziert werden, ob die Summe der Einzelreaktionszeiten der an der Sicherheitsfunktion beteiligten Komponenten, die für die Sicherheitsfunktion zur Verfügung stehenden Gesamtreaktionszeit nicht überschreitet. Hierfür ist es erforderlich für alle beteiligten Komponenten, wie E/A-Komponenten, Logikkomponenten und Buskomponenten, die Reaktionszeiten herauszuarbeiten und rechnerisch zu belegen, zu dokumentieren sowie durch Tests zu überprüfen, dass die Anforderungen an die Reaktionszeiten für jede Sicherheitsfunktion erfüllt werden.

6. Bewertung der Maßnahmen zur Erhöhung der Verfügbarkeit

Da in der Prozesstechnik die Betriebsphasen „Anfahren“ und „Herunterfahren“ einer Anlage immer mit erhöhtem Risiko verbunden sind, sollte möglichst vermieden werden, dass die Anlage unverhältnismäßig oft in diese Betriebsphasen gebracht wird. Die Anlage sollte ohne Minderung der Sicherheit möglichst hoch Verfügbarkeit sein. Um dieses Ziel zu erreichen muss verifiziert werden, ob bei der Konzipierung der Anlage die Gesichtspunkte der Verfügbarkeit ausreichend berücksichtigt worden sind. Für die Erreichung einer hohen Verfügbarkeit ist es wichtig, dass die eingesetzten Komponenten eine genügend hohe Störfestigkeit gegen die in der Anlage auftretenden Störungen ausweisen. Die Eignung der Komponenten für die vorgesehene Umgebungsbedingung ist nachzuweisen. Die durchgeführten Maßnahmen zur Erhöhung Verfügbarkeit sind seitens des Betreibers zu dokumentieren.

7. Bewertung der Einsatzbedingungen

Bei der Bewertung der Einsatzbedingungen muss anhand der zur Verfügung stehenden Datenblätter geprüft werden, ob die verwendeten Komponenten für die spezifizierten Umgebungsbedingungen der Anlage geeignet sind. Die Verifikation dieser Einsatzbedingungen muss Bestandteil des Verifikationsplans sein und die Ergebnisse der Verifikation sind zu dokumentieren. Dieser Bewertungspunkt ist auch maßgeblich für die Beurteilung der Maßnahmen zur Erhöhung der Verfügbarkeit.

8. Bewertung für die Anwendung im Ex-Bereich

Werden Komponenten im Ex-Bereich eingesetzt muss neben dem Eignungsnachweis durch ein entsprechendes Zertifikat überprüft werden, ob alle Auflagen die im Sicherheitshandbuch des Herstellers definiert sind bei der Planung berücksichtigt worden sind.

9. Bewertung nach IEC 61508

Die Spezifikation eines sicherheitsgerichteten Busprotokolls unterliegt ebenso wie dessen Umsetzung in Komponenten der Beurteilung durch eine unabhängige Organisation. Ein ausgestelltes Zertifikat bescheinigt die Konformität mit den entsprechenden Anforderungen. (Siehe hierzu auch Kapitel 6.2.1)
Darüber hinaus ist zu beachten, das der jeweils niedrigste Sicherheits-integritätslevel der Kette Bussystem-Komponenten das Gesamtsystem bestimmt. Es ist zu prüfen, inwieweit dieser mit dem anzustrebenden SIL übereinstimmt.

10. Bewertung der gefährlichen Versagenswahrscheinlichkeit bzw. der Versagensrate pro Stunde

Für jede definierte Sicherheitsfunktion muss zunächst deren Anforderungsrate ermittelt werden. Beträgt diese ungefähr einmal pro Jahr , so ist von einer niedrigen Anforderungsrate auszugehen und die gesamte gefährliche Versagenswahrscheinlichkeit bei Anforderung (PFD) zu bestimmen.
Beträgt diese mehr als einmal pro Jahr , so ist von einer hohen Anforderungsrate auszugehen und die gefährliche Versagensrate pro Stunde (PFH) für die Sicherheitsfunktion zu bestimmen.

Für die Bewertung einer Sicherheitsfunktion müssen von allen daran beteiligten Komponenten die einzelnen Werte vorliegen. Diese Größen sind den Sicherheitshandbüchern der jeweiligen Hersteller zu entnehmen. Entsprechend der Architektur der Sicherheitsfunktion gehen die einzelnen Größen der Komponenten in die Gesamtberechnung ein.

Randbedingungen für die Bewertung

Ausgangsdatenbasis für die Bestimmung der gefährlichen Versagenswahrscheinlichkeiten bzw. der Versagensrate sind die Ausfallraten der Bauteile aus denen die Buskomponenten aufgebaut sind. Die Bestimmung der Ausfallraten sind an einsatzspezifische Umgebungsbedingungen gekoppelt. Umgebungsbedingungen sind beispielsweise Betriebsspannung und Strom, Belastung oder Umgebungstemperatur. Besonders die Umgebungstemperatur hat einen signifikanten Einfluss. Im Allgemeinen wird eine mittlere Umgebungstemperatur von 40°C angenommen. Bei höheren Temperaturen steigt die Ausfallrate zum Teil exponentiell an. Liegt also die zu erwartende mittlere Umgebungstemperatur über 40°C, so ist dem in der Bestimmung der Ausfallraten entsprechend Rechnung zu tragen. Dies hat aber wiederum gravierenden Einfluss auf die Versagenswahrscheinlichkeit bzw. auf die Versagensrate einer Komponente und letztendlich auch auf die gesamte Sicherheitskette. (Siehe hierzu auch Kapitel 6.6.1).

Neben den Umgebungsbedingungen ist bei der Bewertung der Versagenswahrscheinlichkeit bzw. der Versagensrate auch die mittlere Reparaturzeit (siehe IEC 61508-6) der einzelnen Komponenten zu berücksichtigen. Durch organisatorische Maßnahmen muss sichergestellt sein, dass diese Zeiten nicht überschritten werden.

11. Bewertung des Proof-Test Intervall

Wie bereits in Kapitel 6.6.1 erläutert, ist das Proof-Test Intervall eine sicherheitstechnische Kenngröße, die für alle an der Sicherheitsfunktion beteiligten Komponenten vorliegen muss. Sie legt die Zeit fest nach der ein Gerät spätestens überprüft werden muss, damit die geforderte gefährliche Versagenswahrscheinlichkeit nicht überschritten wird und das Gerät wieder in den „Wie-neu-Zustand“ überführt wird.
Hierzu ist es zweckmäßig, dass diese Intervalle in eine Anlagenrevision fallen. Intervalle, welche kleiner sind als eine Anlagenrevision, beeinträchtigen den Produktionsprozess und sind zu vermeiden. (Siehe hierzu auch Kapitel 6.6.1).
Die Proof-Test Intervalle der Komponenten sind den Sicherheitshandbüchern der jeweiligen Hersteller zu entnehmen.

12. Bewertung der Proof-Test Planung

Sind alle Proof-Test Intervalle der Komponenten bekannt, so muss ein Plan existieren, der festhält wann, wie und welche Komponenten einer Wiederholungsprüfung (Proof-Test) zu unterziehen sind. Gegebenfalls sind hier auch die dazu notwendigen Hilfsmittel zu benennen.
Welche Testprozeduren während einem Proof-Test durchzuführen sind, sind den Sicherheitshandbüchern der jeweiligen Hersteller zu entnehmen.

13. Bewertung des Validationsplans des Bussystems und der Komponenten bei Erstinbetriebnahme

Durch die Bewertung des Validationsplanes soll sichergestellt werden, dass alle für das Bussystem notwendigen Informationen, Parameter und/oder organisatorischen Maßnahmen bei der Projektierung des Bussystems berücksichtigt worden sind.

Die gezielte Durchführung aller Verifikationsschritte des Validationsplanes soll einen sicheren und zuverlässigen Betrieb aller an einem Bus beteiligten Komponenten sicherstellen.

14. Bewertung von Konfiguration- und Parametrierwerkzeugen

Konfigurations- und Parametrierwerkzeuge stellen die Schnittstelle zwischen Betreiber/Anwender und Bussystem dar. Über diese Werkzeuge verschafft sich der Betreiber Zugang zu allen bus- und z. T. prozessinternen Aktivitäten.

Bei der Bewertung dieser Werkzeuge ist darauf zuachten,

- dass nur Werkzeuge zum Einsatz kommen, die für das betreffende Bussystem vom Hersteller freigegeben worden sind.
- dass die Zugangskontrolle/-rechte zu den verschiedenen Funktionsebenen dieser Werkzeuge entsprechend realisiert ist. (Siehe hierzu auch Kapitel 5.2).
- ob diese nur während der Wartungsphase oder auch während des Normalbetriebs eingesetzt werden dürfen.

15. Bewertung der Personalqualifikation

Voraussetzung für die Wirksamkeit aller vorangegangenen Maßnahmen und Aktivitäten ist, dass das damit beauftragte Personal oder die beauftragten Firmen grundsätzlich seitens ihrer Ausbildung bzw. Qualifikation dazu geeignet sind. Entsprechende Nachweise sind zu erbringen.

8 Checkliste

		Bewertung		Bemerkungen
lfd. Nr.	**Bewertungspunkte**	**erfüllt**	**nicht erfüllt**	
1	**Bewertung der Dokumentation:** - Anlagenbeschreibung / RI - Plan - Zertifikat - Betriebsanleitung - Sicherheitshandbuch - Montageanleitung - Validationsplan der Sicherheitsfunktionen - Plan für Wartung und Modifikation der Sicherheitsfunktionen Liegen diese Dokumente in ihrer passenden Version für alle Komponenten vor?			
2	**Bewertung zusätzlicher Anforderungen:** - Anwendungsstandards vorhanden? Werden die zusätzlichen Anforderungen der Anwendungsstandards erfüllt?			
3	**Bewertung der Teilnehmeranzahl:** - Gesamtanzahl aller Teilnehmer (sicher/nicht sicher) je Busstrang? Kann das gewählte Bussystem die Teilnehmerzahl bedienen?			
4	**Bewertung der Übertragungsrate**: - Busausdehnung? Entspricht die gewählte Übertragungsrate der Busausdehnung?			
5	**Bewertung der Reaktionszeiten:** - Reaktionszeit für jede Sicherheitsfunktionen? - Reaktionszeiten der an Sicherheitsfunktionen beteiligten E/A-Komponenten? - Programmzykluszeit der Logik (SSPS)? - Übertragungszeiten des Bussystems in jedem Busstrang? Wird die Reaktionszeit für jede definierte Sicherheitsfunktion eingehalten?			

		Bewertung		Bemerkungen
lfd. Nr.	**Bewertungspunkte**	**erfüllt**	**nicht erfüllt**	
6	**Bewertung der Maßnahmen zur Erhöhung der Verfügbarkeit:** - Bustopologie? - Redundante Auslegung der Übertragungswege? - Störfestigkeit (EMV)? - Redundanz der I/O Komponenten? - Komponentenaustausch im Online-Betrieb (Hot plug/Hot repair)? - Erlaubt die Prozesssicherungszeit die mehrfache Übertragung von Telegrammen (Mehrfachauswertung)? Wird die vorgesehene Verfügbarkeit ohne Minderung der Sicherheit durch die getroffenen Maßnahmen erreicht?			
7	**Bewertung der Einsatzbedingungen:** - klimatische Umgebung? - mechanische Belastung? - EMV Umgebung? - Stoffresistenz? - Ex-Umgebung? Sind die einzelnen Komponenten geeignet für die zu erwartenden Umweltbedingungen?			
8	**Bewertung für die Anwendung im Ex-Bereich:** - Werden Komponenten des Bussystems in Ex-Bereichen eingesetzt? - Gibt es besondere Auflagen für den Einsatz im Ex-Bereich seitens des Herstellers? Ist das Bussystem für den Einsatz im Ex-Bereich geeignet?			
9	**Bewertung nach IEC 61508:** - Busprotokoll Ist das verwendete Protokoll des Bussystems von einer unabhängigen Stelle als sicher nach IEC 61508 zertifiziert? - Buskomponenten Sind die verwendeten Busteilnehmer von einer unabhängigen Stelle als sicher nach IEC 61508 zertifiziert? - SIL Welchen SIL haben die Buskomponenten und das Protokoll? Erreichen die SIL des Protokolls und der Teilnehmer den geforderten SIL der Anwendung?			

		Bewertung		Bemerkungen
lfd. Nr.	**Bewertungspunkte**	**erfüllt**	**nicht erfüllt**	
10	**Bewertung der gefährlichen Versagenswahrscheinlichkeit bzw. der Versagensrate pro Stunde:** - PFH Wertes des Bussprotokolls? - PFD/PFH Werte aller sicheren Komponenten? - Für welchen Temperaturbereich sind die Ausfallraten, die der PFD/PFH Berechnung zugrunde gelegt worden sind gültig? - Randbedingungen für die Berechnungen Wird für jede SF die sicherheitstechnische Kenngröße PFD/ PFH eingehalten?			
11	**Bewertung des Proof Test Intervall:** - Proof-Test Intervalle für jede Komponente? Ist das Proof-Test Intervall jeder am Bussystem beteiligten Komponente größer als das geplante Wartungsintervall der Anlage?			
12	**Bewertung der Proof Testplanung:** Existiert ein Plan für die Durchführung der Prof Tests? Ist die Durchführung des Proof-Tests für alle Komponenten beschrieben? Sind die erforderlichen Hilfsmittel verfügbar?			
13	**Bewertung des Validationsplans des Bussystems und der Komponenten bei Erstinbetriebnahme, wie zum Beispiel:** - Busauslastung - Übertragungszeiten - Erdungskonzept - Verkabelung - Busabschlüsse - Steckverbindungstechnik - Sicherheitsfunktion - Konfiguration des Bussystems - Verwendung zugelassener Werkzeuge - Parametrierung der Buskomponenten - Überprüfung der parametrierten Zeiten (Time outs) - Beschreibung des Verfahren bei Ausfällen, Änderungen oder Nachrüstungen - Richtige Umsetzung aller Anforderungen aus den Benutzerunterlagen bzw. des Sicherheitshandbuches Kann mit diesem Validationsplan der Nachweis erbracht werden, dass das betrachtete Bussystem und dessen Buskomponenten nach der Montage in jeder Hinsicht die Spezifikation der Sicherheitsanforderungen erfüllt?			

		Bewertung		Bemerkungen
lfd. Nr.	**Bewertungspunkte**	**erfüllt**	**nicht erfüllt**	
14	**Bewertung von Konfiguration- und Parametrierwerkzeugen:** - Geprüfte Werkzeuge? - Zugangskontrollen? - Organisation von Zugriffsrechten?			
15	**Bewertung der Personalqualifikation:** - Installation - Inbetriebnahme - Betrieb - Wartung und Service (Proof- Test) Sind die Qualifikationen des eingesetzten Personals oder der beauftragten Firmen ausreichend ?			

9 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. Bei der Konfiguration und Parametrierung müssen die vom Hersteller freigegebenen und sicherheitstechnisch beurteilten Werkzeuge eingesetzt werden.

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.

Die Tabelle in Kapitel 8 soll eine allgemeine Hilfestellung bei der Bewertung liefern. Diese Tabelle erhebt nicht den Anspruch einer einfachen ja/nein Analyse, sondern dient vielmehr dazu, die komplexe Kommunikationstechnik transparenter zumachen und einen sicherheitstechnischen Gesamteindruck zu bekommen, oder gezielten Fragen an den Betreiber und ggf. an den Hersteller zu formulieren. Anhand der o. g. Schnittstelleninformationen und in Verbindung mit der Tabelle ist eine Bewertung zu einem in der Anlagensicherheit der Chemie Industrie angewandten Bus-System möglich.

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