Ursachen für das Versagen von Automatisierungssystemen

Timm Grams, Fachhochschule Fulda

Thema ist das Lernen aus den Fehlern im Gefolge von Unfällen und gefährlichen Zwischenfällen. Es werden drei Ebenen der Ursachenanalyse unterschieden: 1. Analyse der unmittelbaren Ursachen und Primärursachen, 2. Aufzeigen von Fehlern und 3. Analyse der Grundursachen. Auf der ersten Analyseebene werden die Primärursachen den Lebenszyklusphasen der technischen Einrichtung zugeordnet: Spezifikation, Realisierung, Installation und Inbetriebnahme, Betrieb und Wartung, Modifikation und Nachrüstung. Deutlich herausgestellt wird die Rolle der Spezifikationsfehler: Sie lassen sich nur im Nachhinein feststellen und sie werden nur sichtbar im Rahmen eines evolutionären Fehlerbeseitigungsprozesses. Und sie gehören zu den häufigsten Fehlern. Ihrer Vermeidung ist vordringliche Aufgabe. Wesentliches Instrument ist die Gefährdungs- und Risikoanalyse.

Gliederung

Einführung

Die folgende Darstellung ist eine Ergänzung zum Kapitel „1 Grundbegriffe“ der Lehrveranstaltung „Qualitäts- und Risikomanagement - Zuverlässigkeit und Sicherheit“ [1].

Unter einem *Automatisierungssystem* wird hier ein Regelungs- oder Steuerungssystem verstanden (Control System). Ein solches Automatisierungssystem antwortet auf Signale vom Prozess oder von einem Operateur und erzeugt Ausgangssignale, die dafür sorgen, dass die *Betriebseinrichtung* (Equipment Under Control, EUC) wie gewünscht reagiert, Bild 1.

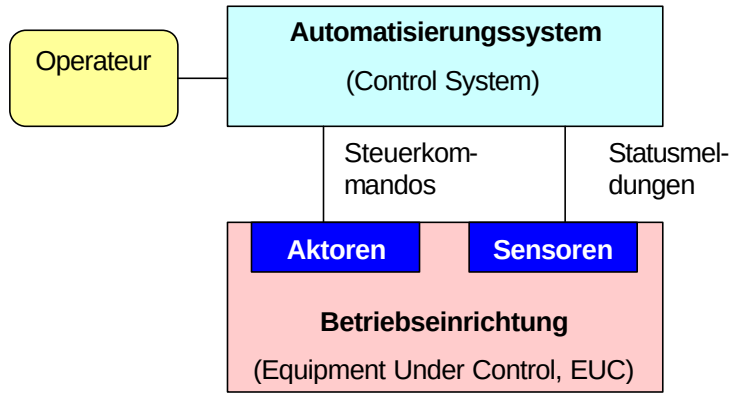

Bild 1: Das Gesamtsystem

Eine Betriebseinrichtung kann beispielsweise eine Turbine in einem Kraftwerk, ein Heizkessel, ein Mikrowellenofen, ein Transportsystem, der Reaktor einer Chemieanlage oder ein Brückenkran sein.

Bei den Automatisierungssystemen wird unterschieden zwischen elektrischen/elektronischen/programmierbar elektronischen Systemen (E/E/PES) und Systemen anderer Technologien wie beispielsweise Hydraulik und Pneumatik.

Den Rahmen für die folgenden Überlegungen bildet die Norm IEC 61508, deren Hauptaugenmerk den sicherheitsbezogenen E/E/PES gilt. Das sind Systeme, die in eine der *sicherheitsbezogenen Anforderungsstufen* (Safety Integrity Levels, SIL) fallen und für die demzufolge eine Sicherheitsspezifikation erstellt werden muss [2]. (Anforderungsstufen werden in deutschen Richtlinien auch *Anforderungsklassen* genannt [1, Kapitel „6 Sicherheitstechnik“].)

Zu den wesentlichen sicherheitsgerichteten Festlegungen des so genannten *Sicherheitsplans* einer Anlage gehören „Verfahren, die sicherstellen, dass gefährliche Zwischenfälle ... analysiert werden und Empfehlungen dahingehend gemacht werden, dass die Wahrscheinlichkeit einer Wiederholung minimiert ist“ [2, Teil 2, Abschnitt 6.2.2, Absatz k]. Hier wird also das *Lernen aus den Fehlern* institutionalisiert.

Wesentlicher Bestandteil einer Analyse von *unerwünschten Ereignissen* (Unfälle, gefährliche Zwischenfälle usw.) ist die *Ursachenanalyse*, die es in verschiedenen Ausprägungen gibt [3]. Ich unterscheide insbesondere die folgenden der Ebenen der Ursachenanalyse, Bild 2:

1. *Analyse der unmittelbaren Ursachen (Analysis of Immediate Causes).*
   Diese Analyse beruht auf der „Logik der Ursachen“: Eine Ursache ist Element einer Menge von Ursachen, von denen jede notwendig und die alle zusammen hinreichend für das Eintreten des unerwünschten Ereignisses sind. Auf dieser Ebene der Ursachenanalyse geht es um das Technical Blow by Blow, um die Ereigniskette, die zum Unfall führte. Die Analyse der unmittelbaren Ursachen hat auch die Aufgabe, die in der Ereigniskette am Anfang liegende wesentliche Ursache aufzuspüren. Eine solche wird hier *Primärursache* genannt.
2. *Aufdecken von Fehlern (Detection of Errors).*
   Unmittelbare Ursachen können Hinweise auf Fehler liefern. Aber nicht jede Ursache für einen Unfall ist auch ein Fehler. Umgekehrt kann ein Fehler durchaus unauffällige Konsequenzen haben und gilt demzufolge auch nicht als Ursache. Über die reine Logik der Ursachen hinaus ist ein normatives Modell vonnöten, das es ermöglicht, richtiges Verhalten von Fehlverhalten zu unterscheiden. Ein normatives Modell für das menschliche Verhalten ist der Entscheidungsbaum [1, Abschnitt 12.4].
3. *Analyse der Grundursachen* (Root Cause Analysis).
   Hier werden die Fehler auf allgemeine Mechanismen zurückgeführt, die in den technischen, psychologischen und soziologischen Wissenschaften untersucht und beschrieben werden. Dies ist ein Prozess der *Verallgemeinerung*, der uns hilft, maximal aus den Fehlern zu lernen. So wird nicht bloß verhindert, dass sich ein solches Unglück wiederholt, sondern darüber hinaus lassen sich ganze Ursachenkategorien entschärfen [4, Kapitel 3 und 4].

Es folgt die Zusammenstellung der Ergebnisse einer HSE-Studie [5], in der eine Reihe von unerwünschten Vorfällen auf ihre Primärursachen hin untersucht worden sind. Diese Primärursachen werden den Lebenszyklusphasen des gesamten Systems zugeordnet.

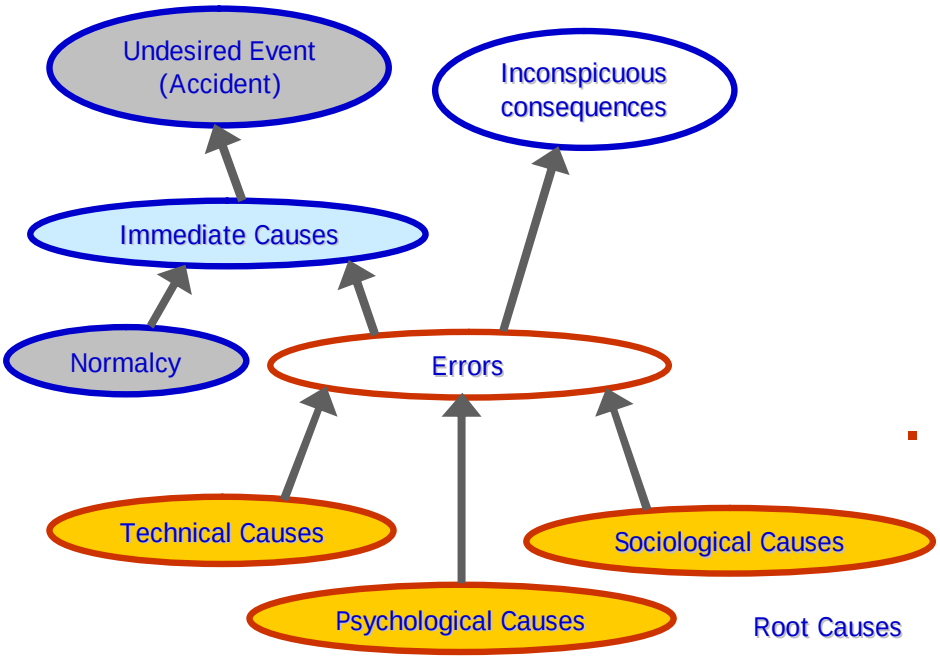

Bild 2: Ursachen und Fehler

Klassifizierung der Primärursachen nach Lebenszyklusphasen

Die Klassifizierung der Primärursachen geschieht im Hinblick auf fünf Phasen des in Bild 3 dargestellten Lebenszyklus-Modells [2, Teil 1, Abschnitt 7] für das gesamte System (Bild 1). Sie sind durch fette Schrift hervorgehoben. Es sind dies die folgenden Phasen.

1. *Spezifikation*
   Hier werden die gesamten Sicherheitsanforderungen für alle Sicherheitssysteme und externen Einrichtungen zur Risikoreduzierung festgelegt. (Zu den externen Einrichtungen zur Risikoreduzierung gehören unter anderem Drainagesysteme, Feuerschutzwälle und Rettungswege.) Bestandteile der Spezifikation sind
   - die funktionalen Sicherheitsanforderungen und
   - die sicherheitsbezogenen Zuverlässigkeitsanforderungen (ausgedrückt in SIL).
   In einem weiteren Schritt erfolgt eine Zuweisung der Sicherheitsanforderungen an die einzelnen Sicherheitssysteme und externen Einrichtungen derart, dass die gesamten Sicherheitsanforderungen erfüllt werden.
2. *Realisierung*
   Die Realisierungsphase hat das Ziel, E/E/PES Sicherheitssysteme, Sicherheitssysteme anderer Technologie und der externen Einrichtungen zur Risikoreduzierung, so zu entwickeln, dass sie die jeweiligen Spezifikationen erfüllen.
3. *Installation und Inbetriebnahme*
4. *Betrieb und Wartung*
5. *Modifikation und Nachrüstung.*

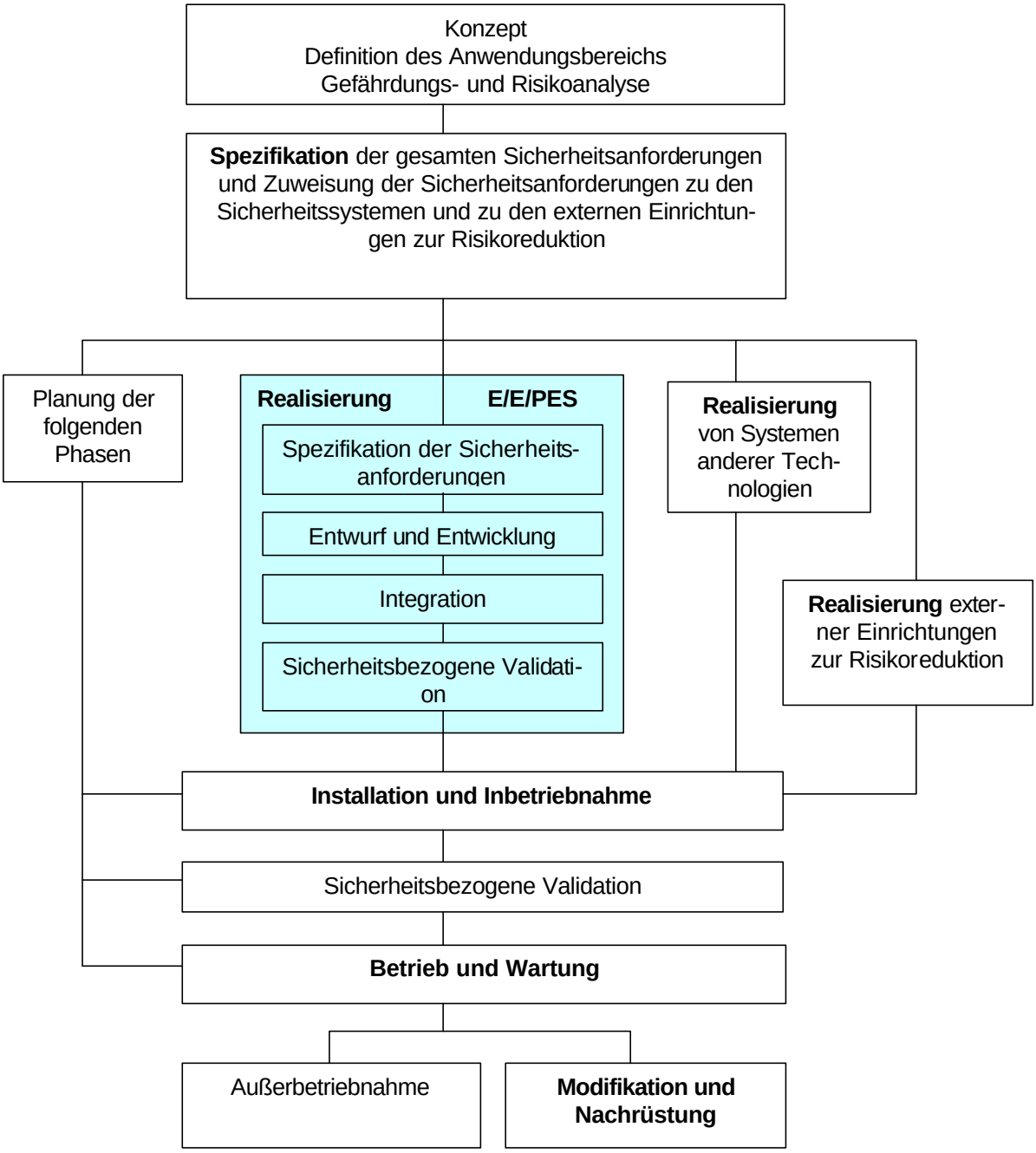

Bild 3: Sicherheitsbezogener Gesamtlebenszyklus
Farbiger Kasten: Elektrisches/elektronisches/programmierbar elektronisches System (E/E/PES)

Ursachen und Fehler

Solange es nur darum geht, unmittelbare Ursachen aufzuzeigen und zu klassifizieren, spielt es keine Rolle, ob die Ereignisse im Rahmen einer Gefährdungs- und Risikoanalyse bereits berücksichtigt werden konnten oder nicht, und ob es sich im engeren Sinne um Fehler handelt oder nicht: Ursachen werden im Hinblick auf ein unerwünschtes Ereignis, im Nachhinein und auf der Grundlage rein formaler Prinzipien untersucht.

Aber die Kenntnis von Ursachen allein hilft uns nicht viel weiter. Erst wenn wir in einer Ursache auch einen Fehler erkennen, haben wir die Möglichkeit daraus zu lernen.

Für die Feststellung, ob es sich bei einer Ursache um einen Fehler handelt, brauchen wir ein normatives Modell. Und gerade für die Lebenszyklusphase Spezifikation steht ein solches nicht von vornherein zur Verfügung Es fehlt, weil jede Spezifikation selbst normativen Charakter hat [1, Abschnitt 1.5].

Und dennoch: Die Analyse der unmittelbaren Ursachen kann zu einer Korrektur der Anforderungen an das System führen und eine Überarbeitung der Spezifikation nach sich ziehen. Die neue Spezifikation ist eine Widerlegung der alten. In diesem Sinne kann dann *im Nachhinein* von einem *Spezifikationsfehler* gesprochen werden. Die Spezifikation unterliegt also einem Evolutionsprozess. Und Evolutionsprozesse sind nichts anderes als Fehlerbeseitigungsprozesse, ob in Biologie, Wissenschaft, Gesellschaft oder auch in der Technik.

Für die anderen Lebenszyklusphasen existieren normative Modelle. Dazu gehören unter anderem die Spezifikation, die technischen Richtlinien und Normen und Entscheidungsbäume.

Ergebnisse der HSE-Studie - Fallbeispiele

In der HSE-Studie [5] wurden 34 Vorfälle untersucht. Für jeden Vorfall wurde eine Primärursache identifiziert. Jede dieser Primärursachen wurde einer Lebenszyklusphase zugeordnet. Das Ergebnis der Studie ist in Bild 4 zusammengefasst. Auffällig ist

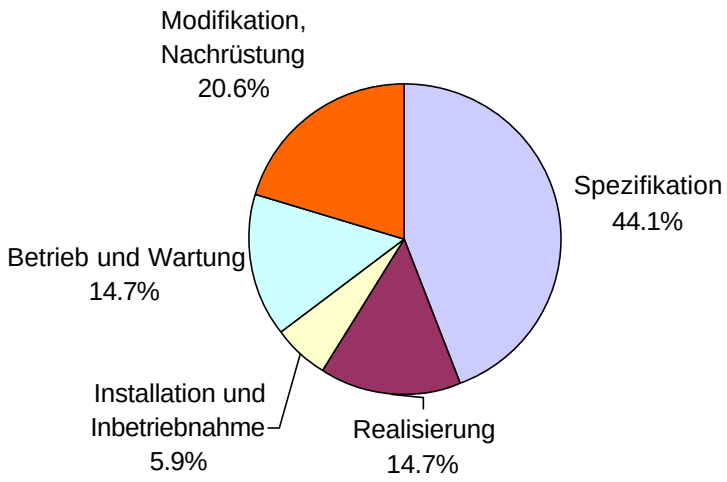

Bild 4: Primärursachen nach Phasen

der große Anteil an Spezifikationsfehlern. Das sind Fehler, die im Rahmen einer Zuverlässigkeitsvorhersage gar nicht in Rechnung gestellt werden können, da sich die Zuverlässigkeitsvorhersage ausschließlich auf die Einhaltung der (möglicherweise bereits fehlerhaften) Spezifikation bezieht. Die Statistik in Bild 4 zeigt, wie wichtig eine ausgiebige und sorgfältige *Gefährdungs- und Risikoanalyse* in der Phase vor der Spezifikation ist. Sie bietet die letzte Möglichkeit, Spezifikationsfehler zu vermeiden (Bild 3).

Für jede der fünf Phasen wird im Folgenden ein Fallbeispiel kurz beschrieben.

Spezifikation [5, S. 14], [6, Abschnitt 12.3]: Der steuernde Computer eines Chargen-Reaktor-Systems war spezifikationsgemäß so programmiert, dass er im Fehlerfall alle Stellgrößen einfror. Kurz nachdem frischer Katalysator in den Reaktor eingefüllt wurde, was normalerweise eine Erhöhung der Kühlwasserzufuhr nach sich ziehen müsste, erhielt der Computer die Nachricht eines zu niedrigen Ölstands in einem Getriebe. Daraufhin hielt er alle Steuergrößen und damit auch den Kühlwasserzufluss konstant. Der Reaktor wurde überhitzt, ein Überlastventil öffnete sich, und es kam zur Freilassung von Reaktorinhalt in die Atmosphäre. Die in der Spezifikation aufgestellte Forderung nach unbedingtem Einfrieren der Stellgrößen im Fehlerfall stellte sich im Nachhinein als falsch heraus. Das hätte bereits durch eine umfassende Gefährdungs- und Risikoanalyse erkannt werden können. Eine solche wurde für den Computer aber nicht durchgeführt. Primärursache ist also ein Spezifikationsfehler; die Grundursache aber liegt in der Organisation: Der *Sicherheitsplan* hätte vorsehen müssen, den Computer in die Gefährdungs- und Risikoanalyse einzubeziehen [2, Teil 1, Abschnitt 6.2.2].

Realisierung [5, S. 20]: Eine Papierschneidemaschine senkte das Schneidemesser zum falschen Zeitpunkt. Grund war ein Relais, das mit zu geringem Strom betrieben wurde. Dadurch wurde das Oxid auf der Oberfläche nicht vollständig abgebrannt und das wiederum führte zu einem zu hohem elektrischen Widerstand bei geschlossenem Relais, so dass es von der Auswertungselektronik fälschlich als offen angesehen wurde. Offenbar wurde hier gegen Grundsätze der Ingenieursarbeit verstoßen, die verlangen, dass die Einsatzbedingungen einer Komponente genau spezifiziert werden und dass geprüft wird, ob die Komponente diesen Bedingungen auch genügt. Außerdem hätte das Relais - wie jede andere sicherheitsrelevante Komponente auch - bezüglich der Ausfallmodi und deren Auswirkungen untersucht werden müssen (Ausfalleffektanalyse).

Installation und Inbetriebnahme [5, S. 23]: In einer computergesteuerten Chemieanlage wurde ein Gasventil unabsichtlich geöffnet. Daraufhin kam es zur Emission schädlicher Gase in die Atmosphäre. Ursache war ein falsch angeschlossenes Adressbit des Ausgabegeräts. Die Adressen der Elektronikkarten am Datenbus waren deshalb nicht eindeutig und das Gerät reagierte auf ein Kommando, das für eine andere Karte gedacht war. Als tiefer liegende Ursachen wurden hier falsche Entwurfsentscheidungen und eine ungeeignete abschließende Geräteprüfung ausgemacht.

Betrieb und Wartung [5, S. 25]: Bei Wartungsarbeiten einer Papierschneidemaschine schloss der Servicetechniker die Zylinderspulen zur Steuerung des Messers falsch an - die Anschlussdrähte trugen keine Farbmarkierung. Der folgende Funktionstest schlug fehl. Noch bevor der Servicetechniker die Anschlussverbindungen tauschen konnte, trat der Operateur an die Maschine heran. Die Unterbrechung der Lichtschranke bewirkte nun nicht eine Blockierung des Messers, sondern setzte es in Bewegung. Dadurch wurde der Operateur schwer verletzt. Tiefere Gründe für diesen Unfall sind das offenbar schlechte Design (fehlende Markierung) aber auch eine mangelhafte Planung und Durchführung der Wartungsarbeit.

Modifikation und Nachrüstung [5, S. 29]: Eine schwimmende Bohrplattform wurde umgebaut und nachgerüstet. Die Modifikation betraf auch das Steuerungssystem der Ballasttanks, das auf Hydraulik umgestellt wurde. Anschließend arbeitete die Bohranlage in verschiedenen Bohraufträgen. Nach einer Stilllegungsphase wurde sie erneut in Betrieb genommen. In der Folge eines Stromausfalls bekam die Bohranlage Schlagseite und stand kurz vor der Evakuierung. Ursachen: Beim Umbau wurde ein Filter des hydraulischen Ballastsystem nicht richtig eingepasst. Dadurch sammelte sich Unrat in

den Absperrventilen. Aufgrund des Stromausfalls öffneten sich die Ventile spezifikationsgemäß. Dabei beschädigte der Unrat die Dichtungen dieser Ventile. Wieder unter Strom schlossen die Ventile nicht richtig und das führte zur Fehlfunktion der Steuerungsventile der Ballasttanks. Auch in diesem Fall liegen die Grundursachen wieder in der schlechten Planung und Organisation und dem Auslassen von Arbeitsschritten nach Durchführung der Modifikation: Mangelhafte Prozedur zum Spülen des Hydrauliksystems, fehlender Nachweis der Erfüllung der Sicherheitsspezifikation.

Literatur + Links

[1] Grams, T.: Grundlagen des Qualitäts- und Risikomanagements. Zuverlässigkeit, Sicherheit, Bedienbarkeit. Vieweg Praxiswissen, Braunschweig, Wiesbaden 2001

[2] IEC 61508: Functional Safety (deutsch: VDE 0801: Funktionale Sicherheit).
Part 1: General requirements (1998)
Part 2: Requirements for E/E/PE safety-related systems (2000)
Part 3: Software requirements (1998)
Part 4: Definitions and abbreviations (1998)
Part 5: Examples of methods for the determination of safety integrity levels (1998)
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2000)
Part 7: Overview of techniques and measures (2000)

[3] Grams, T.: The right decision can cause an accident. Beitrag zum 2. Bieleschweig Workshop on Root Cause Analysis. 1./2. July 2003

[4] Leveson, N. G.: Safeware. System Safety and Computers. Addison-Wesley, Reading, Massachusetts 1995

[5] Health and Safety Executive (GB): Out of Control. Why control systems go wrong and how to prevent failure. HSE Books 1995

[6] Kletz, T.: An Engineer's View of Human Error. 3rd edition. Institute of Chemical Engineers 2001

Zurück zur Seite „Zuverlässigkeit und Sicherheit - Q&R-Management“
