



Gesellschaft für Reaktorsicherheit

---

# Deutsche Risikostudie Kernkraft- werke

Fachband 3

Zuverlässigkeitskenngrößen und  
Betriebserfahrungen

---

Verlag TÜV Rheinland

## **Deutsche Risikostudie/Fachband 3**

### **Nachtrag**

Als Autoren sind nachzutragen:

Hans-Peter Balfanz

Hartmut Jansen

Hermann Ohlmeier

die dem TÜV-Norddeutschland e. V. angehören, sowie

Claus Verstegen

der Mitarbeiter der Gesellschaft für Reaktorsicherheit  
(GRS) mbH ist.



**Gesellschaft für Reaktorsicherheit**

# **Deutsche Risikostudie Kernkraftwerke**

Eine Untersuchung zu dem durch  
Störfälle in Kernkraftwerken  
verursachten Risiko

**Fachband 3**

**Zuverlässigkeitskenngrößen und  
Betriebserfahrungen**

Studie im Auftrage des Bundesministeriums  
für Forschung und Technologie

**Verlag TÜV Rheinland**

Die Autoren dieses Fachbandes 3 "Zuverlässigkeitsdaten und Betriebserfahrungen" der Deutschen Risikostudie - Kernkraftwerke sind:

Volker Albertz  
Wolfgang Güldner  
Paul Hömke  
Helmut Hörtnert  
Erwin Lindauer  
Joachim von Linden  
Wolfgang Preischl  
Günther Reichart  
Wolfgang Röhrs

Alle Autoren sind Mitarbeiter der Gesellschaft für Reaktorsicherheit (GRS) mbH.

*Redaktion:*

*H.-P. Butz, L.F. Franzen, K. Kotthoff, M. Straßenmeyer*

ISBN 3-88585-014-1

Herausgeber: Der Bundesminister für Forschung und Technologie

Copyright: Der Bundesminister für Forschung und Technologie, Bonn 1980

Verlegerische Betreuung und Gesamtherstellung: Verlag TÜV Rheinland GmbH, Köln

Printed in Germany 1980

## Vorwort

Im Frühjahr 1976 hatte der Bundesminister für Forschung und Technologie (BMFT) die "Deutsche Risikostudie - Kernkraftwerke" bei der Gesellschaft für Reaktorsicherheit (GRS) mbH in Auftrag gegeben. Unter der wissenschaftlichen Leitung ihres Geschäftsführers, Prof. Dr. A. Birkhofer, wurden die zugehörigen Arbeiten zusammen mit weiteren technisch-wissenschaftlichen Organisationen durchgeführt und die Ergebnisse im August 1979 vorgelegt. Ziel dieser Studie war es, das durch Störfälle in Kernkraftwerken verursachte Risiko unter Berücksichtigung deutscher Verhältnisse in Anlehnung an die amerikanische Reaktorsicherheitsstudie WASH-1400 zu ermitteln.

Die Studie gliedert sich in zwei Arbeitsphasen. Die erste Phase ist abgeschlossen. Die Ergebnisse sind in einer allgemein verständlichen Kurzfassung, herausgegeben vom BMFT, vom 15. August 1979 und in einem Hauptband, erschienen im Verlag TÜV Rheinland, ebenfalls 1979, dokumentiert. Ergänzend zu diesen Veröffentlichungen werden die für die Studie im einzelnen durchgeführten Untersuchungen und ihre Ergebnisse in einer Reihe von Fachbänden zusammengestellt, die im Laufe des Jahres 1980 erscheinen: F1 - Ereignisablaufanalyse, F2 - Zuverlässigkeitsanalyse, F3 - Zuverlässigkeitsdaten und Betriebserfahrungen, F4 - Einwirkungen von außen (einschließlich anlageninterner Brände), F5 - Untersuchung von Kernschmelzunfällen, F6 - Ermittlung der Spaltproduktfreisetzung, F7 - Ergebnisse der anlagentechnischen Untersuchungen, F8 - Unfallfolgenrechnungen und Risikoergebnisse.

Der hier vorliegende Fachband 3 dokumentiert Zuverlässigkeitsdaten und Betriebserfahrungen, die in die Ereignisablauf- und Fehlerbaumanalysen (Fachbände 1 und 2) eingegangen sind. Mit diesen zusammen werden die Aussagen des Hauptbandes, Kapitel 4 und 5, erweitert und belegt. Das zusammengestellte Material bildet eine der Grundlagen, auf denen die Ergebnisse der anlagentechnischen Untersuchungen (Fachband 7) ruhen. Es werden die Eintrittshäufigkeiten von auslösenden Ereignissen (Kühlmittelverluststörfälle und Transienten), die Ausfallraten und -wahr-

scheinlichkeiten von Komponenten sowie die Wahrscheinlichkeiten menschlichen Fehlverhaltens behandelt.

Köln, im Juli 1980

Gesellschaft für Reaktorsicherheit  
(GRS) mbH

## Kurzfassung

Der vorliegende Fachband stellt die Arbeiten dar, die in Phase A der deutschen Risikostudie zu den folgenden Fragen durchgeführt wurden:

- Eintrittshäufigkeiten auslösender Ereignisse,
- Beurteilung des Reaktordruckbehälters,
- Ausfallraten und -wahrscheinlichkeiten für Komponenten,
- Wahrscheinlichkeiten für menschliches Fehlverhalten.

Der Fachband beschreibt das generelle Vorgehen, das bei der Ermittlung dieser Größen angewandt wurde. Darüber hinaus gibt er die im einzelnen verwendeten Werte und die zu ihrer Ermittlung benutzten Quellen wieder.

## Abstract

This appendix discusses those studies which were carried out in phase A of the German Risk Study on the following problems:

- occurrence frequencies of initiating events
- evaluation of the reactor pressure vessel
- failure rates and failure probabilities for components
- probabilities for human error.

The appendix describes the general procedure used in determining these parameters. In addition, it gives the individual values used and the sources employed to determine these values.

INHALT

	Seite
1. Zusammenfassung . . . . .	1
2. Einleitung . . . . .	6
2.1 Gegenstand des Fachbandes . . . . .	6
2.2 Probleme der Datenermittlung . . . . .	7
2.3 Folgerungen für die Risikostudie . . . . .	10
2.4 Aufbau des Fachbandes . . . . .	12
3. Auslösende Ereignisse . . . . .	13
3.1 Kühlmittelverluststörfälle . . . . .	13
3.1.1 Lecks in einer Hauptkühlmittelleitung . . . . .	13
3.1.2 Kleines Leck am Druckhalter . . . . .	22
3.2 Transienten . . . . .	24
3.2.1 Notstromfall . . . . .	24
3.2.2 Ausfall der Hauptspeisewasserversorgung . . . . .	25
3.2.3 ATWS-Störfälle . . . . .	25
4. Reaktordruckbehälterversagen . . . . .	26
4.1 Statistische Betrachtungen . . . . .	26
4.2 Qualitätssicherung beim Reaktordruck- behälter . . . . .	29
4.3 Folgerungen für die Risikostudie . . . . .	33
5. Zuverlässigkeitskenngrößen . . . . .	36
5.1 Allgemeines . . . . .	36
5.2 Literaturdaten und Betriebserfahrungen . . . . .	40
5.3 Ermittlung der Zuverlässigkeitskenngrößen . . . . .	43
6. Auswertung von Betriebserfahrungen in deutschen Kernkraftwerken . . . . .	52
6.1 Aufgabenstellung . . . . .	52
6.2 Vorgehen . . . . .	53
6.2.1 Wiederkehrende Prüfungen . . . . .	54
6.2.2 Wartungs- und Instandsetzungsarbeiten . . . . .	59
6.2.3 Einzelauswertungen . . . . .	61



6.3	Ergebnisse . . . . .	62
6.3.1	Ausfallraten und Ausfallwahrscheinlichkeiten . . . . .	62
6.3.2	Ausfallwahrscheinlichkeiten von Teilsträngen . . . . .	63
6.3.3	Instandsetzungszeiten von Komponenten . . . . .	64
6.3.4	Nichtverfügbarkeiten von Teilsträngen infolge Instandhaltungsmaßnahmen . . . . .	66
7.	Zuverlässigkeitskenngrößen für verfahrens- und elektrotechnische Komponenten . . . . .	69
7.1	Übersicht . . . . .	69
7.2	Pumpen . . . . .	69
7.2.1	Startversagen . . . . .	69
7.2.2	Betriebsversagen . . . . .	72
7.3	Motorarmatur . . . . .	73
7.4	Magnetventil . . . . .	75
7.5	Pneumatisches Ventil . . . . .	76
7.6	Rückschlagarmatur . . . . .	76
7.6.1	"Öffnet nicht" . . . . .	76
7.6.2	"Schließt nicht" . . . . .	77
7.6.3	Innere Leckage . . . . .	77
7.6.4	Rückschlagarmatur mit Motorantrieb . . . . .	78
7.7	Handarmatur . . . . .	79
7.8	Regelarmatur . . . . .	79
7.9	Sicherheits- und Entlastungsventile. . . . .	80
7.10	Rohrleitungen . . . . .	84
7.11	Notstromdiesel . . . . .	85
7.11.1	Startversagen . . . . .	85
7.11.2	Betriebsversagen . . . . .	86
7.11.3	"Common mode"-Ausfälle . . . . .	87
7.12	Steuerstäbe . . . . .	89
7.13	Sonstige Komponenten . . . . .	91
8.	Zuverlässigkeitskenngrößen für leittechnische Komponenten . . . . .	94
8.1	Ausfallratenermittlung durch Literaturauswertung . . . . .	94
8.1.1	Allgemeines . . . . .	94
8.1.2	Verwendete Auswertemethoden . . . . .	95

8.1.3	Ausgewertete Literatur . . . . .	96
8.2	Betriebserfahrung . . . . .	99
8.3	Ausfallratenermittlung durch Ausfalleffekt- analysen . . . . .	104
8.3.1	Allgemeines . . . . .	105
8.3.2	Experimentelle Ausfalleffektanalyse . . .	107
8.3.3	Theoretische Ausfalleffektanalyse . . . .	107
8.3.4	Ausfalleffektanalyse mit Netzwerkanalyse- programmen . . . . .	108
8.3.5	Anwendung auf leittechnische Komponenten und Geräte . . . . .	108
8.3.6	Ersatzausfallraten für leittechnische Systeme . . . . .	113
8.4	Basisdaten zu "common mode"-Ausfällen in der Leittechnik . . . . .	113
9.	Basisdaten zur Bewertung menschlicher Fehlhand- lungen . . . . .	117
10.	Schrifttum . . . . .	120
11.	Stichwortverzeichnis . . . . .	131
Anhang 1:	Zusammenstellung von Zuverlässigkeitskenn- größen	
Anhang 2:	Zuverlässigkeitskenngrößen aus der Auswer- tung von Betriebserfahrungen aus Kern- kraftwerken	
Anhang 3:	Basis-Ausfallraten für leittechnische Kom- ponenten	

BILDER

	Seite
F3, 5-1: Zeitverhalten der Ausfallrate . . . . .	39
F3, 8-1: Schaltplan Simatic-P-Baustein V21 (UND-Stufe) . . . . .	110
F3, 8-2: Fehlerbaum Simatic-P-Baustein V21 (UND-Stufe) . . . . .	112

TABELLEN

F3, 6-1: Vergleich beobachteter und berechneter Ausfallwahrscheinlichkeiten für Teil- stränge . . . . .	65
F3, 6-2: Instandsetzungszeiten von Komponenten . .	66
F3, 6-3: Nichtverfügbarkeiten von Teilsträngen in- folge Instandhaltungsmaßnahmen . . . . .	67
F3, 7-1: Ausfallraten und Ausfallwahrscheinlich- keiten für verfahrens- und elektrotech- nische Komponenten . . . . .	70
F3, 8-1: Beispiel für die Auswertung der Schadens- statistik des Kraftwerks Irsching . . . . .	102
F3, 8-2: Ausfallratenvergleich . . . . .	103
F3, 8-3: Beispiel für die Aufteilung der Gesamtaus- fallrate . . . . .	111

## 1. ZUSAMMENFASSUNG

Der vorliegende Fachband stellt die Arbeiten dar, die in Phase A der deutschen Risikostudie zu den folgenden Fragen durchgeführt wurden:

- Eintrittshäufigkeiten auslösender Ereignisse,
- Beurteilung des Reaktordruckbehälters,
- Ausfallraten und -wahrscheinlichkeiten für Komponenten,
- Wahrscheinlichkeiten für menschliches Fehlverhalten.

Es werden sowohl das allgemeine Vorgehen zur Ermittlung der Daten als auch die im einzelnen verwendeten Werte dokumentiert. Die in diesem Fachband behandelten Daten stellen die quantitative Basis für die in den Fachbänden 1 und 2 dargestellten Ereignisablauf- und Fehlerbaumanalysen dar. Sie sind damit eine der Grundlagen für die Ergebnisse der anlagentechnischen Untersuchungen der deutschen Risikostudie, die im Hauptband, Kapitel 5, und im Fachband 7 wiedergegeben sind.

Eintrittshäufigkeiten werden für diejenigen auslösenden Ereignisse ermittelt, für die in der Studie detaillierte Ereignisablaufanalysen durchgeführt werden (Fachband 1). Bei den auslösenden Ereignissen wird zwischen Kühlmittelverluststörfällen, das sind Lecks verschiedener Größe in einer Hauptkühlmittelleitung, und Transienten unterschieden.

Für die Ermittlung der Eintrittshäufigkeiten von Lecks in Hauptkühlmittelleitungen wird die verfügbare Literatur über Schäden an Rohrleitungen herangezogen. Für kleine Lecks (effektive Ausströmfläche 2 bis  $80 \text{ cm}^2$ ) stützen sich die verwendeten Zahlen jedoch hauptsächlich auf die bereits vorliegende Betriebserfahrung mit kommerziellen Leichtwasserreaktoren. Für die Eintrittshäufigkeit großer Lecks ( $> 400 \text{ cm}^2$ ) wurde eine um eine Zehnerpotenz geringere Eintrittshäufigkeit angesetzt als für kleine Lecks. Dies entspricht der Einschätzung der relativen Häufigkeiten von kleinen und großen Lecks in Rohrleitungssystemen. Mittlere Lecks (80 bis  $400 \text{ cm}^2$ ) liegen dazwischen. Die Eintrittshäufigkeiten für kleine, mittlere und große Lecks im Reaktorkühlkreislauf werden durch logarithmische Normalvertei-

lungen mit Medianwerten von  $1 \cdot 10^{-3}$  pro Jahr,  $3 \cdot 10^{-4}$  pro Jahr bzw.  $1 \cdot 10^{-4}$  pro Jahr beschrieben. Die Verteilungen sind jeweils so gewählt, daß ihre Werte mit einer Wahrscheinlichkeit von 90 % in einen Bereich fallen, der zwei Zehnerpotenzen umfaßt.

Die Eintrittshäufigkeiten für die untersuchten Transienten werden auf unterschiedliche Art ermittelt:

- Die Eintrittshäufigkeit des Notstromfalles wird mittels Fehlerbaumanalysen für die einzelnen Ursachen bestimmt, die zum Ausfall der Eigenbedarfsversorgung führen können. Dieser Vorgehensweise wird der Vorzug vor einer statistischen Auswertung bisher aufgetretener Notstromfälle gegeben, weil die Ursachen für Notstromfälle und damit ihre Häufigkeit von spezifischen Gegebenheiten der einzelnen Anlagen abhängen. Es wird ein Erwartungswert von  $10^{-1}$  pro Jahr verwendet. Einzelheiten finden sich in Fachband 2.
- Die Eintrittshäufigkeit für den Ausfall der Hauptspeisewasserversorgung wird auf der Basis der vorhandenen Betriebserfahrungen mit deutschen Druckwasserreaktoren zu 0,8 pro Jahr abgeschätzt.
- Bei kleinen Lecks am Druckhalter wird zwischen dem Notstromfall und sonstigen Transienten unterschieden, weil unterschiedliche Systeme zur Beherrschung verfügbar sind. Für die Häufigkeit des Öffnens des Abblaseventils am Druckhalter wird im ersten Fall die Häufigkeit des Notstromfalls,  $10^{-1}$  pro Jahr, verwendet, im zweiten Fall ergibt sich aus der Betriebserfahrung deutscher Druckwasserreaktoren eine Häufigkeit von 0,5 pro Jahr. Die Wahrscheinlichkeit dafür, daß das Ventil nicht schließt und auch die Abblaseleitung nicht abgesperrt wird, wird durch Fehlerbaumanalysen bestimmt (Fachband 2).
- Für die Untersuchung der ATWS<sup>1)</sup>-Störfälle werden aus der Betriebserfahrung 5 Transienten pro Jahr angesetzt, die eine

---

<sup>1)</sup> *Anticipated Transients Without Scram = Zu erwartende Transienten ohne Reaktorschnellabschaltung*

Reaktorschnellabschaltung erfordern. Die Nichtverfügbarkeit der Reaktorschnellabschaltung wurde durch Fehlerbaumanalysen zu  $5 \cdot 10^{-6}$  ermittelt.

Für die Eintrittshäufigkeit eines Berstens des Reaktordruckbehälters läßt sich eine Schätzung weder aus der Betriebserfahrung mit Reaktordruckbehältern ableiten, weil hierfür der Beobachtungsumfang zu gering ist, noch aus der Erfahrung mit konventionellen Druckbehältern, weil diese mit Reaktordruckbehältern nicht ausreichend vergleichbar sind. In der Risikostudie wurde aufgrund einer technischen Bewertung unter Berücksichtigung der konventionellen Erfahrungen mit einem Wert von  $1 \cdot 10^{-7}$  pro Jahr gerechnet. Nach Ansicht der beteiligten Druckbehälterfachleute stellt dies keinen Erwartungswert, sondern eine obere Abschätzung dar.

Die in der Risikostudie verwendeten Werte für Ausfallraten und -wahrscheinlichkeiten von Komponenten stammen aus drei Quellen:

- Auswertung der einschlägigen Literatur,
- Auswertung von Betriebserfahrungen in den Kernkraftwerken Biblis und Stade,
- Ausfalleffektanalysen für einen Teil der leittechnischen Komponenten.

Das Gewicht, das den einzelnen Datenquellen zukommt, ist je nach verfügbarer Information für die jeweiligen Komponenten verschieden. Generelles Ziel ist jedoch eine möglichst weitgehende Absicherung durch Betriebserfahrungen. Entsprechend den vorhandenen Informationen wird für die Ausfallraten bzw. -wahrscheinlichkeiten die folgende Art der Darstellung gewählt:

- Die Komponenten, für die Daten zu ermitteln sind, werden relativ allgemein definiert. Auf eine Differenzierung nach Bauart, Betriebsweise und anderen Parametern, die sich nicht ausreichend durch Daten belegen lassen, wird verzichtet. Beispielsweise wird die Ausfallart "Pumpe startet nicht" durch die gleichen Daten für alle in den Fehlerbaumanalysen vorkommenden Pumpen beschrieben.

- Die Ausfallraten bzw. -wahrscheinlichkeiten werden nicht durch einen einzelnen Wert, sondern durch Verteilungen beschrieben. Das heißt, es wird zugelassen, daß z.B. eine Ausfallrate verschiedene Werte mit durch die Verteilung gegebenen Wahrscheinlichkeiten annehmen kann. Durch die Verteilungen werden sowohl Unsicherheiten der Daten als auch technische Unterschiede abgedeckt, die sich durch die allgemeine Definition der Komponenten ergeben. Die Streuung der Ausgangsdaten wird in den Ergebnissen der Fehlerbaumanalysen voll berücksichtigt. Es werden logarithmische Normalverteilungen verwendet, die die vorhandenen Daten gut wiedergeben.
- Ausfallraten und -wahrscheinlichkeiten werden als zeitlich konstant betrachtet. Wegen der durch die Verteilungen gegebenen Streuung stellt dies praktisch keine Einschränkung dar.

Der Fachband stellt im Detail dar, auf welche Weise die Verteilungen für die einzelnen Komponenten ermittelt werden. Soweit die Daten auf Literaturwerten beruhen, werden die Verteilungen so gewählt, daß die Streuung der aus unterschiedlichen Literaturstellen stammenden Werte zu gleichen Komponenten dadurch wiedergegeben wird. Hieraus ergeben sich zum Teil Verteilungen mit erheblichen Streuungen. Bei der Auswertung der Kraftwerkserfahrungen werden zu den verschiedenen Komponenten Unterpopulationen gebildet. Die Verteilungen werden in diesem Fall so gewählt, daß sie die Streuung der Werte für die verschiedenen Unterpopulationen wiedergeben. Erwartungsgemäß ergeben sich wesentlich geringere Streuungen als bei den aus der Literatur ermittelten Werten. Der Vergleich von Literatur zu Betriebserfahrungen, der in diesem Fachband für die einzelnen Komponenten dargestellt ist, zeigt jedoch in der Regel eine gute Übereinstimmung im Erwartungswert, der für die Ergebnisse der Analysen ausschlaggebend ist.

Zur Wahrscheinlichkeit menschlichen Fehlverhaltens werden in Phase A der Studie keine eigenen empirischen Untersuchungen durchgeführt. Die Bewertung menschlichen Fehlverhaltens wird

in enger Anlehnung an das Vorgehen der amerikanischen Reaktorsicherheitsstudie (WASH-1400) und zum Teil in der AIPA<sup>1)</sup>-Studie vorgenommen. Die verwendeten Modellvorstellungen und Daten sind in diesem Fachband dokumentiert.

---

<sup>1)</sup> *Accident Initiation and Progression Analysis = Unfallauslösungs- und Unfallablaufanalyse (für den HTR-1160)*



## 2. EINLEITUNG

### 2.1 Gegenstand des Fachbandes

Im vorliegenden Fachband wird ein Teil der Eingangsdaten dargestellt, die zur Durchführung einer Risikostudie erforderlich sind. Es handelt sich um Angaben zu den beiden folgenden Klassen von Ereignissen:

- Ereignisse, die einen risikorelevanten Unfallablauf auslösen können, im folgenden auslösende Ereignisse genannt;
- Nichtverfügbarkeit bzw. Ausfall von Komponenten und Systemen, die zur Beherrschung eines Störfallablaufes erforderlich sind.

Ein auslösendes Ereignis kann seine Ursache haben im Versagen einer technischen Einrichtung in der Anlage (z.B. Leck in einer Hauptkühlmittelleitung), im Versagen technischer Einrichtungen außerhalb der Anlage mit Rückwirkungen auf die Anlage (z.B. Ausfall der elektrischen Fremdversorgung), in einer Fehlbedienung, einer äußeren Einwirkung auf die Anlage (z.B. Erdbeben) oder in einer absichtlichen Einwirkung Dritter auf die Anlage.

Versagen und Störungen technischer Einrichtungen innerhalb der Anlage und außerhalb mit Rückwirkungen auf die Anlage werden in diesem Fachband behandelt, insbesondere werden Angaben zu ihren Eintrittshäufigkeiten gemacht. Diese Häufigkeiten decken sowohl primäres technisches Versagen ab als auch etwaige Fehlbedienung, die zur selben Fehlfunktion technischer Einrichtungen führt. Auslösende Ereignisse, die auf Fehlbedienung zurückzuführen sind, werden daher nicht getrennt ausgewiesen. Einwirkungen von außen werden im Fachband 4 behandelt. Einwirkungen Dritter sind nicht Gegenstand der Studie.

Wichtige Daten zur Beschreibung der Wahrscheinlichkeit, daß Komponenten oder Systeme bei Anforderung nicht verfügbar sind oder in Betrieb oder Bereitschaftszustand ausfallen, sind Ausfallraten und Ausfallwahrscheinlichkeiten pro Anforderung.

Diese Daten sind ein wesentlicher Bestandteil des vorliegenden Bandes. Sie werden in erster Linie für Komponenten angegeben. Die entsprechenden Werte für Systeme werden in den Fehlerbaumanalysen aus den Komponentendaten berechnet. Zum Vergleich sind jedoch auch aus den Betriebserfahrungen ermittelte Werte für die Nichtverfügbarkeiten von Teilsystemen angegeben. Neben den Ausfallwahrscheinlichkeiten hat außerdem die Dauer von Wartungs- und Instandsetzungsarbeiten Einfluß auf die Nichtverfügbarkeit der Systeme. Diese Größen werden ebenfalls in diesem Fachband behandelt. Soweit menschliches Fehlverhalten Einfluß auf die Funktion der betrachteten technischen Einrichtungen haben kann, werden die entsprechenden Daten im vorliegenden Band dargestellt.

## 2.2 Probleme der Datenermittlung

Bei den erwähnten Daten handelt es sich ihrem Wesen nach um Erfahrungswerte. Dies soll zum einen bedeuten, daß die interessierenden Größen aus genügend umfangreichen Beobachtungen statistisch ermittelt werden können. Es bedeutet zum anderen auch, daß in der Regel andere Methoden zu ihrer Ermittlung nur in beschränktem Umfang anwendbar sind.

Schwierigkeiten bei der Ermittlung der gesuchten Daten ergeben sich daher in erster Linie, wenn keine ausreichenden Beobachtungen vorhanden sind. Lücken in der Empirie liegen auf verschiedenen Ebenen vor:

### ● Unzureichende Beobachtbarkeit

Ein herausragendes Beispiel hierfür ist der Reaktordruckbehälter (RDB). Die summierte Betriebszeit aller Reaktordruckbehälter beträgt ca. 1000 Jahre. Die Beobachtung allein, daß hierbei kein Versagen auftrat, läßt keine aussagekräftigen Rückschlüsse auf die RDB-Versagenshäufigkeit zu, die sehr viel geringer ist, als daß ein Versagen in der Beobachtungszeit zu erwarten wäre.

Die mangelnde Beobachtung läßt sich nur bedingt durch einen Vergleich mit konventionellen Druckbehältern ersetzen. Hierfür liegt zwar ausreichend Erfahrungsmaterial vor, für die Studie wurden auch statistische Auswertungen vorgenommen. Diese Behälter unterscheiden sich jedoch sowohl in der Konstruktion als auch in der Qualität erheblich von Reaktordruckbehältern, für die eine qualitative Beurteilung wesentlich höhere Zuverlässigkeit erwarten läßt. Die quantitative Bewertung des Reaktordruckbehälters läßt sich daher nur aufgrund einer fachlichen Beurteilung von Experten vornehmen, statistische Angaben zu konventionellen Behältern werden dabei mit berücksichtigt.

In vielen anderen Fällen seltener Ereignisse genügt es, aus der vorhandenen Betriebserfahrung eine obere Abschätzung abzuleiten. Erwartet man z.B. aufgrund empirisch abgesicherter Ausfallarten im Mittel einen Ausfall auf 100 Anforderungen eines gewissen Systems, dann besteht keine Notwendigkeit, die Wahrscheinlichkeit des Auftretens an sich denkbarer Versagensarten abzuschätzen, die z.B. bei 500 Anforderungen nicht beobachtet wurden, sofern sie vergleichbare Auswirkungen hätten. Solche Abschätzungen sind insbesondere geeignet, den Einfluß unterstellter Ausfallursachen zu begrenzen, die Auswirkungen auf mehrere redundante Stränge eines Systems haben.

#### ● Schwierige Erschließung der Erfahrungen

Für die Durchführung einer Risikostudie ist die Kenntnis einer Reihe von Einzelinformationen wünschenswert, die in dieser Form für andere Zwecke nicht benötigt werden und daher auch nicht unmittelbar verfügbar sind. Vielfach sind diese Informationen in Betriebsdokumentationen enthalten, in erster Linie in den Instandhaltungsunterlagen, zum Teil sind die Daten auch nicht in einer für die Zwecke einer Risikostudie passenden Form erfaßt.

Im Rahmen der Risikostudie wurden in großem Umfang Auswertungen von Betriebsunterlagen vorgenommen. Die Arbeiten sind in

diesem Band dargestellt. Eine praktische Begrenzung dieser Arbeiten ist der große Arbeitsaufwand, den sie erfordern. Angesichts der Vielzahl der benötigten Daten ist die Information über eine Reihe von Komponenten, die in großer Zahl im Einsatz sind, weniger durch die vorhandene Betriebserfahrung, sondern mehr durch den Aufwand ihrer Auswertung beschränkt. Die praktische Durchführung einer Risikostudie ist ein sehr geeignetes Mittel, zu entscheiden, an welcher Stelle der Aufwand zur Reduzierung von Datenunsicherheiten am nutzbringendsten einzusetzen ist. Dieser Umstand wirkte sich bereits in der Phase A der Studie aus und wird zukünftig verstärkt zum Tragen kommen. Denn da die Systemuntersuchungen und die Datenerfassung parallel durchgeführt wurden, trat der Bedarf nach weiterer Absicherung einzelner Daten zum Teil erst zu einem Zeitpunkt auf, der den Abschluß der erforderlichen Auswertungen für den vorliegenden Bericht nicht mehr erlaubte.

Zur Illustration des Sachverhaltes seien etwa Sicherungen angeführt. Muß ein System unmittelbar nach seiner Anforderung verfügbar sein, dann bedeutet das fälschliche Ansprechen einer Sicherung den Ausfall des abgesicherten Systemteils. Entsprechend ist diese Versagensart in der Systemanalyse zu berücksichtigen. Obwohl Sicherungen in großer Zahl eingesetzt sind, ist es schwierig, gesicherte Daten hierzu zu ermitteln, weil keine auf diesen Zweck gerichteten Aufschreibungen verfügbar sind. In der Regel liegt für das Ansprechen einer Sicherung ein Grund vor, z.B. Kurzschluß, in Einzelfällen läßt sich kein Grund ermitteln und das System funktioniert nach Ersetzen der Sicherung. Eine nachträgliche Rekonstruktion solcher Fälle anhand vorhandener Unterlagen ist mit großen Unsicherheiten behaftet.

Dieses Beispiel zeigt einerseits Quellen von Datenunsicherheiten auch bei Komponenten, über die an sich umfangreiche Betriebserfahrungen vorliegen. Zum anderen zeigt das Beispiel aber auch, daß das Gewicht dieser Unsicherheiten durch die sicherheitstechnische Bedeutung der betrachteten Komponenten stark relativiert wird. Bei einem nach den Regeln der Technik abgesicherten System sollte das fälschliche Ansprechen von Si-

cherungen wenig zur Nichtverfügbarkeit des Systems beitragen, so daß auch größere Unsicherheiten in diesem Punkt keinen bemerkenswerten Einfluß auf die Qualität der Gesamtaussage haben.

● Geringe Differenzierung der Angaben

Bei der Durchführung einer Systemanalyse werden Wahrscheinlichkeiten für das Auftreten einer ganz bestimmten Versagensart einer speziellen Komponente unter bestimmten Betriebs- und Umgebungsbedingungen benötigt. In der Regel liegen ausreichende Angaben zu genau dieser Fragestellung nicht vor, dagegen existieren Informationen zu einer breiteren Klasse von Ereignissen, denen das betrachtete Ereignis zugeordnet werden kann. Beispielsweise ist eine Reihe von Informationen über Ausfallraten von Pumpen verfügbar, die sich jedoch auf verschiedene Typen von Pumpen unterschiedlicher Qualitätsanforderungen, mit unterschiedlicher Wartung und unterschiedlichen Betriebsbedingungen beziehen.

Diese Situation kann gegeben sein, wenn man wegen zu geringen Gesamtumfanges der vorliegenden Informationen zu einer speziellen Fragestellung Daten erhebt, um eine gesicherte Aussage daraus abzuleiten. Verstärkt ist das Problem vorhanden, wenn man Angaben aus der Literatur übernimmt, weil die verschiedenen Parameter, die z.B. Einfluß auf die gesuchte Ausfallrate haben können, daraus nicht detailliert genug zu entnehmen sind und der quantitative Einfluß dieser Parameter auch nicht genau angebar ist. In beiden Fällen führt dies dazu, daß keine scharfe Aussage zu der speziellen Fragestellung gemacht werden kann, sondern ein Bereich angegeben wird, in dem der gesuchte Wert liegt.

### 2.3 Folgerungen für die Risikostudie

Die Überlegungen des vorangegangenen Abschnitts lassen sich dahingehend zusammenfassen, daß die Ermittlung von Eintrittshäu-

figkeiten für auslösende Ereignisse und von Zuverlässigkeitskenngrößen für Komponenten unvermeidlich mit Unsicherheiten behaftet ist. Die Unsicherheiten resultieren teils daraus, daß die interessierenden Werte statistische Größen sind, teils resultieren sie aus den zur Verfügung stehenden Informationsquellen. Für die Ermittlung der Daten und ihre Darstellung wird daraus gefolgert:

- Für die Festlegung der Daten und ihre Verwendung in der Risikostudie ist ein Konzept anzuwenden, bei dem die vorhandenen Unsicherheiten explizit berücksichtigt werden. Die Unschärfe der Eingangsdaten findet ihren Niederschlag in einer Unschärfe der resultierenden Risikoaussagen.
- Die Daten werden nur für den jeweiligen Anwendungszweck in der Risikostudie ermittelt. Eine feinere Differenzierung oder größere Genauigkeit, als es der Anwendungszweck erfordert, wird nicht angestrebt. Teilweise werden obere Abschätzungen verwendet.
- Die Art der Datenermittlung orientiert sich an den jeweils zur Verfügung stehenden Informationen. Eine durchgängige, einheitliche Methodik ist nicht anwendbar.
- Aus der Darstellung der Ergebnisse soll im einzelnen nachvollziehbar sein, aus welchen Ausgangsinformationen auf welche Art welche Daten abgeleitet wurden. Soweit ingenieurmäßige Abschätzungen erforderlich sind, die sich auf eine allgemeine technische Bewertung statt auf einzeln belegbare Fakten stützen, wird dies explizit ausgewiesen. Solche Abschätzungen sollen sich auf offensichtliche Fälle beschränken und pessimistisch vorgenommen werden. Existieren beispielsweise Daten zu einer Komponente zu ungünstigeren Umgebungsbedingungen, als sie im Anwendungsfall der Studie vorliegen, und ist der Einfluß der Umgebungsbedingungen nicht quantitativ belegbar, dann werden die Daten unverändert übernommen.

Der letzte Punkt widerspricht etwas dem Ziel, möglichst realistische Risikoaussagen zu machen, weil er eine gewisse Konservativität impliziert. Dieser Nachteil erscheint jedoch unver-

meidlich, wenn der Bericht einer objektiven Diskussion zugänglich bleiben soll.

## 2.4 Aufbau des Fachbandes

Kapitel 3 beschäftigt sich mit den Eintrittshäufigkeiten der auslösenden Ereignisse. Es werden nur die Ereignisse behandelt, die die größten Beiträge zum Gesamtrisiko erwarten lassen und für die daher detaillierte Ereignisablaufanalysen durchgeführt wurden (Fachband 1).

In Kapitel 4 werden die Untersuchungen zur Abschätzung der Versagenshäufigkeit des Reaktordruckbehälters dargestellt. Die Darstellung der Arbeiten zur Ermittlung der Zuverlässigkeitskenngrößen für die übrigen Komponenten ist wegen des umfangreichen Materials auf die Kapitel 5 bis 8 und die Anhänge verteilt.

Kapitel 5 gibt den Überblick über das allgemeine Vorgehen, die Behandlung der Datenunsicherheiten, die angewendeten Modellvorstellungen und die Kombination von Daten aus der Literatur mit eigenen Betriebsauswertungen.

Kapitel 6 besteht aus der zusammenfassenden Darstellung der Auswertung von Betriebserfahrungen und der erzielten Ergebnisse.

In den Kapiteln 7 und 8 ist die Ermittlung der Daten für die einzelnen in der Risikostudie verwendeten Komponenten wiedergegeben. Dabei beschäftigt sich Kapitel 7 mit den verfahrens- und elektrotechnischen Komponenten, Kapitel 8 mit der Leittechnik. Eine getrennte Behandlung ergibt sich aus den unterschiedlichen zur Verfügung stehenden Ausgangsinformationen. Die in diesen Kapiteln verwendeten Ausgangsquellen und ihre Zuordnung zu den einzelnen Komponenten sind in Übersichtstabellen in den Anhängen zusammengefaßt.

Kapitel 9 beschreibt die für die Fehlerbaumanalysen verwendeten Basisdaten zu menschlichem Fehlverhalten.

### 3. AUSLÖSENDE EREIGNISSE

In der Phase A der Studie wurden detaillierte Ereignisablaufanalysen für folgende auslösende Ereignisse durchgeführt:

- Kühlmittelverluststörfälle:
  - kleines Leck
  - mittleres Leck
  - großes Leck
  - kleines Leck am Druckhalter
- Transienten:
  - Notstromfall
  - Ausfall der Hauptspeisewasserversorgung
  - ATWS-Störfälle

Eine gesonderte Untersuchung des Ereignisablaufs bei Versagen des Reaktordruckbehälters wurde wegen der geringen Eintrittshäufigkeit nicht durchgeführt.

#### 3.1 Kühlmittelverluststörfälle

##### 3.1.1 Lecks in einer Hauptkühlmittelleitung

Im folgenden werden die Eintrittshäufigkeiten der auslösenden Ereignisse für die in den Fachbänden 1 und 2 untersuchten Störfallabläufe mit Kühlmittelverlust über Lecks in einer Hauptkühlmittelleitung ermittelt. Die Definition der zu untersuchenden Ereignisse orientiert sich an den Wirksamkeitsanforderungen, die der Systemanalyse zugrunde liegen. Sie sind in Tabelle 5-1 des Hauptbandes angegeben. Dort werden die verschiedenen Leckgrößen entsprechend der effektiven Ausströmfläche folgendermaßen unterschieden:

großes Leck	> 400 cm <sup>2</sup>
mittleres Leck	80 cm <sup>2</sup> bis 400 cm <sup>2</sup>
kleines Leck	2 cm <sup>2</sup> bis 80 cm <sup>2</sup>
sehr kleines Leck	< 2 cm <sup>2</sup>



Bei der zuletzt genannten Leckgröße können die Kühlmittelverluste durch das Volumenregelsystem abgedeckt werden. Zusätzlich stehen die gleichen Systeme wie zur Beherrschung kleiner Lecks zur Verfügung. Da die sehr kleinen Lecks damit keinen merklichen Beitrag zum Risiko liefern, wurden hierfür keine detaillierten Ereignisablaufanalysen durchgeführt. Im folgenden werden daher nur die Eintrittshäufigkeiten solcher Ereignisse betrachtet, bei denen die erforderlichen Wirksamkeitsbedingungen den Ausströmraten der drei übrigen Leckgrößen entsprechen. Bei der Bewertung der Betriebserfahrungen werden damit neben sehr kleinen Lecks auch absperrbare Leckagen ausgeschlossen. Grenzfälle werden im folgenden diskutiert, um zu demonstrieren, wie weit sie durch die durchgeführten Systemanalysen abgedeckt sind.

Zur Ermittlung der Eintrittshäufigkeiten sind grundsätzlich zwei Vorgehensweisen denkbar:

- Untersuchungen von Schadensfällen in Rohrleitungssystemen im nichtnuklearen Bereich, Übertragung der Ergebnisse auf den Reaktorkühlkreislauf eines Druckwasserreaktors;
- Auswertung der Betriebserfahrungen mit Leichtwasserreaktoren auf die interessierenden Ereignisse hin.

Es existieren mehrere zusammenfassende Darstellungen zur Versagenshäufigkeit von Rohrleitungssystemen, in denen die jeweils verfügbaren Quellen zu konventionellen und nuklearen Anlagen ausgewertet wurden /F3, 3-1, -2 und -3/. Die Autoren stimmen darin überein, daß solche Auswertungen mit relativ großen Unsicherheiten behaftet sind. Diese stammen aus mangelnder Kenntnis des jeweiligen Bestandes (charakterisiert durch Länge des betrachteten Rohrleitungssystems, Werkstoffe, Qualitätsanforderungen usw.), Schwierigkeiten bei der Klassifizierung der Schäden und Unsicherheiten beim Vergleich von Rohrleitungen mit unterschiedlichen Betriebsbedingungen und Qualitätsstandards. Die Aussagen geben daher nur die Größenordnung wieder und lassen Raum für subjektive Interpretation. Im folgenden werden zunächst die wichtigsten Quellen diskutiert, auf die sich die Abschätzungen in /F3, 3-1/ beziehen:

Auswertungen der Betriebserfahrungen amerikanischer Kernkraftwerke liefern infolge ihres beschränkten Umfangs nur obere Grenzwerte, die je nach Interpretation der Daten für kleine Lecks zwischen  $10^{-2}$  und  $7 \cdot 10^{-4}$  pro Jahr und für große zwischen  $7 \cdot 10^{-3}$  und  $5 \cdot 10^{-4}$  pro Jahr liegen. Diese und die im folgenden genannten Zahlen beziehen sich jeweils auf den ganzen Reaktorkühlkreislauf. Aus einem General-Electric-Bericht (GEAP 574) über Rohrleitungen in konventionellen Anlagen wird für kleine Lecks ein Wert von  $2 \cdot 10^{-3}$  pro Jahr und für große von  $9 \cdot 10^{-5}$  pro Jahr abgeleitet. Die hauptsächliche Unsicherheit liegt hierbei in der Übertragung der Daten auf den Reaktorkühlkreislauf eines Kernkraftwerkes, sowohl was die Relevanz der Schäden als auch den Bestand der unterschiedlichen Rohrleitungen angeht.

Aus Phillips und Warwick /F3, 3-4/ wird  $5 \cdot 10^{-4}$  pro Jahr für kleine und  $2 \cdot 10^{-5}$  pro Jahr für große Brüche übernommen. Die Zahlen stammen aus der Auswertung von Schäden in Rohrleitungssystemen konventioneller Kesselanlagen, jedoch wurde von den Autoren eine Bewertung der einzelnen Schäden daraufhin vorgenommen, wieweit sie auf den Reaktorkühlkreislauf von Kernkraftwerken übertragbar sind. Eine Unsicherheit ergibt sich aus der unterschiedlichen Kategorisierung der Schäden. In /F3, 3-4/ wird nicht nach kleinen und großen Lecks unterschieden, sondern nach "potentiell gefährlichen" und "katastrophalen" Schäden. Als katastrophal werden Brüche bezeichnet, die größere Reparaturen oder Austausch erfordern, als potentiell gefährliche Schäden, die beseitigt werden müssen und bei denen die Betriebsbedingungen zu einer gefährlichen Ausweitung des bekannten Schadens führen können. In /F3, 3-1/ werden diese beiden Kategorien als näherungsweise anwendbar auf die Klassen großer und kleiner Brüche interpretiert.

Schließlich werden Auswertungen des Systems "Reliability Service" in Großbritannien an konventionellen Kesselanlagen zitiert und daraus Werte von  $< 3 \cdot 10^{-3}$  pro Jahr für kleine Lecks und  $1,5 \cdot 10^{-4}$  pro Jahr für große Lecks abgeleitet.

Die in /F3, 3-1/ verwendeten Eintrittshäufigkeiten für die verschiedenen Leckgrößen wurden durch logarithmische Normalverteilungen beschrieben. Die Datenunsicherheit drückt sich darin aus, daß der Bereich, in dem die Werte mit einer Wahrscheinlichkeit von 90 % liegen, jeweils zwei Größenordnungen umfaßt. Es wurden folgende Werte verwendet:

Leckgröße (inch)	Eintrittshäufigkeit (pro Jahr)	
	90-%-Bereich	Median
1/2 - 2	$1 \cdot 10^{-4}$ bis $1 \cdot 10^{-2}$	$1 \cdot 10^{-3}$
2 - 6	$3 \cdot 10^{-5}$ bis $3 \cdot 10^{-3}$	$3 \cdot 10^{-4}$
> 6	$1 \cdot 10^{-5}$ bis $1 \cdot 10^{-3}$	$1 \cdot 10^{-4}$

Bush /F3, 3-2/ stützt sich im wesentlichen auf dieselben Quellen wie in WASH-1400, erweitert durch eine neuere Arbeit von Smith und Warwick /F3, 3-5/, die in WASH-1400 noch nicht berücksichtigt wurde. Darin werden aus konventionellen Kesselanlagen bei Betrachtung der auf den Reaktorkühlkreislauf übertragbaren Schäden  $6 \cdot 10^{-4}$  pro Jahr für potentiell gefährliche Schäden und  $4,7 \cdot 10^{-5}$  pro Jahr für katastrophale Schäden ermittelt. Die Arbeiten /F3, 3-4 und -5/ decken verschiedene Betriebszeiträume ab, d.h., die verwendeten Bestände sind unabhängig voneinander. Bush gibt den Bereich für die Eintrittshäufigkeit von großen Lecks in Rohrleitungen mit  $10^{-4}$  bis  $10^{-6}$  pro Jahr an mit steigender Tendenz für geringere Durchmesser. Die gegenüber WASH-1400 um etwa eine Größenordnung günstigeren Werte sind im wesentlichen auf eine andere Beurteilung der Frage zurückzuführen, welche Fehler für Aussagen zum Versagen von Hauptkühlmitteleitungen herangezogen werden sollten.

Boesebeck und Heuser /F3, 3-3/ geben keine Empfehlung über anwendbare Ausfallraten, sondern eine zusammenfassende Darstellung der verfügbaren Quellen. Neben den oben diskutierten Zahlen weisen sie insbesondere auf Auswertungen für Kernreaktoren hin, die in /F3, 3-4 und -5/ zusätzlich zu den oben diskutier-

ten Angaben über konventionelle Anlagen genannt werden und in WASH-1400 nicht herangezogen wurden. Bei Gleichsetzung der unterschiedlichen Schadenskategorien, die in diesen beiden Quellen einerseits und in WASH-1400 andererseits verwendet wurden, führen diese Auswertungen zu ungünstigeren Werten, als sie in WASH-1400 für den Reaktorkühlkreislauf angesetzt wurden. Absicht der Autoren von /F3, 3-4 und -5/ war nicht, Eintrittshäufigkeiten für Kühlmittelverluststörfälle abzuleiten. Sie ziehen aus ihren Untersuchungen lediglich den Schluß, daß die Übertragung von Schadensraten konventioneller Anlagen auf nukleare nicht notwendig pessimistisch ist. Da sie in beiden Fällen dieselben Schadenskategorien anwenden, bleibt dieser Schluß von der Bewertung der Einzelfälle unberührt.

In /F3, 3-4/ werden für Kernkraftwerke keine katastrophalen Fehler berichtet und deswegen hierüber keine Aussagen gemacht. Für potentiell gefährliche Fehler wird eine Zahl von  $1 \cdot 10^{-2}$  pro Jahr genannt. Für diese Kategorie gibt /F3, 3-5/ einen Wert von  $1,7 \cdot 10^{-2}$  pro Jahr und für katastrophale Fehler  $5,7 \cdot 10^{-3}$  pro Jahr wieder, basierend auf sechs Schäden. Darüber hinaus wurden die Bestände von /F3, 3-4 und -5/ zusammengefaßt und daraus Werte von  $1,5 \cdot 10^{-2}$  pro Jahr bzw.  $2,5 \cdot 10^{-3}$  pro Jahr für beide Kategorien abgeleitet.

Die gegenüber WASH-1400 hohen Werte erklären sich aus den unterschiedlichen zugrunde liegenden Schadenskategorien. Aus der Aufschlüsselung der Art der Entdeckung von potentiell gefährlichen Schäden geht hervor, daß ein Drittel durch Leckage, der Rest durch optische Inspektion, zerstörungsfreie Prüfung und Druckproben entdeckt wird. Das heißt mit anderen Worten, daß in der Mehrzahl der Fälle kein Kühlmittelverlust vorlag. Sie können daher nicht für die Bestimmung der Eintrittshäufigkeit von Lecks im Reaktorkühlkreislauf herangezogen werden. Die Größe der Leckagen ist nicht angegeben; zweifellos ist auch hiervon nur ein Teil für die Untersuchung von Kühlmittelverluststörfällen relevant. Damit sind die Angaben von /F3, 3-4 und -5/ in guter Übereinstimmung mit dem Bereich, der in WASH-1400 für die Eintrittshäufigkeiten kleiner Lecks angenommen wird.

Die katastrophalen Versagen, die in /F3, 3-5/ für nukleare Anlagen herangezogen wurden, sind einzeln aufgezählt. Es handelt sich tatsächlich nicht um sechs, sondern nur um fünf Fälle, zwei der Berichte, die verschiedenen Quellen entnommen wurden, beziehen sich auf dasselbe Ereignis.

Keines der Ereignisse stellt einen Kühlmittelverluststörfall dar. Nur in einem Fall war der Reaktorkühlkreislauf eines Druckwasserreaktors betroffen, der Schaden trat jedoch nicht während des Betriebs, sondern bei einer Druckprüfung auf. Ein weiterer Schaden bezieht sich auf einen gasgekühlten Reaktor, der Fehler ereignete sich bei Prüfungen vor Beladen des Reaktors. Die restlichen drei Fälle betreffen den Sekundärkreis von Druckwasserreaktoren, zwei davon traten bei der heißen Funktionsprüfung vor Inbetriebnahme der Anlagen auf. In einer Statistik, aus der die Häufigkeit von Lecks im Reaktorkühlkreislauf eines in Betrieb befindlichen Reaktors abgeschätzt werden soll, sind diese Schäden nicht zu berücksichtigen. Im Rahmen der Unsicherheit, die sich durch Unterschiede des betrachteten Bestandes ergibt (z.B. Einbeziehung gasgekühlter Reaktoren), führt damit auch die Untersuchung dieser Fälle etwa auf den Bereich, der in WASH-1400 für die Eintrittshäufigkeit von Kühlmittelverluststörfällen angegeben wird.

Eine Auswertung von Betriebserfahrungen kommerzieller Leichtwasserreaktoren im Hinblick auf Kühlmittelverlust läßt schärfere Aussagen erwarten, als das in WASH-1400 der Fall war, weil die Anzahl der Betriebsjahre inzwischen gestiegen ist. Zumindest die für kleine Lecks angesetzten Werte liegen in der Größenordnung des statistisch Belegbaren. Zu bedenken ist dabei, daß der Erwartungswert einer logarithmischen Normalverteilung, deren 90-%-Bereich zwei Zehnerpotenzen umfaßt, um den Faktor 2,7 höher liegt als ihr Median, für kleine Lecks also bei  $2,7 \cdot 10^{-3}$  pro Jahr.

Die Betriebsjahre mit Leichtwasserreaktoren liegen weltweit in der Größenordnung von 1000, die entsprechenden Betriebserfahrungen sind jedoch unterschiedlich gut zugänglich. So gut wie

keine Informationen sind für Reaktoren in osteuropäischen Ländern verfügbar. Sie sind für eine statistische Auswertung daher nicht verwendbar. Schließt man diese Anlagen aus, dann verbleiben etwa 800 Jahre, die sich etwa gleichmäßig auf Druck- und Siedewasserreaktoren verteilen. Auch hierüber lagen keine für die Studie auswertbaren umfassenden Dokumentationen vor, doch kann mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden, daß gravierende Ereignisse wie Kühlmittelverluststörfälle bekanntgeworden wären. Beschränkt man sich auf die Erfahrungen der Bundesrepublik und der USA, für die ausreichend Unterlagen vorhanden sind, dann verbleiben etwa 500 Betriebsjahre kommerzieller Leichtwasserreaktoren wieder etwa zur Hälfte auf Druck- und Siedewasserreaktoren verteilt.

Die Erfahrungen mit Siedewasserreaktoren können herangezogen werden, wenn die typspezifischen Unterschiede Beachtung finden. Zu berücksichtigen sind Kühlmittelverluste des Frischdampf- und Speisewasserkreises innerhalb des Sicherheitsbehälters, die nicht absperbar sind.

Zur Abschätzung der Häufigkeit von Kühlmittelverluststörfällen aus der Betriebserfahrung sind solche Ereignisse heranzuziehen, bei denen Kühlmittelverluste in dem Umfang auftreten, wie dies für die Analysen der Risikostudie unterstellt wird, bzw. bei denen in vergleichbarem Umfang der Einsatz von Sicherheitssystemen erforderlich ist.

Aus den deutschen und amerikanischen Erfahrungen ergab sich, daß in einigen Fällen Sicherungssysteme, in erster Linie die Sicherheitseinspeisung, automatisch in Betrieb gingen. Die Kühlmittelverluste waren jedoch in allen Fällen weniger gravierend, als dies in der Ereignisablaufanalyse der Risikostudie unterstellt wurde.

Der bisher größte Kühlmittelverlust aus einem Reaktorkühlkreislauf trat mit 550 t im Kernkraftwerk Robinson, Block 2, im Mai 1975 auf; die maximale Ausströmrates betrug ca. 100 t/h. Ursache war die defekte Dichtung einer Hauptkühlmittelpumpe. Von der

Ausströmrate und der insgesamt ausgetretenen Menge her liegt dieser Fall in dem Bereich, den die Untersuchungen zum kleinen Leck abdecken. Tatsächlich lief der Störfall erheblich günstiger ab, als dies in der Ereignisablaufanalyse unterstellt wurde, weil die starke Ausströmung erst 4 Stunden nach Abschaltung des Reaktors auftrat, die bei wesentlich geringerer Leckage ausgelöst worden war. Leckagen über Dichtungen von Hauptkühlmittelpumpen traten auch bei anderen Anlagen auf, jedoch handelte es sich jeweils um weit geringere Ausströmraten und Mengen.

Eine noch höhere Ausströmrate mit maximal ca. 180 t/h trat 1972 im Kernkraftwerk Obrigheim aufgrund des fälschlichen Öffnens einer Entwässerungsleitung auf. Das Leck konnte jedoch nach 13 Minuten durch Schließen einer Armatur abgesperrt werden, insgesamt traten ca. 34 t Primärwasser aus. Dieser Fall ist aufgrund anlagentechnischer Unterschiede nicht auf die Referenzanlage übertragbar.

Ein Leck von ca. 1 cm Durchmesser trat 1972 im Kernkraftwerk Surry 1 durch Lösen eines Temperaturfühlers auf. Dieses Leck liegt unterhalb des für die Ereignisablaufanalysen definierten Bereichs für kleine Lecks mit einer Mindestleckfläche von  $2 \text{ cm}^2$ . Leckagen über kleinere Leckflächen können durch das Volumenregelsystem ausgeglichen werden. Im vorliegenden Fall wurde die Sicherheitseinspeisung, die bei amerikanischen Anlagen gegen den Betriebsdruck einspeisen kann, von Hand vorübergehend in Betrieb genommen.

Brüche eines Dampferzeuger-Heizrohrs traten in zwei Fällen auf. Auch hier lag der Kühlmittelverlust unterhalb der Menge, die bei den Analysen der kleinen Lecks betrachtet wurde.

Zusammenfassend läßt sich feststellen, daß in den betrachteten ca. 500 Betriebsjahren keine Leckage auftrat, die an die Sicherheitssysteme solche Anforderungen stellte, wie dies für kleine Lecks unterstellt wird. Damit ist es unwahrscheinlich, daß die Eintrittshäufigkeit für kleine Lecks wesentlich über  $2 \cdot 10^{-3}$  pro Jahr liegt. Bei einem unterstellten Wert von  $1 \cdot 10^{-2}$  pro

Jahr ist z.B. die Wahrscheinlichkeit, in 500 Jahren keinen Fall zu beobachten, kleiner als 1 %. Andererseits erhält man aus den vorhandenen Erfahrungen für Kühlmittelverluste mit geringeren Anforderungen an Sicherheitssysteme einen Wert von ca.  $1 \cdot 10^{-2}$  pro Jahr. Beide Überlegungen zeigen, daß die vorhandenen Unsicherheiten durch eine logarithmische Normalverteilung, bei der die Werte mit einer Wahrscheinlichkeit von 90 % zwischen  $10^{-4}$  und  $10^{-2}$  pro Jahr liegen, bei weitem abgedeckt werden, und daß es nach den vorliegenden Betriebserfahrungen unwahrscheinlich ist, daß der tatsächliche Wert am oberen Ende dieses Bereiches liegt. Eine solche Verteilung wurde daher für die Eintrittshäufigkeit kleiner Lecks verwendet.

Für die Ermittlung von Eintrittshäufigkeiten mittlerer (80 bis 400 cm<sup>2</sup> Leckagefläche) und großer Kühlmittelverluste (über 400 cm<sup>2</sup> Leckagefläche) reichen die Betriebserfahrungen mit Kernkraftwerken nicht aus. Die konventionellen Erfahrungen liefern hierfür Werte, die um etwa eine Größenordnung günstiger sind als für kleine Lecks, wobei eine genaue Differenzierung nach Leckgrößen schwierig ist. Dennoch wurde für die Ereignisablaufanalysen wegen des unterschiedlichen zu erwartenden Ablaufs zwischen großen und mittleren Lecks unterschieden. Die geringere Eintrittshäufigkeit großer Lecks ist plausibel, zum einen, weil sie nur an Leitungen mit entsprechend großem Querschnitt auftreten können, zum anderen, weil sich nur ein Teil der Lecks zu großen Querschnitten ausweitet. Für die Ereignisablaufanalysen wurde daher eine Verteilung der Eintrittshäufigkeit für große Lecks verwendet, die um eine Größenordnung niedriger liegt als die für kleine. Für mittlere Lecks wurde zwischen diesen beiden Bereichen interpoliert. Die Differenzierung zwischen großen und mittleren Lecks, die sich nach dieser Festlegung etwa um den Faktor 3 unterscheidet, liegt unterhalb der Auflösungsgenauigkeit der vorhandenen Ausgangsdaten. Qualitativ ist jedoch die Einordnung zwischen kleinen und größeren Lecks sinnvoll. Zu berücksichtigen ist, daß die für die einzelnen Leckgrößen angesetzten Schwankungsbreiten größer sind als der Abstand der Werte für mittlere Lecks von denen für große bzw. kleine Lecks.



Zusammenfassend ist festzuhalten: Für die Eintrittshäufigkeiten der verschiedenen behandelten Kühlmittelverluststörfälle müssen zwar entsprechend der Unschärfe der vorliegenden Daten relativ breite Bereiche zugelassen werden, diese Bereiche selbst sind aber durch die vorhandenen Erfahrungen gut belegbar. Insbesondere zeigen sie, daß eine Unterschätzung der Eintrittshäufigkeiten durch die verwendeten Daten unwahrscheinlich ist.

### 3.1.2 Kleines Leck am Druckhalter

Beim folgenschwersten Störfall in einem Kernkraftwerk, dem Störfall in Three Mile Island (TMI), spielte Kühlmittelverlust über ein Druckhalterabblaseventil eine entscheidende Rolle. Die Untersuchung dieses Störfalles hat bestätigt, daß es nicht sinnvoll ist, die Eintrittshäufigkeit eines solchen Ereignisses statistisch aus den Erfahrungen mit unterschiedlichen Anlagen abzuschätzen, weil sie sehr stark vom Anlagenkonzept abhängt. Die Wahrscheinlichkeit für Kühlmittelverlust über ein Druckhalterabblaseventil setzt sich zusammen aus den Häufigkeiten bzw. Wahrscheinlichkeiten für

- Öffnen des Ventils,
- fälschliches Offenbleiben,
- Unterbleiben der Absperrung durch ein zusätzliches Absperrventil in der Abblaseleitung.

Die Häufigkeit des Öffnens ist von einer Vielzahl von Anlageeigenschaften abhängig, die auf die Häufigkeit von Transienten und ihren Verlauf Einfluß haben. Die Wahrscheinlichkeit für das Unterbleiben der Absperrung hängt in erster Linie davon ab, wie die Offenstellung des Abblaseventils überwacht und welche Aktion daraus abgeleitet wird. Die erheblichen Unterschiede zu anderen Anlagen sind nach dem TMI-Störfall ausführlich diskutiert worden; darauf soll hier nicht eingegangen werden. Sie äußern sich z.B. dadurch, daß von den 11 bekannten Fällen, bei denen vor dem Störfall in Three Mile Island an amerikanischen Druckwasserreaktoren ein Abblaseventil offen blieb, 9 an Anlagen desselben Herstellers auftraten. An deutschen Druckwas-

serreaktoren trat kein Fall eines offenbleibenden Abblaseventils auf.

In der Risikostudie wurde die Häufigkeit für einen Kühlmittelverlust über ein Abblaseventil daher analytisch ermittelt. Sie ergibt sich aus der Häufigkeit von Transienten, die zu einem Ansprechen des Abblaseventils führen, der Wahrscheinlichkeit für Offenbleiben des Ventils und der Wahrscheinlichkeit, daß zusätzlich die Absperrarmatur in der Abblaseleitung nicht geschlossen wird. Hierbei werden die speziellen Verhältnisse in der Referenzanlage zugrunde gelegt. Die Analysen sind im Fachband 2 dargestellt.

An Transienten, die zu einem Öffnen des Abblaseventils führen, sind zu unterscheiden:

- Notstromfall,
- sonstige Transienten, die zu einem Öffnen des Abblaseventils führen.

Die Häufigkeit des Notstromfalls wurde zu 0,1 pro Jahr ermittelt. Darauf wird im folgenden Abschnitt eingegangen.

Die Häufigkeit von sonstigen Transienten, die zu einem Ansprechen des Abblaseventils führen, wurde mit Hilfe der Betriebserfahrung deutscher Druckwasserreaktoren bestimmt. Hierbei ist jedoch zu berücksichtigen, daß in den Auslegungsdaten und in der Konzeption der Regelung Unterschiede zwischen den Anlagen bestehen.

Bei deutschen Kernkraftwerken mit Druckwasserreaktor wurden bei insgesamt 24 Transienten Druckhalter-Abblaseventile geöffnet. Dies ist auf 26 Betriebsjahre zu beziehen. Die Hälfte der Fälle trat an einer Anlage auf, die im Gegensatz zu neueren Anlagen keinen Stabeinwurf hat. Weitere 6 Fälle sind auf einen inzwischen beseitigten Fehler in der Verdrahtung der Stabsteuerung einer anderen Anlage zurückzuführen, aufgrund dessen einzelne Stäbe nicht eingeworfen wurden. In der Referenzanlage führte in den gut 3 Jahren seit der Übergabe einmal eine Transiente zum Öffnen des Abblaseventils. Aus diesen Informationen

kann für die Referenzanlage eine Häufigkeit von ca. 0,5 pro Jahr für das Öffnen eines Druckhalter-Abblaseventils abgeschätzt werden. Zieht man davon die Häufigkeit des Notstromfalls ab, so erhält man die Häufigkeit der sonstigen Transienten, die zu einem Öffnen des Abblaseventils führen, nämlich 0,4 pro Jahr.

### 3.2 Transienten

#### 3.2.1 Notstromfall

Die Eintrittshäufigkeit des Notstromfalles wurde nicht statistisch ermittelt. Zwar handelt es sich hierbei um ein Ereignis, dessen Eintrittshäufigkeit einer statistischen Behandlung zugänglich ist, zum einen ist jedoch eine vollständige Dokumentation aufgetretener Notstromfälle und ihrer jeweiligen Ursachen nicht verfügbar, zum anderen ergeben sich auch Probleme der Übertragbarkeit der Daten für verschiedene Anlagen. Soweit Notstromfälle durch Störungen außerhalb der Anlage verursacht werden, hängt ihre Häufigkeit vom Aufbau des Netzes ab, in das das Kraftwerk einspeist, sowie von der Art der Netzeinbindung. Beide Faktoren unterscheiden sich von Anlage zu Anlage.

Dasselbe trifft auch für Störungen zu, die ihre Ursache innerhalb der Anlage haben; hier ist der Aufbau der entsprechenden Systeme von Bedeutung.

Aus diesem Grunde wurde die Eintrittshäufigkeit des Notstromfalles durch Analyse der Einzelursachen ermittelt, die zum Ausfall der Eigenbedarfsversorgung führen können. Die Einzelbewertungen sind im Fachband 2 dargestellt, insgesamt ergibt sich eine Eintrittshäufigkeit von  $10^{-1}$  pro Jahr. Dieser Wert ist mit den Kraftwerkserfahrungen verträglich, eine Bestätigung anhand der Referenzanlage ist nicht möglich. Sie nahm den Leistungsbetrieb vor ca. drei Jahren auf, ein Notstromfall trat in dieser Zeit nicht ein.

### 3.2.2 Ausfall der Hauptspeisewasserversorgung

Ein vollständiger Ausfall der Hauptspeisewasserversorgung tritt beim Notstromfall ein. Unabhängig davon ist aufgrund der Betriebserfahrungen in deutschen Kernkraftwerken mit vollständigen Ausfällen der Hauptspeisewasserversorgung zu rechnen: In 26 Betriebsjahren der Anlagen mit Druckwasserreaktor traten 20 derartige Ausfälle ein. Daraus ergibt sich eine mittlere Eintrittshäufigkeit von 0,8 pro Jahr. Zu beachten ist dabei, daß in der Hälfte der Fälle die Hauptspeisewasserversorgung innerhalb weniger Minuten wieder in Betrieb genommen werden konnte.

### 3.2.3 ATWS - Störfälle

Versagt bei zu erwartenden Transienten, die das Eingreifen von Sicherheitssystemen erfordern, die Reaktorschnellabschaltung, so spricht man von ATWS-Störfällen. Wegen der hohen Zuverlässigkeit der Reaktorschnellabschaltung sind solche Störfälle sehr unwahrscheinlich. Sie sind noch nie aufgetreten. Ihre Häufigkeit kann daher nicht aus der Betriebserfahrung ermittelt werden.

Aus der Betriebserfahrung in deutschen Kernkraftwerken mit Druckwasserreaktor kann aber die Eintrittshäufigkeit von zu erwartenden Transienten, die das Eingreifen von Sicherheitssystemen erfordern, abgeschätzt werden. Dafür liefert die Häufigkeit der bei Leistungsbetrieb ausgelösten Reaktorschnellabschaltungen einen oberen Grenzwert. Diese Häufigkeit variiert zwischen etwa 3 und 7 pro Jahr, der Mittelwert liegt bei 5 pro Jahr.

Die Wahrscheinlichkeit des Ausfalls einer angeforderten Reaktorschnellabschaltung muß analytisch ermittelt werden. In Zuverlässigkeitsuntersuchungen wurde eine Wahrscheinlichkeit von  $5 \cdot 10^{-6}$  abgeschätzt (Fachband 2). Durch Multiplikation mit der Häufigkeit der Auslösung der Reaktorschnellabschaltung ergibt sich die Häufigkeit von ATWS-Störfällen zu  $3 \cdot 10^{-5}$  pro Jahr.

#### 4. REAKTORDRUCKBEHÄLTERVERSAGEN

##### 4.1 Statistische Betrachtungen

Zum Jahresende 1977 waren weltweit Kernkraftwerke mit insgesamt 206 Reaktorblöcken in Betrieb, die bis zu diesem Zeitpunkt zusammen etwa 1500 Reaktorbetriebsjahre erbracht hatten. Ein Aufreißen oder Bersten eines Reaktordruckbehälters ist bisher nicht eingetreten. Wird angenommen, ein Reaktordruckbehälter sei gebrochen, so ergibt sich bei 1500 Betriebsjahren eine Versagenshäufigkeit, die im Vergleich zu Zahlen aus der herkömmlichen Druckbehältertechnik unrealistisch hoch ist. Daran wird deutlich, daß die in Kernkraftwerken gesammelten Betriebserfahrungen zu gering sind, um daraus eine hinreichend verlässliche Versagenshäufigkeit für einen Reaktordruckbehälter bestimmen zu können.

Eine wesentliche zuverlässigere Aussage über Versagenshäufigkeiten läßt sich für die in anderen technischen Bereichen eingesetzten Druckbehälter machen, wie z.B. im Dampfkesselbetrieb oder in der chemischen Industrie. Im Rahmen der Risikostudie wurde daher eine Schadensstatistik für derartige Behälter aufgestellt /F5, 4-1/. Zur Ermittlung der Schäden wurden die beim VdTÜV-Fachauschuß "Schadensfragen" vorliegenden Schadensberichte aus dem Zeitraum 1959 bis 1976 ausgewertet. Die dazugehörige Bezugsmenge bildete sich aus den im gleichen Zeitraum nach der Dampfkesselverordnung bzw. nach der Unfallverhütungsvorschrift von den Technischen Überwachungs-Vereinen wiederkehrend zu prüfenden Dampfkesseln und Druckbehältern (TÜV-Bestand). Für die in der Statistik zu erfassenden Versagen wurden folgende Definitionen getroffen:

##### ● Versagen mit Bersten des Behälters

Zerknall - spontane Werkstofftrennung in der drucktragenden Umschließung des Behälters, einschließlich der Stutzen und Verschraubungen, die mit dem plötzlichen Verlust eines großen Vo-

lumens des eingeschlossenen Druckmittels verbunden ist (disruptive vessel failure).

● Versagen ohne Bersten des Behälters

Versagen mit potentielltem Bersten - ein durch Fehlergröße und/oder Rißwachstumsrate charakterisierter, durch geeignete Maßnahmen zu behebender Zustand, deren Unterlassung zum Bersten des Behälters führen kann. Geeignete Maßnahmen sind Reparatur, Herabsetzung der Beanspruchung durch Veränderung der Betriebsbedingungen oder Außerbetriebnahme des Behälters (potentially disruptive vessel failure).

Nichtkritisches Behälterversagen - eine lokale Beeinträchtigung der drucktragenden Umschließung des Behälters, einschließlich der Stutzen und Verschraubungen durch örtlich begrenzte Rißbildung oder andere Fehler mit oder ohne geringfügige Leckage, die jedoch kein kritisches Ausmaß erreichen und nicht zum Bersten des Behälters führen kann (non-critical vessel failure).

Die in diesem Kapitel festzulegende Versagenshäufigkeit des Reaktordruckbehälters soll nur für solche Versagensarten gelten, deren Ursache in den Bereichen Auslegung, Konstruktion, Werkstoff und Verarbeitung zu suchen ist, also in den Bauteilen selber liegt (einschließlich falscher Dimensionierung und falscher Werkstoffwahl). Das Verhalten des Reaktordruckbehälters bei extremen Betriebsbelastungen, z.B. Versagen der Überdrucksicherung, oder bei hypothetischen Störfällen, z.B. Dampfexplosion, wird in der Risikostudie an anderer Stelle bewertet und braucht von der hier aufzustellenden Versagenshäufigkeit nicht abgedeckt zu werden. Deshalb wurden bei der Bewertung in der Schadensstatistik für nichtnukleare Druckbehälter auch nur solche Schäden berücksichtigt, bei denen die Ursachen der hier gestellten Zielsetzung entsprachen /F3, 4-1/.

Als relevant im Sinne eines Risikos sind die Zerkmale gemäß der vorn getroffenen Definition anzusehen. Im untersuchten Zeitraum

sind bei den nichtnuklearen Druckbehältern 40 solcher Zerknalle eingetreten, die bei der Bestimmung der Versagenshäufigkeit zu berücksichtigen waren. Der zugehörige mittlere Bestand an Behältern betrug 363 525 Stück, die zugehörige Anzahl der Behälterbetriebsjahre  $6,5 \cdot 10^6$ . Damit ergab sich bei einem Vertrauensbereich von 99 % eine Häufigkeit für den Zerknall von  $0,88 \cdot 10^{-5} \text{ a}^{-1}$ . Ein besonders interessantes Ergebnis daraus ist, daß sich die Häufigkeit für einen Zerknall in der Zeit von 1959 bis 1976 um mehr als eine Größenordnung vermindert hat.

Ein genauerer Vergleich läßt erkennen, daß die mit den nichtnuklearen Druckbehältern gewonnene Versagenshäufigkeit nicht unmittelbar auf den Reaktordruckbehälter übertragbar ist. Die Gründe dafür sind:

Es bestehen erhebliche Unterschiede zwischen den Merkmalen der "konventionellen" Behälter und des Reaktordruckbehälters. Dies zeigt eine im Rahmen der Statistik durchgeführte Stichprobenauswertung für den Bereich des TÜV Rheinland /F3, 4-1/. Es ergibt sich, daß die erfaßten Behälter zu 95 % eine Wanddicke unter 20 mm aufweisen (RDB: 243 mm), daß der Außendurchmesser zu 95 % unter 2500 mm liegt (RDB: 5500 mm), daß die gespeicherte Energie zu 95 % eine Größenordnung geringer ist als beim Reaktordruckbehälter und daß die Nennspannung zu 85 % nur  $100 \text{ N/mm}^2$  und zu 50 % gar nur  $70 \text{ N/mm}^2$  beträgt (RDB:  $180 \text{ N/mm}^2$ ).

Es bestehen Unterschiede zwischen "konventionellen" Behältern und dem Reaktordruckbehälter bei Auslegung und Konstruktion sowie den sonstigen für die Qualität maßgebenden Einflußgrößen samt den zugehörigen Überwachungs- und Prüfungsmaßnahmen /F3, 4-2 und -3/. Dies sind im wesentlichen:

- vollständige Lasterfassung aus allen als noch realistisch anzunehmenden Betriebs- und Störfällen einschließlich seltener Extremzustände,
- vollständige Spannungsanalyse unter Zugrundelegung der vorgenannten Lasten,
- optimale Konstruktion,
- Reinheit des Werkstoffes,

- Zähigkeit des Werkstoffes,
- Verarbeitungsunempfindlichkeit des Werkstoffes,
- Überwachung der Schweißarbeiten,
- Überwachung der Wärmebehandlung,
- mehrfach unabhängige Ultraschallprüfung der Schweißnähte nach den Wärmebehandlungen und nach der Erstdruckprüfung,
- wiederkehrende zerstörungsfreie Prüfung im Betrieb,
- Überwachung des Langzeitverhaltens durch Einhängeprouben.

Eine fachliche Bewertung dieser Unterschiede führt zu dem Schluß, daß durch die in der Nukleartechnik üblichen Anforderungen die Qualität eines Reaktordruckbehälters gegenüber einem "konventionellen" Behälter wesentlich höher ist. Die sich aus der Schadensstatistik für nichtnukleare Druckbehälter ergebende Versagenshäufigkeit ist für den Reaktordruckbehälter nur sehr bedingt aussagefähig und beschreibt zunächst die erreichte Zuverlässigkeit der "konventionellen" Druckbehältertechnik.

#### 4.2 Qualitätssicherung beim Reaktordruckbehälter

Im folgenden werden kurz die wichtigsten Maßnahmen beschrieben, durch die die hohe Qualität des Reaktordruckbehälters erreicht wird:

##### ● Auslegung und Konstruktion

Sämtliche im Betrieb zu erwartenden Belastungen werden im Rahmen einer Spannungsanalyse hinsichtlich ihrer Wirkung auf den Reaktordruckbehälter untersucht. Das Ergebnis ist die genaue Kenntnis der auftretenden Spannungen, die unter Berücksichtigung der Lastart und des Werkstoffverhaltens begrenzt werden. Darüber hinaus wird die konstruktive Ausbildung so ausgeführt, daß der Reaktordruckbehälter eine spannungsgerechte Gestalt aufweist.

Die zulässige primäre Membranspannung im Reaktordruckbehälter beträgt etwa  $180 \text{ N/mm}^2$  und ist damit höher als die überwiegend in den nichtnuklearen Behältern herrschende Spannung, wie sie



sich aus einer Stichprobenerhebung im Rahmen der erwähnten Schadensstatistik ergab. Mit der Absicherung durch den Faktor 3 gegen die Zugfestigkeit bei Raumtemperatur ( $568 \text{ N/mm}^2$ ) sowie durch die detaillierte Spannungsanalyse ist jedoch die dem Werkstoff angemessene Belastbarkeit nicht in Frage gestellt. Weiterhin wirkt sich die optimierte Konstruktion günstig aus, durch die folgende Bedingungen erfüllt werden:

- keine Wanddurchbrüche unterhalb des Behälterflansches,
- übermäßig verstärkter Behälterflansch mit aufgesetzten Stützen,
- besonders verstärkter Deckel im Bereich der Steuerstabdurchführungen,
- keine Längsschweißnähte durch Verwendung nahtloser Schmiederinge,
- Beschränkung der Strahlenbelastung der Behälterwand durch einen ausreichend großen Wasserspalt.

Auslegung und Konstruktion des Reaktordruckbehälters werden vom unabhängigen Sachverständigen durch eigene Analysen nachgerechnet und überprüft.

#### ● Werkstoffwahl

Als Grundwerkstoff des Reaktordruckbehälters für die Referenzanlage wurde der Werkstoff 22 NiMoCr 37 gewählt. Die Eigenschaften dieses Werkstoffes sind durch eine Vielzahl von geprüften Bauteilen bekannt und statistisch abgesichert. Chemische Analyse, Erschmelzung, Verarbeitung und Wärmebehandlung wurden so aufeinander abgestimmt, daß die festgelegten Mindestwerte für Festigkeit und Zähigkeit an keiner Stelle unzulässig unterschritten werden, auch nicht im Schweißgut und in der Wärmeeinflußzone, und daß diese Werte über die Wanddicke und das gesamte Volumen nicht unzulässig schwanken. Dies wurde durch umfangreiche zerstörende Werkstoffprüfungen nachgewiesen. Durch zerstörungsfreie Prüfungen wurde sichergestellt, daß herstellungsbedingte Fehlerstellen weit unterhalb sicherheitstechnisch bedeutsamer Grenzen liegen.

Die erreichte integrale Zähigkeit und der nachweislich begrenzte Fehlerzustand gewährleisten eine ausreichende Widerstandsfähigkeit gegenüber den zu erwartenden Belastungen, auch wenn im Hinblick auf Grundwerkstoff und Wärmeeinflußzone noch kein ausgesprochen optimierter Stahl vorliegt. Für eine Kurzzeitbetrachtung im Hinblick auf die erste Betriebsphase von etwa 10 bis 20 Jahren ergibt sich somit keine Einschränkung für die Sicherheit gegenüber katastrophalem Versagen. Auch für eine zweite Betriebsphase von etwa weiteren 20 Jahren ist nach dem heutigen Kenntnisstand eine unzulässige Verringerung des Sicherheitsabstandes nicht zu erwarten. Eine letzte Bestätigung hierfür muß aus dem ständig weiterentwickelten Stand von Wissenschaft und Technik zum jeweiligen Beurteilungszeitpunkt hervorgehen. Die Sicherstellung eines ausreichenden Kenntnisstandes wiederum wird durch Verwertung von Betriebserfahrungen und konsequenter Fortsetzung der Anstrengungen in Forschung und Entwicklung erreicht. Für die Schrauben der Deckelverbindung gelten im Prinzip die gleichen Qualitätsanforderungen wie für die Behälterschale.

#### ● Fertigung

Die für das Bauteilverhalten wesentlichen Arbeitsgänge, das Schweißen und die Wärmebehandlung, wurden während der Durchführung laufend überwacht und durch den unabhängigen Sachverständigen stichprobenweise kontrolliert. Durch simuliert behandelte und durch bei der Fertigung mitlaufende Bauteilproben wurde nachgewiesen, daß die erforderlichen Eigenschaften des Werkstoffes auch nach der Verarbeitung vorhanden waren und die Fertigung einwandfrei erfolgte.

Bei dem für den Reaktordruckbehälter des Kernkraftwerkes Biblis, Block B, vorliegenden Werkstoff sind Mikro- und Millimeterrißbildungen im grobkörnig verbliebenen Überhitzungsbereich der Wärmeeinflußzone nicht auszuschließen. Infolge der Viellagenschweißtechnik ist die Ausdehnung dieser Rißbildungen jedoch begrenzt, so daß bei den umfangreichen mechanisch-technologischen Prüfungen keine Beeinträchtigung der Widerstandsfähigkeit nach-

gewiesen werden konnte. Für die erste Betriebsphase ist daher keine Einschränkung der Sicherheitsaussage notwendig. Im übrigen gilt für die spätere Betriebsphase die gleiche Aussage, wie sie bereits weiter oben zum Werkstoff gemacht wurde.

- Bauprüfung und Erstdruckprüfung

Während der Fertigung wurde die Qualität laufend durch zerstörungsfreie Prüfverfahren überprüft. Hierzu wurde insbesondere die Ultraschallprüfung eingesetzt. Diese wurde an den Schweißnähten unmittelbar nach den Zwischenwärmebehandlungen, nach der Endwärmebehandlung und nach der Erstdruckprüfung unabhängig voneinander vom Hersteller, Systemlieferer und Sachverständigen durchgeführt. Durch diese Mehrfachprüfung können Veränderungen bei der Fertigung verfolgt und menschliches Versagen weitgehend ausgeschlossen werden. Nach dem Zusammenbau des gesamten Druckbehälters wurde er in einer Erstdruckprüfung mit dem 1,3fachen des Berechnungsdruckes belastet. Damit wurde nachgewiesen, daß die den betrieblichen Erfordernissen entsprechende Tragfähigkeit vorhanden ist.

- Wiederkehrende Prüfungen im Betrieb

Der Reaktordruckbehälter wird wiederkehrend im Betrieb mittels weitgehend automatisierter Ultraschallprüfung und Druckprüfung hinsichtlich seines Fehlerzustandes überprüft, so daß dieser auch mit fortschreitender Lebensdauer entsprechend den betrieblichen Gegebenheiten unter Kontrolle bleibt.

- Betriebsüberwachung

Im Rahmen des Probetriebes wird das Betriebsverhalten und die Funktion des gesamten Primärkreises getestet. Während des späteren Leistungsbetriebes werden Temperaturen und Drücke sowie die Häufigkeit der verschiedenen Lastzustände überwacht und re-

gistriert. Dadurch ist gewährleistet, daß die Belastung des Reaktordruckbehälters im Betrieb nicht unkontrolliert erfolgt und jederzeit nachprüfbar bleibt.

Durch die Neutronenbestrahlung verändert sich im Bereich des Reaktorkerns die Zähigkeit des Grundwerkstoffes. Um diese Veränderung möglichst gering zu halten, wird die über die Lebensdauer integrierte Neutronenfluenz durch einen ausreichenden Wasserspalt zwischen Kern und Behälterwand auf  $1 \cdot 10^{19} \text{ cm}^{-2}$  begrenzt /F3,4-3/. Durch Einhängenproben - das sind den betrieblichen Bedingungen und der Neutronenbestrahlung ausgesetzte Werkstoffproben, die mit fortschreitendem Betrieb sukzessive entnommen werden - wird die Zähigkeitsänderung überwacht. Damit wird sichergestellt, daß die Zähigkeit auch mit fortschreitender Lebensdauer bekannt ist und eine den betrieblichen Erfordernissen entsprechende Grenze nicht unterschreitet.

#### 4.3 Folgerungen für die Risikostudie

Bei einer zusammenfassenden Bewertung aller Maßnahmen, die zur Ermittlung und Absicherung der Belastungen und zur Erzeugung und zum Nachweis der Qualität durchgeführt werden, ist die Möglichkeit für einen katastrophalen Zerknall des Reaktordruckbehälters aufgrund inhärenter Ursachen nicht zu erkennen. Anforderung und Qualität stehen beim Reaktordruckbehälter in einem solchen Verhältnis, daß ein Versagen durch unzureichende Auslegung, unzureichenden Werkstoff und unsachgemäße Herstellung unter den dargelegten Voraussetzungen praktisch auszuschließen ist.

Für die Unfallannahme "Zerknall des Reaktordruckbehälters" durch eine in der Auslegung, im Werkstoff oder in der Verarbeitung liegende Ursache wird in der Phase A der deutschen Risikostudie eine rechnerische Versagenshäufigkeit von  $1 \cdot 10^{-7}$  pro Reaktordruckbehälter und Jahr angenommen. Diese Zahl ist nach Ansicht maßgebender deutscher Druckbehälterfachleute eine obere Abschätzung. Sie stellt keinen Erwartungswert für das Versagen dar, sondern ist als rein rechnerischer Maximalwert für die Untersu-

chungen in der Risikostudie zu verstehen. Sie gilt für den bestimmungsgemäßen Betrieb. Für Störfälle, bei denen ein höheres Spannungsniveau zulässig ist, wird sich diese Zahl rechnerisch erhöhen. Jedoch sind in Anbetracht der Auslegung des Reaktor-druckbehälters - keine größeren plastischen Verformungen über etwa 0,5 % - und der damit verbundenen konstruktiven, werkstoffmäßigen und prüftechnischen Voraussetzungen im Störfall keine Bedingungen zu erwarten, die für diese Lastfälle ein erhöhtes Risiko zur Folge haben.

Untersuchungen in den USA und Großbritannien haben ergeben, daß auch andere Betrachtungsweisen zu vergleichbaren Resultaten führen. So zeigen in den USA durchgeführte Vergleiche /F3, 4-4/ zwischen nichtnuklearen Druckbehältern und Reaktordruckbehältern, daß die Wahrscheinlichkeit des Aufreißens eines Reaktor-druckbehälters allgemein mindestens eine Größenordnung kleiner ist, und daß die Wahrscheinlichkeit des Aufreißens bis zu Lecks, die vom Notkühlsystem nicht mehr beherrscht werden, noch niedriger ist. In Großbritannien auf der Basis der probabilistischen Bruchmechanik durchgeführte Berechnungen /F3, 4-5/ bestätigen die Aussagen aus den USA. Die Ergebnisse aus USA und Großbritannien können als eine Bestätigung der hier angesetzten Größenordnung der Versagenswahrscheinlichkeit für den Reaktordruckbehälter angesehen werden.

Im Einklang mit dieser Vorgehensweise läßt sich nicht ausschließen, daß bei einem RDB-Bersten Bruchstücke weggeschleudert werden. Durch die Anordnung des Reaktordruckbehälters im Reaktorgebäude ist es jedoch nicht denkbar, daß derartige Bruchstücke die Reaktorsicherheitshülle im Bereich unterhalb der Äquatorlinie erreichen; der biologische Schild aus 3 m dickem Beton sowie weitere Gebäudemauern von über 1 m Dicke sollten dies verhindern. Für nach oben geschleuderte Bruchstücke sind als Hindernisse die ca. 120 cm dicken Betonabdeckriegel des Reaktorraumes und der Reaktorgebäudekran anzusehen, beide von erheblicher Masse. Bei geradliniger Flugbahn müssen nach oben fliegende Bruchstücke Wege von über 35 m zurücklegen, bis sie die Sicherheitshülle erreichen. Kleinere Bruchstücke können zwar am Kran vorbeifliegen,

jedoch ist aufgrund ihrer Masse und des relativ langen Flugweges schwer vorstellbar, daß sie noch die 29 mm dicke Sicherheitshülle durchschlagen. Größere Bruchstücke dürften nur nach Berührung des Kranes, an dem sie dann erheblich an Energie verlieren werden, die Sicherheitshülle erreichen. Für die Phase A der Studie wird deshalb angenommen, daß beim Bersten des Reaktordruckbehälters die Sicherheitshülle intakt bleibt. Diese Annahme sollte im Rahmen zukünftiger Arbeiten über die möglichen Bruchformen beim Bersten des Reaktordruckbehälters sowie über die Wirkung der gebäudlichen Bedingungen auf weggeschleuderte Bruchstücke weiter abgesichert werden.

## 5. ZUVERLÄSSIGKEITSKENNGRÖSSEN

### 5.1 Allgemeines

Für die Durchführung der Fehlerbaumanalysen sind die folgenden Angaben von Bedeutung:

- Wahrscheinlichkeiten, daß Komponenten bei Anforderung als ausgefallen entdeckt werden bzw. in bestimmten Zeitintervallen ausfallen,
- Instandsetzungs- und Wartungszeiten, die Einfluß auf die Verfügbarkeit von Systemen haben,
- Intervalle für Prüfungen, bei denen bis dahin nicht bemerkte Fehler entdeckt werden.

Auf den letzten Punkt braucht hier nicht eingegangen zu werden, weil die Prüfintervalle für die Referenzanlage festgelegt sind, so daß keine besonderen Ermittlungen erforderlich sind (Fachband 2). Zur Nichtverfügbarkeit von Systemen aufgrund von Instandsetzung und Wartung werden lediglich einige Angaben aus der Auswertung von Betriebserfahrungen deutscher Kernkraftwerke gemacht, Literaturangaben zu diesem Thema sind relativ spärlich.

Dies ist auch darin begründet, daß die Instandsetzungszeiten weit geringeren Einfluß auf die Ergebnisse der Fehlerbaumanalysen haben als die Ausfallwahrscheinlichkeiten der Komponenten. Die wesentlichen Gründe dafür sind, daß zum einen die Instandsetzungszeiten in der Regel kürzer sind als die mittlere Zeit, in der ein Fehler in einem "stand by"-System unentdeckt bleibt, und daß zum anderen administrative Beschränkungen der Instandsetzungsarbeiten festgelegt sind. So ist gleichzeitige Instandsetzung redundanter Stränge von Sicherheitssystemen bei einem Leistungsbetrieb nicht zulässig. Für Instandsetzungsarbeiten an einzelnen Strängen existieren maximal zulässige Reparaturzeiten. Für die Durchführung der Fehlerbaumanalysen genügt daher eine relativ pauschale Art der Berücksichtigung der Instandsetzung (Fachband 2).

Im folgenden sind damit in erster Linie die Ausfallwahrscheinlichkeiten von Komponenten zu diskutieren. Die Betrachtung beschränkt sich dabei an dieser Stelle auf unabhängige Ausfälle. Allgemeine Ausführungen zu "common mode"-Ausfällen und Ausfällen aufgrund menschlichen Fehlverhaltens finden sich im Fachband 2. Der vorliegende Band enthält Daten zu "common mode"-Ausfällen einzelner Komponenten.

Die Ausfallwahrscheinlichkeit einer Komponente kann generell mit einer der beiden folgenden Darstellungsweisen beschrieben werden:

- als Ausfallrate  $\lambda$ , definiert als auf die Zeiteinheit bezogene Wahrscheinlichkeit für den Ausfall einer funktionsfähigen Komponente. Diese Darstellungsart ist geeignet, das Ausfallverhalten einer in Betrieb befindlichen Komponente zu beschreiben, ebenso das Ausfallverhalten einer "stand by"-Komponente, wenn diese während des Bereitschaftszustandes ausfällt;
- als Wahrscheinlichkeit  $P$ , daß eine Komponente ihre Funktion bei Anforderung nicht erfüllt. Auf diese Art kann das Ausfallverhalten einer "stand by"-Komponente beschrieben werden.

Welche der beiden Darstellungen für "stand by"-Komponenten zu wählen ist, hängt von der Ausfallart ab. Die zuletzt genannte Darstellungsart entspricht dem realen Ausfallverhalten, wenn das Versagen nicht bereits vorlag und bei der Anforderung lediglich manifest wird, sondern erst bei der Anforderung hervorgerufen wird. Dies kann durch Fehlbedienung oder Überlastung der Fall sein. Überlastung kann nur auftreten, wenn die Komponente für die ihr zuge dachte Funktion nicht ausgelegt ist. Falls Fehlbedienung eine nennenswerte Rolle spielt, ist dies gesondert zu berücksichtigen. Daher ist das Ausfallverhalten von Komponenten in der Studie überwiegend durch Ausfallraten beschrieben. Hervorzuheben ist jedoch, daß die Darstellungsart bedeutungslos ist, wenn das System, für das die Fehlerbaumanalyse erstellt wird, mit dem System, aus dessen Beobachtung die Daten stammen, in den Intervallen zwischen den Anforderungen über-



einstimmt. In diesem Fall führen beide Darstellungsweisen zum selben Ergebnis, daher sind die Ergebnisse der Auswertungen von Betriebserfahrungen deutscher Kernkraftwerke zum Teil als Wahrscheinlichkeiten je Anforderung wiedergegeben. Ausfallraten bzw. -wahrscheinlichkeiten können im allgemeinen Fall Funktionen der Zeit oder der Zahl der Anforderungen sein. In beiden Fällen sind unterschiedliche Phasen des betrieblichen Einsatzes zu unterscheiden.

Zu Anfang des betrieblichen Einsatzes ist die Möglichkeit gegeben, daß Komponenten Fehler, z.B. aus der Fertigung, aufweisen, die bei vorbetrieblichen Qualitätsprüfungen nicht entdeckt wurden. Betrachtet man eine größere Population, dann wirkt sich das so aus, daß einzelne Komponenten nach relativ kurzer Lebensdauer ausfallen. Berechnet man eine mittlere Ausfallrate bzw. -wahrscheinlichkeit, dann erhält man zunächst relativ hohe Werte.

Nach Eliminierung dieser Frühausfälle besteht die betrachtete Population aus Komponenten, deren Eigenschaften der vorgesehenen Betriebsweise entsprechen. In dieser Phase, die den wesentlichen Teil der Komponentenlebensdauer ausmacht, sind Ausfälle selten, d.h. die entsprechenden Ausfallraten bzw. -wahrscheinlichkeiten klein. Da das Ausfallverhalten nicht von einer systematischen Ursache bestimmt wird, ist keine zeitliche Abhängigkeit zu erwarten. Da die Ausfallzeitpunkte zufällig verteilt sind, spricht man von Zufallsausfällen, obwohl natürlich jeder Ausfall auf eine konkrete Ursache zurückzuführen ist.

Besteht die Möglichkeit, daß nach längerer Betriebszeit Verschleißerscheinungen auftreten, die zum Ausfall der Komponente führen, dann sind gleichartige Komponenten von diesem Prozeß nach etwa gleichen Betriebszeiten betroffen; d.h., die Ausfallraten bzw. -wahrscheinlichkeiten steigen nach dieser Zeit steil an. Qualitativ ergibt sich ein Verlauf entsprechend Bild F3, 5-1, die sogenannte Badewannenkurve.

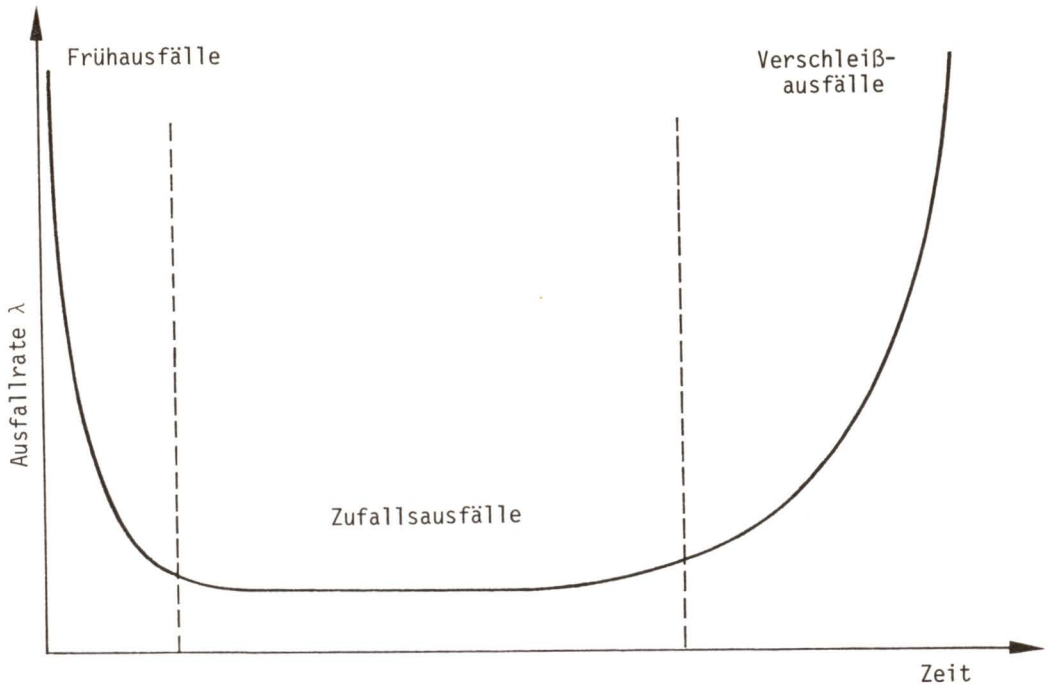


Bild F3, 5-1:

Zeitverhalten der Ausfallrate

Die beschriebene zeitliche Abhängigkeit des Ausfallverhaltens kann für elektronische Komponenten, von denen große Populationen beobachtet wurden, empirisch belegt werden. Für Komponenten mit geringerem Umfang der vorliegenden statistischen Daten ist die Angabe einer zeitlichen Abhängigkeit häufig nicht möglich. Da die beschriebenen Mechanismen, die zu dieser Zeitabhängigkeit führen, jedoch auch bei den meisten anderen Komponenten beobachtet werden, kann auch hierfür ein ähnliches Verhalten unterstellt werden. Insbesondere wird die Verwendung zeitlich konstanter Ausfallraten bzw. -wahrscheinlichkeiten für Komponenten, bei denen keine systematische Ausfallursache vorliegt, dadurch gestützt, daß Ausfälle solcher Komponenten

auf unterschiedliche Ursachen zu zufälligen Zeitpunkten zurückzuführen sind.

Früh- und Verschleißausfälle können durch Anwendung qualitätssichernder Maßnahmen bei Fertigung und Betrieb verringert werden. Diese Möglichkeiten werden in Kernkraftwerken genutzt, so daß davon auszugehen ist, daß diese Ausfallmechanismen eine untergeordnete Rolle spielen. Trotzdem sind sie nicht völlig auszuschließen, d.h., diese Effekte bewirken eine gewisse Unsicherheit der Zuverlässigkeitskenngrößen. Auf weitere Ursachen für Datenunsicherheiten wird im nächsten Abschnitt eingegangen. Um diese Unsicherheiten insgesamt zu berücksichtigen, wurde für die Studie das folgende Vorgehen gewählt:

- Ausfallraten und -wahrscheinlichkeiten werden als zeitlich konstant angesetzt.
- Für die Berechnung der Systemanalyse werden keine mittleren Ausfallraten und -wahrscheinlichkeiten verwendet, sondern Verteilungen, die sämtliche verfügbaren empirischen Daten berücksichtigen. Damit sind Früh- und Verschleißausfälle, die in statistischen Erhebungen auch erfaßt werden, mit abgedeckt.

## 5.2 Literaturdaten und Betriebserfahrungen

Über Zuverlässigkeitskenngrößen existiert eine relativ umfangreiche Literatur. Dies ist eine wesentliche Quelle zur Ermittlung der für die Fehlerbaumanalysen benötigten Daten. Die zweite wichtige Quelle ist die eigene Auswertung von Betriebserfahrungen in Kernkraftwerken. Für elektronische Bauteile wurden außerdem Ausfalleffektanalysen und Laborversuche herangezogen.

Von wenigen Ausnahmen abgesehen, können der Literatur die für die Durchführung der Fehlerbaumanalysen erforderlichen Daten entnommen werden. Trotzdem wird auf die eigene Auswertung hohes Gewicht gelegt, weil die Literaturwerte mit Unsicherheiten

behaftet sind, die ihre Verlässlichkeit zum Teil beträchtlich einschränken.

Zunächst stammt ein großer Teil der Werte nicht aus Beobachtungen in Kernkraftwerken, sondern aus Anwendungen in anderen Industriezweigen. Die Verwendung auch solcher Daten erscheint gerechtfertigt, da die Einsatzbedingungen der Mehrzahl der in den Fehlerbäumen betrachteten Komponenten denen in anderen Industrien entsprechen. Trotzdem bestehen Unterschiede, z.B. im Prüfumfang sowohl von der Inbetriebsetzung als auch während des Betriebs. Erfahrungen aus Kernkraftwerken sind daher wichtig, um die Anwendbarkeit der allgemeinen Literaturdaten zu beurteilen.

Weiterhin sind die in der Literatur verfügbaren Informationen häufig sehr allgemein. Das Ausfallverhalten von Komponenten kann durch eine Reihe von Faktoren beeinflusst werden, z.B. durch die Art des betrieblichen Einsatzes, durch Umgebungsbedingungen, konstruktive Gestaltung, Auslegung, Leistungsgröße, Art der Instandhaltung und anderes mehr. Ebenso sind unterschiedliche Ausfallarten zu berücksichtigen. Diese Faktoren sind in der Literatur häufig nicht genau beschrieben. Unklarheiten können auch bezüglich der Wertung von Ausfallarten bestehen. Je nach dem Zweck einer Erhebung können z.B. alle Vorkommnisse erfaßt werden, die Instandsetzungsmaßnahmen nach sich ziehen, z.B. auch kleinere Leckagen, oder nur Vorkommnisse, die unmittelbar zur Funktionsunfähigkeit der Komponente führen, oder auch nur Schäden, die längere Ausfallzeiten verursachen. Bei manchen Literaturstellen steht auch weniger die Ermittlung von Daten im Vordergrund, sondern mehr ihre Anwendung, so daß die Herkunft der Daten nur kurz abgehandelt wird.

All diese Faktoren bewirken, daß aus der Literatur ermittelte Daten sehr große Streuungen aufweisen. Deren Ursachen können zwar allgemein angegeben werden, jedoch meist nicht quantitativ für den Einzelfall, so daß der sich ergebende Unsicherheitsbereich nicht durch Einzelanalyse der Daten reduziert werden kann. Da in den Ereignisablaufanalysen die Datenunsicherheiten

voll berücksichtigt werden, bedeutet dies zunächst auch entsprechend breite Unsicherheitsbereiche der Ergebnisse.

Das Ziel bei der Ermittlung von Zuverlässigkeitskenngrößen war, die Literaturwerte möglichst weitgehend durch Betriebserfahrungen abzusichern und womöglich zu ersetzen. Dementsprechend wurde ein relativ großer Aufwand für die Auswertung von Betriebserfahrungen getrieben. Diese Arbeiten werden im Kapitel 6 ausführlicher dargestellt. Der Versuch, die Zuverlässigkeitskenngrößen für die Phase A der Studie hauptsächlich von Betriebserfahrungen aus Kernkraftwerken abzuleiten, stößt auf zwei Begrenzungen:

- Die Auswertung von Betriebserfahrungen ist zeitaufwendig. Da für die Durchführung der Analysen Zuverlässigkeitskenngrößen zu einem relativ frühen Zeitpunkt benötigt werden, mußte dann auf verfügbare Literaturwerte zurückgegriffen werden.
- Die Aussagen aus Betriebserfahrungen sind durch den gegebenen Beobachtungsumfang begrenzt. Daraus kann sich zum einen bei Komponenten mit niedriger Ausfallrate, die in geringer Anzahl eingesetzt sind, eine geringe statistische Aussage-sicherheit ergeben. Außerdem besteht bei einer begrenzten Absolutzahl von Komponenten die Möglichkeit, daß nicht alle relevanten Effekte in der Stichprobe auftreten. Beispielsweise ist es unwahrscheinlich, in einer kleinen Stichprobe eine erhöhte Ausfallrate infolge von Fertigungsmängeln zu beobachten. Stützt man sich allein auf diese Beobachtung, kann dies zu einer Unterschätzung der Schwankungsbreite führen, die die Ausfallrate von Komponenten der betrachteten Art hat.

Für die Ermittlung der Zuverlässigkeitskenngrößen wurden daher sowohl Literaturdaten als auch eigene Auswertungen von Betriebserfahrungen verwendet. Das Gewicht, das diesen beiden Datenquellen zukommt, unterscheidet sich dabei von Komponente zu Komponente, je nach Art und Umfang des zur Verfügung stehenden Materials. Ebenso können unterschiedliche Arten des Vorgehens bei der Ermittlung der Zuverlässigkeitskenngrößen zweckmäßig sein.

Eine generelle Unterscheidung wurde zwischen verfahrens- und elektrotechnischen Komponenten einerseits und leittechnischen Komponenten andererseits vorgenommen, weil die verfügbaren Informationen sowohl aus der Literatur als auch aus Betriebserfahrungen für diese beiden Gruppen von Komponenten unterschiedlich sind. So wurden z.B. für die Ermittlung der Zuverlässigkeitskenngrößen leittechnischer Komponenten Ausfalleffektanalysen herangezogen. Das im folgenden Abschnitt dargestellte Vorgehen wurde für verfahrens- und elektrotechnische Komponenten allgemein angewandt, für leittechnische Komponenten nur, soweit die Daten aus Literaturwerten ermittelt wurden. Die Ermittlung der Daten für leittechnische Komponenten wird im Kapitel 8 dargestellt.

### 5.3 Ermittlung der Zuverlässigkeitskenngrößen

Für die Durchführung der Fehlerbaumanalysen werden Zuverlässigkeitskenngrößen zu bestimmten Komponenten und bestimmten Ausfallarten unter bestimmten Betriebsbedingungen benötigt. Wie bereits erwähnt, lassen sich die Daten in einer so weitgehenden Differenzierung im allgemeinen weder aus der Literatur noch aus den Betriebserfahrungen ableiten. Daher wurden die verfahrens- und elektrotechnischen Komponenten, für die Zuverlässigkeitskenngrößen ermittelt wurden, wie in WASH-1400 relativ allgemein definiert (z.B. "Pumpe" statt einer Reihe unterschiedlicher Bauarten von Pumpen). Die verwendeten Komponenten sind aus Tabelle F3, 7-1 ersichtlich. In Einzelfällen, bei denen spezifisch für die betrachteten Komponenten ausreichend Betriebserfahrungen vorlagen, wurden diese verwendet. Ein Beispiel hierfür sind Rückschlagarmaturen im Not- und Nachkühlssystem.

Entsprechend der allgemeinen Definition der Komponenten werden die erforderlichen Zuverlässigkeitskenngrößen auf der Basis von Ausgangsdaten ermittelt, die sich auf unterschiedliche Bauarten, Betriebsbedingungen usw. beziehen. Hieraus folgt eine Streuung der Daten in einem relativ großen Bereich, die durch eine Verteilung zu beschreiben ist. Da es sich bei Zuverlässig-

keitskenngrößen um statistische Größen handelt, ist zwar auch bei genau definierten Komponenten mit einer Streuung der Daten zu rechnen, z.B. aufgrund von zufälligen Einflüssen bei der Fertigung. Diese Unschärfe vergrößert sich jedoch, wenn man unterschiedliche Komponenten zu einer Klasse zusammenfaßt. Dieses Vorgehen läßt daher eine Verteilung erwarten, mit der die Schwankungsbereiche spezieller Komponenten abgedeckt werden, die jedoch eine größere Breite aufweist.

Im folgenden wird zunächst die Ermittlung von Zuverlässigkeitskenngrößen aus Literaturangaben dargestellt. Bei der Festlegung einer Verteilung sind für jede Komponente die beiden folgenden Schritte vorzunehmen:

- Ermittlung einer Stichprobe, d.h. einer Anzahl von Einzelwerten, z.B. für eine Ausfallrate. Die gesuchte Verteilung soll die Streuung der Angaben, die sich zu einer Komponente in der Literatur finden, wiedergeben. Daher wird jede Ausfallrate, die in einer Literaturstelle für die betrachtete Komponente genannt wird, als Stichprobenwert der zu bestimmenden Verteilung aufgefaßt.
- Schätzung einer Verteilung aufgrund dieser Stichprobe. Hierbei hat die Ermittlung der Einzelwerte größeren Einfluß auf das Ergebnis. Von Bedeutung sind insbesondere die Festlegung eines Zahlenwertes, der aus einer Literaturangabe z.B. für eine Ausfallrate abzuleiten ist, und die Festlegung relativer Gewichte für die verschiedenen Einzelwerte.

Bei der Festlegung des Zahlenwertes sind unterschiedliche Gesichtspunkte zu berücksichtigen. Zum einen können die Komponenten, auf die sich eine Literaturangabe bezieht, technisch von den in den Zuverlässigkeitsanalysen betrachteten Komponenten abweichen. Diese Abweichung läßt sich durch eine Korrektur der in der Literaturstelle angegebenen Ausfallrate aufgrund ingenieurmäßiger Beurteilung berücksichtigen. Auf eine solche Korrektur der Ausgangsdaten wurde aus mehreren Gründen verzichtet. Zunächst gehen die für eine solche Beurteilung erforderlichen Informationen in vielen Fällen aus der Literatur nicht klar genug hervor. Weiter ist eine solche Bewertung selbst mit Un-

sicherheiten behaftet. Zwar ist häufig plausibel, in welche Richtung ein Parameter eine Ausfallrate beeinflussen kann, eine Quantifizierung jedoch ist schwierig. Die unvermeidliche Subjektivität einer solchen Beurteilung würde daher die Nachvollziehbarkeit der Festlegung der Zuverlässigkeitskenngrößen beeinträchtigen. Eine Ausnahme stellen in dieser Hinsicht leittechnische Komponenten dar. Hier existieren belegbare Korrekturfaktoren für Belastung und ähnliche Parameter.

Bei der Festlegung der einzelnen Zahlenwerte ist weiter die Zuordnung von Ausfallraten zu Ausfallarten zu betrachten. Zum Beispiel geben manche Literaturstellen die Häufigkeit von Ausfällen von Armaturen an, ohne danach zu differenzieren, ob die Armatur nicht öffnet oder nicht schließt. Solche Summenausfallraten wurden auf die für die Fehlerbaumanalyse interessierenden Ausfallarten in dem Verhältnis aufgeteilt, das sich aus anderen Quellen mit differenzierteren Angaben ergibt.

Die Einzelwerte aus verschiedenen Literaturstellen können außer durch eine Änderung des Zahlenwertes auch durch die Zuordnung unterschiedlicher Gewichte bewertet werden. Das Gewicht eines Einzelwertes wäre um so höher anzusetzen, je besser die Vergleichbarkeit der in der Literaturstelle behandelten Komponenten mit den in den Fehlerbaumanalysen zu betrachtenden Komponenten ist. Hierbei treten die gleichen Schwierigkeiten auf, wie sie oben im Zusammenhang mit einer Korrektur der Zahlenwerte diskutiert wurden. Aus den gleichen Gründen wurde daher auch auf eine unterschiedliche Gewichtung der Einzelwerte verzichtet.

Ein weiteres mögliches Kriterium für unterschiedliche Gewichte kann auch der unterschiedliche Beobachtungsumfang sein, der den Literaturangaben zugrunde liegt. Da statistische Unsicherheiten jedoch weniger ins Gewicht fallen als Abweichungen aufgrund technischer Unterschiede, wurde z.B. aus unterschiedlichen Beobachtungszeiten kein unterschiedliches Gewicht der Einzelwerte abgeleitet. Soweit einzelne Literaturstellen Angaben zu



verschiedenen Populationen einer Komponentenklasse enthalten, werden daraus mehrere Einzelwerte gebildet.

Zusammenfassend ist zur Festlegung der einzelnen Zahlenwerte aus der Literatur festzustellen, daß sie bis auf die Aufteilung von Summenausfallraten auf Ausfallarten unverändert übernommen und mit gleichem Gewicht in den Verteilungen berücksichtigt wurden. Dieses Verfahren führt zu breiteren Verteilungen als bei Veränderung der Zahlenwerte oder Gewichte aufgrund einer technischen Beurteilung. Die zusätzliche Einführung eines Expertenurteils würde zu einer Betonung des durch diese Beurteilung bevorzugten Bereiches führen. Es ist anzumerken, daß die Einführung einer Expertenbeurteilung durchaus zu einer realistischeren Festlegung einzelner Zuverlässigkeitskenngrößen führen kann. Jedoch ist dies häufig objektiv nicht ausreichend belegbar. Angesichts der vorhandenen Datenunsicherheit erscheint es daher angemessen, eine gewisse Konservativität in Kauf zu nehmen und das Schwergewicht auf die eindeutige Nachvollziehbarkeit zu legen. Zu berücksichtigen ist ferner, daß ein zutreffendes Expertenurteil sich im wesentlichen auf Betriebserfahrungen stützen muß. Da solche Erfahrungen für die Studie ausgewertet wurden und weiter ausgewertet werden, ist es zweckmäßiger, die realen Betriebserfahrungen über die Ergebnisse dieser Auswertungen einzubringen als über eine Expertenbeurteilung von Literaturwerten. Auch die Durchführung der Risikostudie in zwei Phasen legt ein solches Vorgehen nahe.

Anhang 1 gibt die verwendeten Literaturstellen und die daraus für die einzelnen Komponenten entnommenen Zahlenwerte wieder. Die einzelnen Zahlenwerte sind mit ganz wenigen Ausnahmen statistisch voneinander unabhängig. Mehrfachwertungen, die dadurch entstehen können, daß sich mehrere Autoren letztlich auf dieselbe Primärinformation beziehen, wurden durch Rückverfolgung der Zitate eliminiert. Soweit in den Literaturstellen eine Rate ohne Unterscheidung nach Ausfallarten angegeben ist, wird im Anhang 1 für mehrere Ausfallarten nur ein Zahlenwert angegeben, wie im folgenden Beispiel:

Komponente	Ausfallart	(MI - 60 - 54) Ausfallrate, 1/h
Rückschlag- armatur	öffnet nicht	$5 \cdot 10^{-6}$
	schließt nicht	

Bei den Anmerkungen zu den einzelnen Komponenten in Kapitel 7 ist erläutert, wie diese Ausfallraten auf die unterschiedlichen Ausfallarten bezogen wurden. Tabelle F3, A1-2 gibt schließlich die für die Festlegung der Zuverlässigkeitskenngrößen verwendeten Einzelwerte aus der Literatur wieder, wie in folgendem Beispiel:

Komponente	Ausfallart	(MI - 60 - 54) Ausfallrate, 1/h
Rückschlag- armatur	öffnet nicht	$1,8 \cdot 10^{-6}$
	schließt nicht	$3,2 \cdot 10^{-6}$

Die Werte in Tabelle F3, A1-2 stellen zusammen mit den Ergebnissen der Auswertung der Betriebserfahrungen die Basis für die Zuverlässigkeitskenngrößen dar, die für die Fehlerbaumanalysen in der Phase A der Studie verwendet wurden. Die Art der Zusammenfassung von Literaturdaten und Betriebserfahrungen unterscheidet sich dabei je nach dem Material, das für die einzelnen Komponenten für die Festlegung der Zuverlässigkeitskenngrößen vorlag. Einzelheiten sind in Kapitel 7 zu den einzelnen Komponenten angegeben, allgemein sind folgende Fälle zu unterscheiden:

- Die Daten basieren allein auf Betriebserfahrung. Die vorliegenden Erfahrungswerte müssen hierfür aussagekräftiger sein als die verfügbaren Literaturangaben. Diese werden in solchen Fällen nur zum Vergleich angegeben. Beispiel: Diesel.

- Für eine allgemeine Komponentenklasse werden die Daten aufgrund von Literaturangaben festgelegt. Für eine spezielle Unterpopulation, für die ausreichend Erfahrungen vorliegen, wird die Ausfallrate aufgrund der Erfahrungswerte bestimmt. Beispiel: Rückschlagarmaturen großer Nennweiten im Not- und Nachkühlssystem.
- Es werden sowohl Literaturangaben als auch Erfahrungswerte gemeinsam zur Ermittlung der Ausfallrate herangezogen. In diesem Fall werden aus der Betriebserfahrung für abgrenzbare Unterpopulationen Einzelwerte abgeleitet, die im weiteren wie die Einzelwerte aus der Literatur behandelt werden. Beispiel: Handarmaturen.
- Die Daten werden allein auf der Basis von Literaturangaben bestimmt. Häufig liegen für solche Komponenten umfangreiche Betriebserfahrungen vor, die jedoch erst nach der Fixierung der Datenbasis für die Phase A der Studie verfügbar waren. Diese zwischenzeitlich ermittelten Ergebnisse werden zum Vergleich mit angegeben. Beispiel: Pumpen.

Die Einzelwerte aus Literatur und Betriebserfahrung spannen einen Bereich auf, in dem sich die zu beschreibende Zuverlässigkeitskenngröße bewegen kann. Sie werden im folgenden als Stichprobe einer Verteilung aufgefaßt, die angibt, mit welcher Wahrscheinlichkeit zu erwarten ist, daß die betrachtete Zuverlässigkeitskenngröße einen gewissen Wert annimmt.

Die spezielle Wahl der Art der Verteilung ist nicht ausschlaggebend, solange sie die Stichprobe ausreichend gut wiedergibt. Dies ist der Fall bei der logarithmischen Normalverteilung, die zur Beschreibung der Verteilung der Zuverlässigkeitskenngrößen gewählt wurde:

- Sie läßt nur Werte  $> 0$  zu, wie dies für Ausfallraten und -wahrscheinlichkeiten zu fordern ist.<sup>1)</sup>

---

<sup>1)</sup> Die logarithmische Normalverteilung wurde aus Gründen der einfachen Handhabung auch für Ausfallwahrscheinlichkeiten verwendet, obwohl diese natürlich nur Werte  $\leq 1$  annehmen können. Numerisch ist dies in allen auftretenden Fällen bedeutungslos. Für die Rechnungen wurden Werte  $\geq 1$  gleich 1 gesetzt.

- Die Bilder F3, A1-1 bis -18, in denen die Einzelwerte und die ermittelten Verteilungen eingezeichnet sind, zeigen, daß sich die Verteilungen den Stichproben gut anpassen. Eine Erläuterung dieser Bilder wird weiter unten gegeben.

Die Dichtefunktion einer logarithmischen Normalverteilung für X läßt sich z.B. so schreiben:

$$f(x) = \frac{1}{\sqrt{2\pi} s \cdot x} e^{-\frac{(\ln x - \mu)^2}{2s^2}} \quad (\text{für } x > 0)$$

$\mu$  und  $s^2$  sind dabei Mittelwert und Streuung einer Normalverteilung, der  $Y = \ln X$  gehorchen soll. Die folgenden Eigenschaften der logarithmischen Normalverteilung werden im weiteren benutzt:

$x_{50}$  sei der Median, d.h. der Wert, bei dem die Wahrscheinlichkeit von Werten über und unter  $x_{50}$  jeweils 50 % beträgt. Damit ist:

$$x_{50} = e^{\mu}$$

Für den Erwartungswert  $\bar{x}$  gilt:

$$\bar{x} = x_{50} \cdot e^{s^2/2} = e^{\mu + s^2/2}$$

$x_p$  sei die p-%-Fraktile, d.h., es existiere eine Wahrscheinlichkeit von p % für Werte  $\leq x_p$ . Dann besteht die folgende Symmetrie:

$$\frac{x_p}{x_{50}} = \frac{x_{50}}{x_{1-p}} = e^{u_p \cdot s}$$

Dabei ist  $u_p$  die  $x_p$  entsprechende Fraktile der Standardnormalverteilung.

Eine logarithmische Normalverteilung ist durch die Angabe von zwei Parametern bestimmt. Hier werden verwendet:

- Median  $x_{50} = e^{\mu}$

$$\begin{aligned} - \text{ Streufaktor } K_{95}^{1)} &= \frac{x_{95}}{x_{50}} \\ &= e^{1,645 \cdot s} \end{aligned}$$

Wegen der angegebenen Symmetrieeigenschaft ist die Wahrscheinlichkeit für Werte im Bereich  $(x_{50}/K_{95}, x_{50} \cdot K_{95})$  gleich 90 % und jeweils 5 % für Werte darüber und darunter.

Die Verteilung wird aus den  $n$  Einzelwerten  $x_1$  bis  $x_n$  durch Schätzung der Parameter  $\mu$  und  $s^2$  mittels folgenden "maximum-likelihood"-Schätzfunktionen bestimmt:

$$\begin{aligned} \mu &= \frac{1}{n} \sum_{i=1}^n \ln x_i \\ s^2 &= \frac{1}{n} \sum_{i=1}^n (\ln x_i - \mu)^2 \end{aligned}$$

Median und Streufaktor der geschätzten Verteilungen werden jeweils auf die nächste ganze Zahl gerundet, außer wenn die erste geltende Ziffer 1 oder 2 ist.

Die Geraden in den Bildern F3, A1-1 bis -18 stellen die Verteilungsfunktionen der so ermittelten Verteilungen dar. Zwischen der Verteilungsfunktion  $F(x)$  und der Dichtefunktion  $f(x)$  besteht der Zusammenhang

$$F(x) = \int_0^x f(x) dx$$

Die Teilung der Achsen ist so gewählt, daß sich eine logarithmische Normalverteilung als Gerade darstellt. Die Einzelwerte werden an den Punkten  $(x_i, \frac{i - 1/2}{n} \cdot 100 \%)$  eingetragen, wobei  $i$  in der Reihenfolge aufsteigender Werte gezählt wird.

---

<sup>1)</sup>  $K_{95}$  wird im Fachband 2 vereinfacht mit  $K$  bezeichnet.

In Tabelle F3, 7-1 sind Median und Streufaktor der Verteilungen angegeben, die für die einzelnen Komponenten in den Fehlerbaumanalysen benutzt wurden. Die Ausgangsdaten und das Vorgehen bei der Festlegung der Verteilung sind den Tabellen F3, A1-1 und -2 sowie den Anmerkungen zu den einzelnen Komponenten in Kapitel 7 zu entnehmen.

## 6. AUSWERTUNG VON BETRIEBSERFAHRUNGEN IN DEUTSCHEN KERNKRAFTWERKEN

### 6.1 Aufgabenstellung

Wesentliches Ziel der Auswertung von Betriebserfahrungen für die Phase A der Studie war die Bereitstellung von Zuverlässigkeitskenngrößen. Da diese Größen zur Beurteilung von Literaturdaten herangezogen werden, ist an sie die Forderung zu stellen, daß sie spezifische Unsicherheiten, wie sie in Kapitel 5 für Literaturdaten diskutiert wurden, nicht aufweisen. Das bedeutet:

- Die betrachteten Komponenten und Systeme müssen mit den in den Fehlerbaumanalysen untersuchten ausreichend vergleichbar sein.
- Die Auswertung muß darauf angelegt sein, Ergebnisse zu liefern, die entsprechenden Größen der Fehlerbaumanalyse - entweder Eingangsgrößen oder Zwischengrößen - eindeutig zuzuordnen sind.

Diese Forderungen lassen sich am besten durch eigene Auswertungen von Betriebsunterlagen in Kernkraftwerken erfüllen. Für die Auswertungen wurden die Systeme gewählt, die in den Fehlerbaumanalysen eine wesentliche Rolle spielen, d.h. die wichtigen Sicherheitssysteme.

Schwerpunkt der Arbeiten war die Ermittlung von Ausfallraten und Ausfallwahrscheinlichkeiten für Komponenten. Vergleichbare Komponenten sind in relativ großer Anzahl im Einsatz, daher ist hierfür ein ausreichender Beobachtungsumfang verfügbar. Entsprechende Größen wurden auch für größere Systemteile bis hin zu Teilsträngen von redundanten Systemen ermittelt. Solche Aussagen sind wertvoll, weil sie einen Vergleich mit wichtigen Teilergebnissen der Fehlerbaumanalysen zulassen. Wegen der geringeren Anzahl der beobachteten Einheiten erhält man jedoch eine vergleichsweise geringe statistische Aussagesicherheit.

In geringerem Umfang wurden auch Instandsetzungszeiten von Betriebsmitteln und Nichtverfügbarkeiten von Systemen infolge In-

standhaltung ermittelt. Neben den im Vordergrund stehenden quantitativen Ergebnissen liefern die Auswertungen auch qualitative Erkenntnisse über auftretende Ausfallarten, die zur Absicherung der Fehlerbaumanalysen verwendet werden.

## 6.2 Vorgehen

Die Auswertungen wurden in den Kernkraftwerken Biblis und Stade durchgeführt. In Biblis konzentrierten sich die Arbeiten auf den Block A, weil in Block B (Referenzanlage) ein gesondertes Vorhaben zur Ermittlung von Zuverlässigkeitskenngrößen durchgeführt wird, bei dem zur Berücksichtigung unterschiedlicher Einflußgrößen eine Vielzahl von Auslegungs- und Betriebsdaten der betrachteten Komponenten erfaßt und in einer Datenbank gespeichert wird. Ergebnisse aus diesem längerfristig angelegten Vorhaben werden für die Phase B der Studie zur Verfügung stehen. Der Beobachtungszeitraum, der für die Auswertungen zugrunde gelegt wurde, umfaßt insgesamt ca. 9 Reaktorbetriebsjahre.

In den beiden Kernkraftwerken stehen für die Auswertungen im wesentlichen die gleichen Unterlagen zur Verfügung. Wegen der in Einzelheiten unterschiedlichen Betriebsorganisation sind auch die Dokumentationsverfahren und die Bezeichnungen der Unterlagen etwas unterschiedlich. Soweit zur Illustration im folgenden darauf eingegangen wird, findet die Terminologie von Biblis Verwendung.

Neben technischen Unterlagen zur Beschreibung der Komponenten und Systeme und ihrer Betriebsweise wurden zur Ermittlung der Zuverlässigkeitskenngrößen in erster Linie die folgenden Unterlagen herangezogen:

- **Protokolle der wiederkehrenden Prüfungen**

Für die Sicherheitssysteme sind Funktionsprüfungen in regelmäßigen Abständen vorgeschrieben. Anhand vorgegebener Prüfanweisungen wird die Funktion einer Reihe von Komponenten überprüft. Der Ablauf der Prüfung und insbesondere Abweichungen vom geforderten Ablauf werden im Prüfprotokoll festgehalten.



• Dokumentation der Instandhaltungsarbeiten (Arbeitsaufträge)

Der Arbeitsauftrag ist die wichtigste Unterlage zur organisatorischen Abwicklung der Instandhaltungsarbeiten. Er dient der Initiierung von Instandhaltungsarbeiten, der Kontrolle ihres Ablaufs und der kostenmäßigen Abrechnung. Für den vorliegenden Zweck ist von Bedeutung, daß er die auftretenden Schäden und die zur Instandsetzung durchgeführten Arbeiten wiedergibt. Darüber hinaus lassen sich daraus die Dauer der Instandsetzung und Nichtverfügbarkeit der betroffenen Komponenten oder Systeme entnehmen.

Zur Unterstützung der Auswertung wurden weitere Unterlagen wie Schichtbücher, Freischaltbücher etc. herangezogen. Eine wichtige Hilfe waren zusätzliche Erläuterungen, die auf der Basis dieser Unterlagen bei den zuständigen Fachabteilungen der Kraftwerke eingeholt wurden.

#### 6.2.1 Wiederkehrende Prüfungen

Die wiederkehrenden Prüfungen werden nach schriftlichen Prüfanweisungen durchgeführt. Darin sind in Prüfschritten die vorzunehmenden Betätigungen und die geforderten Rückmeldungen des Systems festgehalten. Zusätzlich zum Prüfprotokoll wird ein Ausdruck des Prozeßrechners erstellt (Prüfungsstörablaufprotokoll), der eine Reihe von Binärsignalen (z.B. Armaturenstellungen) und Analogmeßwerten enthält. Geprüft wird jeweils die Reaktion des Systems auf die Reaktorschutzsignale, die das System im Störfall anregen. Der Prüfumfang umfaßt damit:

- Einspeisung des Signals in die elektronische Steuerung des Systems,
- Bildung der Steuersignale für die Ansteuerung der elektrischen Abzweige unter Berücksichtigung von Verriegelungsbedingungen und Aggregateschutzsignalen,
- Einschaltung oder Betätigung der jeweils angeforderten verfahrenstechnischen Aggregate,
- Rückmeldung der Funktion der Aggregate,
- Anzeige von Meßwerten über die Funktion des Systemteilstranges.

Nicht eingeschlossen ist die Prüfung von Aggregaten, bei deren Betätigung der Kraftwerksnormalbetrieb gestört wird, und die Bildung der Reaktorschutzsignale. Diese Funktionen werden gesonderten Prüfungen unterzogen.

Die Prüfung untergliedert sich in drei Teile:

- Prüfvorbereitung,
- Systemprüfung,
- Prüfrücksetzung.

Die Prüfvorbereitung dient dazu, das System in einen Zustand zu bringen, in dem alle geforderten Prüfungen durchgeführt werden können. Hierzu werden zunächst eventuell laufende betriebliche Funktionen des Systems unterbrochen. Weiter werden Systemteile abgesperrt, deren Reaktion auf die Systemzustände bei einzelnen Prüfschritten unterbunden werden soll. Beispielsweise werden die Druckspeicher abgesperrt, wenn die Einspeisung aus den Hoch- und Niederdrucksystemen des Notkühlsystems geprüft wird, damit sich die Druckspeicher nicht in die Prüfleitung entleeren. Schließlich werden die zu prüfenden Komponenten in einen dem gewünschten Endzustand entgegengesetzten Schaltzustand versetzt. Soll z.B. das Öffnen einer Armatur geprüft werden, wird sie während der Prüfvorbereitung geschlossen. Für die Mehrzahl der Komponenten ist dies erforderlich, um überhaupt eine Prüfung durchführen zu können, denn die Sicherheitssysteme befinden sich ständig in erhöhter Betriebsbereitschaft. Das bedeutet, Armaturen, die bei Anforderung des Systems im Störfall offen sein sollen, sind auch in der Bereitschaftsstellung offen, soweit dies technisch möglich ist. Sie müssen bei Anforderung nicht verfahren werden. Die Prüfung hat hier den Zweck, nachzuweisen, daß diese Komponenten auch dann ihre Funktion erfüllen, wenn sie sich aus betrieblichen Gründen oder infolge eines Fehlers nicht in der normalen Bereitschaftsstellung befinden.

Bei der eigentlichen Prüfung werden die Systeme durch die Reaktorschutzsignale, die im Störfall anstehen würden, angeregt. Es wird überprüft, ob die Komponenten die geforderte Funktion erfüllen, und das Ergebnis protokolliert. Bei der Prüfrücksetzung werden die Komponenten- und Systemzustände wieder hergestellt, die vor der Prüfung vorhanden waren.

Aus wiederkehrenden Prüfungen lassen sich für die betrachteten Komponenten und Systeme Ausfallwahrscheinlichkeiten bei Anforderung ableiten. Die Protokolle enthalten die dazu benötigten Angaben:

$A_i$ : Anzahl der Anforderungen einer bestimmten Komponenten- und Funktionsart  $i$

$N_i$ : Anzahl der zugehörigen Funktionsversagen

Der Schätzwert für die Ausfallwahrscheinlichkeit ist

$$P_i = \frac{N_i}{A_i}$$

Für die Abschätzung der Ausfallwahrscheinlichkeit bei Anforderung wird dabei unterstellt, daß es sich um einen konstanten Wert handelt, der weder von der Häufigkeit der Anforderungen noch vom zeitlichen Abstand seit der letzten Anforderung abhängt. Dementsprechend werden sämtliche Betätigungen einer Komponente bei der Prüfung für die Ermittlung der Anzahl der Anforderungen herangezogen. Wenn beispielsweise einzelne Komponenten bei einer Prüfung zweimal betätigt werden, was bei einigen Prüfungen der Fall ist, wird dies als zwei Anforderungen gewertet. In solchen Fällen kann das idealisierte Modell einer konstanten Ausfallwahrscheinlichkeit bei Anforderung zu günstige Ergebnisse liefern, weil die Versagenswahrscheinlichkeit einer Komponente, die bei derselben Prüfung bereits einmal funktionierte, möglicherweise geringer ist als die einer seit Wochen nicht betätigten Komponente.

Dieser Überlegung liegt eine andere Modellvorstellung des Ausfallverhaltens zugrunde, nämlich die, daß Ausfälle im Bereitschaftszustand eintreten und durch die Anforderung lediglich aufgedeckt werden. Dieses Verhalten ist durch eine Ausfallrate zu beschreiben; die Ausfallwahrscheinlichkeit bei Anforderung hängt dann wesentlich vom zeitlichen Abstand seit der letzten Anforderung ab. Die Beschreibung des Ausfallverhaltens durch eine Ausfallrate wurde für die im nächsten Abschnitt dargestellten Auswertungen der Arbeitsaufträge angewandt. Damit ist das Komponentenverhalten durch die beiden extremen Modellvorstellungen so eingegrenzt, daß die Ausfallwahrscheinlichkeit einmal gar nicht

und das andere Mal proportional vom zeitlichen Abstand von der letzten Prüfung abhängt. Für die hier dargestellte Abschätzung der Ausfallwahrscheinlichkeit pro Anforderung wurde daher darauf verzichtet, Korrekturen an der Anzahl der Anforderungen je nach Abstand von der vorherigen vorzunehmen. Quantitativ würde sich eine solche Korrektur bei den betroffenen Komponentenstichproben mit einem Faktor  $< 2$  auswirken.

Von dem hier diskutierten Sonderfall abgesehen, hat die Entscheidung, ob die Ausfallwahrscheinlichkeit als konstanter Wert pro Anforderung oder als zeitlich konstante Rate dargestellt wird, keinen besonderen Einfluß, wenn die Werte in der Analyse auf Komponenten mit vergleichbaren Prüffristen angewandt werden. Die aus Prüfungen ermittelten Ausfallwahrscheinlichkeiten pro Anforderung sind hier eher pessimistisch, weil die Anforderung jeweils am Ende des Prüfintervalls liegt, d.h. den größtmöglichen zeitlichen Abstand zur vorhergehenden Anforderung hat. Betrachtet man in der Analyse dagegen Komponenten mit wesentlich größeren Prüf- oder Anforderungsabständen, dann liefert die Beschreibung mittels Ausfallrate ein konservatives Ergebnis, weil der größere Abstand zur vorhergehenden Anforderung voll berücksichtigt wird. In den Fehlerbaumanalysen der Risikostudie werden in diesen Fällen Ausfallraten verwendet.

Ausfallraten, d.h. auf die Betriebszeit bezogene Ausfallwahrscheinlichkeiten, wurden aus den wiederkehrenden Prüfungen nicht ermittelt. Der Grund dafür ist, daß bei dieser Art der Auswertung nicht alle während der Betriebszeit aufgetretenen Schäden erfaßt werden, da ein Teil davon nicht während wiederkehrender Prüfungen, sondern bei betrieblichem Einsatz oder bei der Revision entdeckt werden. Dieser Effekt beeinträchtigt jedoch nicht die Vergleichbarkeit mit den Werten der Fehlerbaumanalyse. Denn hierfür ist gerade die Wahrscheinlichkeit von Interesse, daß ein in Bereitschaft stehendes System oder eine Komponente bei Anforderung ihre Funktion nicht erfüllen.

Beim Vergleich mit den Fehlerbaumanalysen ist die zum Teil unterschiedliche Abgrenzung der Komponenten zu beachten. Bei den Analysen werden in manchen Fällen Daten für kleinere Betracht-

tungseinheiten verwendet, als sie sich aus den Protokollen für wiederkehrende Prüfungen ergaben. So werden beispielsweise gesonderte Zuverlässigkeitskenngrößen für eine Pumpe und ihre Ansteuerung verwendet. Bei der Prüfung werden diese Betriebsmittel integral erfaßt, da während der Prüfung selbst häufig noch nicht erkennbar ist, welches Betriebsmittel dafür verantwortlich ist, daß die Pumpe nicht anläuft. Zum Vergleich ist daher das Zwischenergebnis der Fehlerbaumanalyse heranzuziehen, das die entsprechenden Betriebsmittel beinhaltet.

Hinsichtlich der Auswirkungen eines Ausfalls ist zu beachten, in welchem Teil der Prüfung der Ausfall auftrat. Für die Ermittlung von Ausfallwahrscheinlichkeiten für die einzelnen Komponenten können sämtliche Ausfälle herangezogen werden, z.B. auch solche, die bei der Prüfvorbereitung auftraten. Für die Ausfallwahrscheinlichkeit des Systems sind dagegen nur die Ausfälle zu berücksichtigen, die die Systemfunktion beeinträchtigen. Steht etwa eine Armatur in der Offenposition, die sie auch während eines Störfalls nicht verlassen soll, dann ist die Funktionsfähigkeit des Systems nicht betroffen, wenn sich die Armatur während der Prüfvorbereitung nicht schließen läßt. Läßt sie sich zwar schließen, aber anschließend nicht wieder öffnen, dann ist der entsprechende Systemteil bis zur Beendigung der Instandsetzung nicht verfügbar. Für die Ausfallwahrscheinlichkeit des Systemteils zu einem beliebigen Zeitpunkt ist dieser Ausfall darüber hinaus mit der Wahrscheinlichkeit gewichtet zu berücksichtigen, mit der sich die Armatur bei Anforderung in geschlossener Stellung befinden kann.

Für die in diesem Fachband dargestellten Untersuchungen wurden wiederkehrende Prüfungen an folgenden Systemen herangezogen:

- Not- und Nachkühlssysteme,
- zugehörige nukleare Zwischen- und Nebenkühlkreisläufe,
- Notstromanlage,
- Gebäudeabschluß lufttechnischer Anlagen.

### 6.2.2 Wartungs- und Instandsetzungsarbeiten

Die Auswertung der Dokumentationen über Wartungs- und Instandsetzungsarbeiten erlaubt es, auch die Schäden zu ermitteln, die außerhalb von wiederkehrenden Prüfungen entdeckt wurden. Damit ist eine verlässliche Basis für die Ermittlung von Ausfallraten gegeben, indem man die aufgetretenen Schäden auf die Zeit bezieht. Für die hier dargestellten Auswertungen wurde hierfür die Kalenderzeit gewählt. Die Abschätzung unterstellt einen zeitlich konstanten Wert der Ausfallrate. Damit ist die Schätzformel:

$$\lambda = \frac{N_i}{\sum_{j=1} T_{ij}}$$

Dabei sind  $\lambda$  die Ausfallrate,  $N$  die Anzahl der Schäden und  $T_j$  die Beobachtungszeit der Komponente  $j$ . Der Index  $i$  charakterisiert die betrachtete Komponenten- und Ausfallart.

Die unterschiedlichen Modellvorstellungen, die der Beschreibung des Ausfallverhaltens durch eine Ausfallwahrscheinlichkeit pro Anforderung bzw. eine Ausfallrate zugrunde liegen, wurden bereits im vorhergehenden Abschnitt diskutiert. In den Fehlerbaumanalysen der Risikostudie werden überwiegend Ausfallraten verwendet. Damit sind die Ergebnisse der in diesem Abschnitt dargestellten Auswertung unmittelbar mit den Werten der Fehlerbaumanalyse vergleichbar. Hinzuweisen ist jedoch auf eine Abweichung in der Art der Fehlerentdeckung. In der Analyse wird davon ausgegangen, daß selbstmeldende Fehler sofort beseitigt werden, alle anderen werden erst bei der Prüfung entdeckt. Eine Fehlerentdeckung bei Kontrollgängen oder bei betrieblichem Einsatz des Systems wird nicht in Rechnung gestellt. Dies führt zu einem leichten Pessimismus der Analyse.

Die Unterlagen zu den durchgeführten Instandsetzungs- und Wartungsarbeiten erlauben eine feinere Unterteilung der Betrachtungseinheiten als die Kontrolle der wiederkehrenden Prüfungen,

da sich die Schäden leichter den einzelnen Betriebsmitteln zuordnen lassen. Hierauf wurde jedoch verzichtet und die gleiche Abgrenzung der Komponenten zugrunde gelegt wie bei den Auswertungen der wiederkehrenden Prüfungen. Zum einen sollte damit die Vergleichbarkeit der Ergebnisse erhalten und zum anderen auch der Aufwand verringert werden. Der Aufwand für die Auswertung der Dokumentation über Wartungs- und Instandsetzungsarbeiten ist ohnehin wesentlich größer. So kann die Information "Pumpe läuft nicht an" einem Prüfprotokoll unmittelbar entnommen werden, einem Arbeitsauftrag häufig nur durch technische Wertung der aufgetretenen Schäden. Daher wurde auch nicht für alle Systeme und Komponenten, für die Prüfprotokolle ausgewertet wurden, die Dokumentation über Wartungs- und Instandsetzungsarbeiten ausgewertet. Aufschreibungen für folgende Systeme wurden herangezogen:

- Not- und Nachkühlssysteme,
- zugehörige nukleare Zwischen- und Nebenkühlwasserkreisläufe.

Die Arbeitsaufträge eignen sich auch für die Ermittlung von Instandsetzungszeiten und Nichtverfügbarkeitszeiten aufgrund von Instandsetzungen. Unter Instandsetzungszeit wird dabei der Zeitraum von Beginn bis Ende der Arbeiten vor Ort verstanden, abzüglich 15 % für erforderliche Abrüstarbeiten. Die Instandsetzungszeit wird zweckmäßigerweise einer Komponente zugeordnet. Nichtverfügbarkeitszeiten sind dagegen auf größere Systemteile zu beziehen, die selbständig eine gewisse Systemfunktion erfüllen. Sie beschreiben die Zeit, während der diese Funktion aufgrund von Wartungs- oder Instandsetzungszeiten nicht verfügbar ist. Daher sind für die Nichtverfügbarkeitszeiten nicht nur die Instandsetzungszeiten zu berücksichtigen, sondern die gesamte Zeit von der Freischaltung bis zur Wiederschaltung. Für die Beurteilung von Sicherheitsfunktionen sind nur die Zeiten von Interesse, während der die betrachtete Funktion sicherheitstechnisch erforderlich ist. Für die hier untersuchten Not- und Nachkühlssysteme wurden Nichtverfügbarkeitszeiten bei abgeschaltetem Reaktor außer Betracht gelassen.

### 6.2.3 Einzelauswertungen

Die Protokolle der wiederkehrenden Prüfungen und die Dokumentation der durchgeführten Wartungs- und Instandsetzungsarbeiten sind die wesentlichen Informationsquellen, die zur Auswertung von Betriebserfahrungen für die Phase A der Studie herangezogen wurden. Einige Angaben, die für die Durchführung der Analysen erforderlich waren, ließen sich hieraus jedoch nicht ableiten, so daß auf andere Quellen zurückgegriffen werden mußte. Eine wesentliche Informationsquelle sind die Störberichte, die Angaben über Einleitung, Ablauf und Ursachen von aufgetretenen Störungen im Kernkraftwerk enthalten. Eine ausführliche Auswertung solcher Störberichte ist für die Phase B der Risikostudie vorgesehen. Für die Phase A stellten die Kraftwerksbetreiber Angaben zu folgenden Fragen zur Verfügung:

- Häufigkeit von Transienten, die zum Öffnen von Abblaseventilen auf dem Druckhalter führten (Abschnitt 3.1.2);
- Häufigkeit des Ausfalls des Hauptspeisewassersystems (Abschnitt 3.2.2);
- Ausfallwahrscheinlichkeit der Umleitstation. Es wurde die Anzahl der Öffnungsanforderungen an die Umleitstation (81) und die Anzahl der Ausfälle (2) ermittelt. Daraus wurde ein Erwartungswert für die Ausfallwahrscheinlichkeit pro Anforderung von  $\bar{p} = 3,7 \cdot 10^{-2}$  geschätzt;
- Ausfallwahrscheinlichkeit von Sicherheitsventilen. Es wurde die Anzahl der Prüfungen und Transienten ermittelt, bei denen sich Frischdampf-Sicherheitsventile geöffnet hatten (Abschnitt 7.9).

Bei Notstromdieseln führten die Auswertungen in den beiden betrachteten Kernkraftwerken auf einen zu geringen Beobachtungsumfang. Daher wurden die Erfahrungen sämtlicher deutscher Kernkraftwerke berücksichtigt. Hierzu wurden die Meldungen über besondere Vorkommnisse herangezogen (Abschnitt 7.11).

Die Ausfallrate für das Nichteinfallen von Steuerstäben wurde auf der Basis der Steuerstabbetriebsstunden und der Anzahl der Ausfälle (Null) bei Reaktorschnellabschaltungen abgeschätzt,



wobei ausschließlich KWU-Druckwasserreaktoren berücksichtigt wurden (Abschnitt 7.12).

### 6.3 Ergebnisse

#### 6.3.1 Ausfallraten und Ausfallwahrscheinlichkeiten

Im Anhang 2 sind die ermittelten Ausfallraten und Ausfallwahrscheinlichkeiten pro Anforderung in Form einer Übersicht wiedergegeben. Zu den einzelnen Größen ist jeweils die zugrunde liegende Anzahl von Ausfällen angegeben, somit kann die Betriebszeit bzw. die Anzahl der Anforderungen leicht erkannt werden. Einige Werte wurden aufgrund von null Ausfällen abgeschätzt. Als Abschätzung wurde hier der 50-%-Wert der  $\chi^2$ -Verteilung verwendet. Das ist der Wert einer Wahrscheinlichkeit von 50 %, daß bei dem gegebenen Umfang keine Ausfälle beobachtet werden. Zwischen dem angegebenen Wert und dem Beobachtungsumfang besteht dabei die folgende Beziehung:

$$\lambda = \frac{\chi^2_{50;2}}{T} = \frac{0,693}{T} \text{ bzw. } p = \frac{\chi^2_{50;2}}{N} = \frac{0,693}{N} \quad 1)$$

Die Ergebnisse sind den allgemeinen Komponentenklassen zugeordnet, wie sie für die Verwendung von Fehlerbaumanalysen definiert wurden. Die Stichproben, aus denen die einzelnen Werte gebildet wurden, sind nach solchen Gesichtspunkten zusammengestellt worden, daß zum einen die Stichprobe groß genug ist, um statistisch signifikante Ergebnisse zu erzielen, und zum anderen die Komponenten der Stichprobe bezüglich konstruktiver und betrieblicher Daten ausreichend vergleichbar sind.

Die verschiedenen Ausfallraten, die im Anhang 2 für eine Komponente angegeben sind, beruhen auf verschiedenen, voneinander

---

<sup>1)</sup> Zur  $\chi^2$ -Verteilung vergleiche Fachband 2. Für die Bestimmung von Vertrauensintervallen für Ausfallwahrscheinlichkeiten ist die  $\chi^2$ -Verteilung nicht generell geeignet. In allen hier betrachteten Fällen ergibt sich jedoch kein numerischer Unterschied gegenüber einer strengeren Behandlung.

unabhängigen Stichproben. Dasselbe gilt für die dort angegebenen Ausfallwahrscheinlichkeiten. Dagegen kann ein einzelner Wert für eine Ausfallrate und für eine Ausfallwahrscheinlichkeit auf sich überschneidenden Stichproben basieren. Wie bereits erwähnt, unterscheiden sich die Abgrenzungen der Komponenten zum Teil von den für die Fehlerbaumanalysen verwendeten (z.B. Pumpe ohne bzw. mit Ansteuerung). Bei Vergleichen zwischen den Werten im Anhang 2 und den für die Fehlerbaumanalysen verwendeten Größen sind daher die Anmerkungen zu berücksichtigen, die zu den einzelnen Komponenten in Kapitel 7 gemacht werden.

Bei den Auswertungen fielen auch Zuverlässigkeitskenngrößen für Komponenten oder Ausfallarten an, die für die Fehlerbaumanalysen nicht von Bedeutung sind. Diese Daten sind im Anhang 2 ebenfalls angegeben. Weiter sind Daten für Meßstellen aufgeführt. Die für die Fehlerbaumanalysen verwendeten Werte hierzu sind in Kapitel 8 dargestellt. Die Ergebnisse für die einzelnen Komponenten werden in Kapitel 7 diskutiert.

### 6.3.2 Ausfallwahrscheinlichkeiten von Teilsträngen

Aus den wiederkehrenden Prüfungen wurden außer für Komponenten auch Ausfallwahrscheinlichkeiten für Funktionsversagen von Teilsträngen im Anforderungsfall ermittelt. Es wurde unterschieden zwischen Ausfällen, die nur im Prüfungsfall und solchen, die auch bei Anforderung im Störfall auftreten können. Beispiel für den ersteren Fall ist etwa, daß eine in Bereitschaftsstellung offene Armatur für die Prüfung geschlossen wird und sich danach nicht wieder öffnen läßt. Im Störfall muß diese Armatur nicht verfahren werden. Die Zahlen geben jeweils die Ausfallwahrscheinlichkeit eines von vier redundanten Teilsträngen an. Die angegebenen 50 % beim Druckspeicher bedeuten, daß eine von zwei Einspeiseleitungen eines Druckspeichers betroffen war. Soweit einzelne Ausfälle mehrere Funktionen betreffen (z.B. Flut- und Sumpfbetrieb des Niederdrucksystems), wurde der Ausfall bei jeder Funktion mitgezählt.

Zum Vergleich sind die entsprechenden Werte der Fehlerbaumanalyse angegeben. Sie wurden für die gleichen Teilsystemabgrenzungen, die für die beobachteten Werte gelten, mit den in der Risikostudie verwendeten Zuverlässigkeitskenngrößen berechnet. Als Zeitraum seit der letzten Anforderung wurde das Prüfintervall zugrunde gelegt. Es wurden nur die für Anforderung im Störfall geltenden Werte berechnet (Tabelle F3, 6-1).

Berücksichtigt man, daß die beobachteten Ausfallwahrscheinlichkeiten auf einer sehr geringen Anzahl von Ausfällen basieren, ist eine gute Übereinstimmung von Rechnung und Erfahrung festzustellen. Die berechneten Werte liegen durchweg ca. um einen Faktor 2 höher, sind also pessimistisch. Nahezu völlige Übereinstimmung zwischen beobachteten und berechneten Werten erhält man, wenn man statt der Ausfallwahrscheinlichkeit am Ende des Prüfintervalls die mittlere Ausfallwahrscheinlichkeit berechnet, die gerade um den Faktor 2 niedriger ist als die maximale.

### 6.3.3 Instandsetzungszeiten von Komponenten

Aus der Dokumentation wurden Instandsetzungszeiten für unterschiedliche Populationen von Pumpen und Armaturen sowie für Meßstellen ermittelt. In Tabelle F3, 6-2 werden jeweils die Anzahl der zugrunde liegenden Instandsetzungen, der Mittelwert und die Standardabweichung der Instandsetzungszeit sowie der maximal beobachtete Wert angegeben. Zu beachten ist, daß bei Sicherheitssystemen im Betrieb gleichzeitig jeweils nur ein Strang instand gesetzt werden darf und daß die maximale Instandsetzungszeit durch Auflagen beschränkt ist.

Andere Meßstellen, für die zu wenig Einzelwerte vorlagen, um Mittelwerte anzugeben, liegen mit einer Ausnahme im Bereich bis 7 Stunden. Bei einer Durchflußmeßstelle war eine Impulsleitung verstopft und konnte nicht freigespült werden. Die Instandsetzung nahm 36 Stunden in Anspruch.

Systemteil	Anzahl der Ausfälle		Ausfallwahrscheinlichkeiten		Berechnete Ausfallwahrscheinlichkeit
	N <sub>prüf</sub> <sup>1)</sup>	N	P <sub>prüf</sub>	P	
Hochdruckeinspeisestrang	-	2	-	$8 \cdot 10^{-3}$	$1,6 \cdot 10^{-2}$
Niederdruckeinspeisestrang (Fluten)	4	1 <sup>2)</sup>	$3,2 \cdot 10^{-2}$	$8 \cdot 10^{-3}$	$1,6 \cdot 10^{-2}$
Niederdruckeinspeisestrang (Sumpfbetrieb)	4	2 <sup>2)</sup>	$3,2 \cdot 10^{-2}$	$1,6 \cdot 10^{-2}$	$2,4 \cdot 10^{-2}$
Druckspeicher 50 %	1	-	$8 \cdot 10^{-3}$	-	<sup>4)</sup>
Zwischenkühlstrang	-	1	-	$8 \cdot 10^{-3}$	$1,8 \cdot 10^{-2}$
Nebenkühlstrang <sup>3)</sup>	3	4	$2,4 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	$1,6 \cdot 10^{-2}$
Nachkühlstrang, betriebliches Kühlen	-	7	-	$5,6 \cdot 10^{-2}$	<sup>5)</sup>

- 1) Index "prüf": Ausfälle, die nur im Prüfungsfalle auftreten können; ohne Index: Ausfälle, die auch im Störfall auftreten können.
- 2) Beinhaltet einen Fehler, der bei der Revision auftrat und bereits beim Anfahren durch eine zum Nachweis der Funktionsfähigkeit durchgeführte Prüfung entdeckt wurde. Das unbemerkte Auftreten eines entsprechenden Fehlers bei Normalbetrieb ist unwahrscheinlich; die Berücksichtigung des Falles ist daher pessimistisch.
- 3) N<sub>prüf</sub> und N sind auf eine unterschiedliche Anzahl von Anforderungen zu beziehen, da die Ausfälle unter N<sub>prüf</sub> nur bei einem Teil der Prüfungen auftreten können.
- 4) Die Nichtverfügbarkeit der Druckspeichereinspeisungen wird durch halbjährlich und jährlich geprüfte Funktionselemente bestimmt; die hier betrachteten monatlichen Prüfungen sind daher für einen Vergleich nicht geeignet.
- 5) Die Systemfunktion "betriebliches Kühlen" wurde in den Fehlerbaumanalysen nicht untersucht, daher ist kein Vergleichswert verfügbar.

Tab. F3, 6-1:

Vergleich beobachteter und berechneter Ausfallwahrscheinlichkeiten für Teilstränge

Komponente	Anzahl der Instandsetzungen	Mittlere Instandsetzungszeit	Standardabweichung [h]	Maximalwert [h]
Pumpe	35	8,3	11,6	42
	35	5,4	8,6	40
	13	17,8	22,1	72
	18	4,6	3,6	18
	4	3,4	1,5	5
	4	15,4	9,4	24
Motorventile	37	7,1	7,9	30
Motorschieber	10	4,4	5,2	13
Handventile	10	6,1	3,5	15
Handschieber	4	4,6	2,6	7,5
Rückschlagventile	2	6	-	10
Kleinventile und Verschraubungen	13	3,5	2,8	8
Druckmeßstelle	9	3,2	2,4	6

Tab. F3, 6-2:

Instandsetzungszeiten von Komponenten

#### 6.3.4 Nichtverfügbarkeiten von Teilsträngen infolge Instandhaltungsmaßnahmen

Für die Teilstränge des Not- und Nachkühlsystems sowie des Gebäudesprühsystems wurden Nichtverfügbarkeiten infolge von Instandhaltungsmaßnahmen ermittelt. Berücksichtigt wurden dabei alle Wartungs- und Instandsetzungsarbeiten, die während des Leistungsbetriebes der Anlage durchgeführt wurden, und während derer der betreffende Teilstrang nicht verfügbar war, d.h. bei Anforderung nicht unmittelbar in Betrieb gegangen wäre. Der Leistungsbetrieb wurde so gegen die Stillstände abgegrenzt, daß Nichtverfügbarkeiten, die in Stillstände bis zu 5 Stunden Dauer

fielen, mit berücksichtigt wurden, Arbeiten während längerer Stillstände, z.B. Revision, dagegen nicht. Die Nichtverfügbarkeiten wurden ermittelt als Verhältnis der Summe aller Zeiten, während derer ein Teilstrang unter den genannten Bedingungen nicht verfügbar war, zur Gesamtbetriebszeit. Es wurde die Kalenderzeit angesetzt. Einige Instandhaltungsmaßnahmen führen zur Nichtverfügbarkeit sowohl der Niederdruckeinspeisung als auch der Nachkühlung. Solche Zeiten wurden bei beiden Teilfunktionen berücksichtigt. Tabelle F3, 6-3 gibt die Ergebnisse wieder; zur Demonstration der Streuung der Werte werden die Werte für die einzelnen Redundanzen NV und der Mittelwert  $\overline{NV}$  angegeben.

Teilfunktion	NV <sub>1</sub>	NV <sub>2</sub>	NV <sub>3</sub>	NV <sub>4</sub>	$\overline{NV}$
Hochdruckeinspeisung	$4,3 \cdot 10^{-4}$	$9,7 \cdot 10^{-4}$	$5,1 \cdot 10^{-4}$	$1,3 \cdot 10^{-3}$	$8,1 \cdot 10^{-4}$
Druckspeicher-einspeisung	$3,1 \cdot 10^{-4}$	$6,9 \cdot 10^{-4}$	$1,4 \cdot 10^{-3}$	0	$5,9 \cdot 10^{-4}$
Niederdruckeinspeisung	$2,2 \cdot 10^{-3}$	$3,4 \cdot 10^{-3}$	$1,4 \cdot 10^{-2}$	$1,7 \cdot 10^{-3}$	$5,3 \cdot 10^{-3}$
Nachkühlung	$4,1 \cdot 10^{-3}$	$3,4 \cdot 10^{-3}$	$1,4 \cdot 10^{-2}$	$1,9 \cdot 10^{-3}$	$5,9 \cdot 10^{-3}$
Gebäudesprühen	$9,3 \cdot 10^{-3}$	$2 \cdot 10^{-4}$	0	$1,1 \cdot 10^{-3}$	$2,7 \cdot 10^{-3}$

Tab. F3, 6-3:

Nichtverfügbarkeiten von Teilsträngen infolge Instandhaltungsmaßnahmen

In den Fehlerbaumanalysen wurden die hier dargestellten beobachteten Nichtverfügbarkeiten den einzelnen Komponentenarten (Pumpen, Armaturen usw.) zugeordnet und zu den Nichtverfügbarkeiten infolge anderer Ursachen, z.B. unentdeckter Komponentenausfälle, addiert. Die Zahlenwerte wurden den hier dargestellten Betriebserfahrungen entnommen, daher erübrigt sich ein Vergleich von Rechnung und Beobachtung.

Aus einem Vergleich der Tabellen F3, 6-1 und -3 ist ersichtlich, daß die Nichtverfügbarkeit infolge Instandhaltung einen vergleichsweise geringen Beitrag zur genannten Nichtverfügbarkeit von Sicherheitssystemen im Anforderungsfall liefert.

## 7. ZUVERLÄSSIGKEITSKENNGRÖSSEN FÜR VERFAHRENS- UND ELEKTRO- TECHNISCHE KOMPONENTEN

### 7.1 Übersicht

In den Kapiteln 5 und 6 wurde das Vorgehen zur Ermittlung von Zuverlässigkeitskenngrößen aus Literatur und Betriebserfahrungen generell dargestellt. In diesem Kapitel wird die Ermittlung der Daten für die einzelnen Komponenten dokumentiert. Das angewandte Vorgehen wird im einzelnen in Abschnitten für die jeweiligen Komponenten dargestellt. Dabei werden auch Betriebserfahrungen, die zum Zeitpunkt der Festlegung der Daten noch nicht verfügbar waren, zum Vergleich angegeben. Tabelle F3, A1-1 gibt einen Überblick über die der Literatur entnommenen Ausgangsdaten. Tabelle F3, A1-2 enthält die daraus abgeleiteten Werte in der Form, wie sie zur Festlegung der Daten für die Risikostudie verwendet wurden. Soweit Modifikationen der Ausgangsdaten vorgenommen wurden, wird dies in den Abschnitten zu den einzelnen Komponenten begründet. Die Bilder F3, A1-1 bis -16 geben eine grafische Darstellung der ermittelten logarithmischen Normalverteilungen und der zugrunde liegenden Einzelwerte. Die Zahlen, die den Einzelwerten zugeordnet sind, geben die Literaturstelle wieder, B kennzeichnet Betriebserfahrungen. Tabelle F3, 7-1 enthält den Überblick über die für die Rechnungen verwendeten Daten.

### 7.2 Pumpen

#### 7.2.1 S t a r t v e r s a g e n

Die Verteilung der Ausfallrate für Startversagen wurde aufgrund der in Bild F3, A1-1 eingetragenen Literaturstellen ermittelt. Zur Quelle /F3, 7-34/ ist anzumerken, daß es sich hierbei um eine eigene Auswertung von Betriebserfahrungen in einem Braunkohlekraftwerk handelt. Dabei wurden entsprechend dem in Kapitel 6 für die Auswertung der Dokumentation über Instandhaltungsarbeiten dargestellten Verfahren in Bild F3, A1-1 eingetragenen Werte für 9 unterschiedliche Populationen ermittelt.



Komponente	Ausfallart	Median		Streufaktor K <sub>95</sub>
		Ausfallrate 1/h <sup>1)</sup>	Ausfallwahrscheinlichkeit 1/A <sup>2)</sup>	
Pumpe	Startversagen	8 · 10 <sup>-6</sup>		7
	Betriebsversagen	2,5 · 10 <sup>-5</sup>		15
Motorarmatur	öffnet nicht oder schließt nicht	7 · 10 <sup>-6</sup>		5
Magnetventil	öffnet nicht oder schließt nicht	7 · 10 <sup>-6</sup>		20
Pneumatisches Ventil	öffnet nicht oder schließt nicht	7 · 10 <sup>-6</sup>		23
Rückschlagarmatur	öffnet nicht	8 · 10 <sup>-7</sup>		10
	schließt nicht	2,5 · 10 <sup>-6</sup>		3
	innere Leckage	1,5 · 10 <sup>-5</sup>		10
Rückschlagarmatur mit Motorantrieb (ohne Motor)	öffnet nicht	1,5 · 10 <sup>-6</sup>		10
	schließt nicht	1 · 10 <sup>-6</sup>		3
	innere Leckage	1 · 10 <sup>-5</sup>		10
Handarmatur	öffnet nicht oder schließt nicht	1,5 · 10 <sup>-6</sup>		12
Regelarmatur	fährt nicht auf	5 · 10 <sup>-6</sup>		7
	fährt nicht zu	5 · 10 <sup>-6</sup>		7
Umschaltventil	schaltet nicht um		4 · 10 <sup>-2</sup>	10
FD-Schnellschlußschieber	öffnet nicht oder schließt nicht		6 · 10 <sup>-3</sup>	4
Entlastungsventil	öffnet nicht oder schließt nicht		4 · 10 <sup>-3</sup>	6
Steuerventil	öffnet nicht oder schließt nicht		4 · 10 <sup>-3</sup>	6
Si-Ventil mit einem Vorsteuerventil	öffnet nicht oder schließt nicht		7 · 10 <sup>-3</sup>	4
Si-Ventil mit zwei Vorsteuerventilen	öffnet nicht		4 · 10 <sup>-3</sup>	6
	schließt nicht		7 · 10 <sup>-3</sup>	4
Si-Ventil mit drei Vorsteuerventilen	öffnet nicht		4 · 10 <sup>-3</sup>	6
	schließt nicht		7 · 10 <sup>-3</sup>	4
Si- oder Entlastungsventil	öffnet unbeabsichtigt	2 · 10 <sup>-6</sup>		7
Notstromdiesel	Startversagen		2,5 · 10 <sup>-2</sup>	3
	Betriebsversagen	5 · 10 <sup>-3</sup>		2
Dichtung	Leckage	4 · 10 <sup>-7</sup>		8
Steuerstab	fällt nicht ein	1,4 · 10 <sup>-7</sup>		4
Elektromotor	Startversagen	1 · 10 <sup>-6</sup>		8
	Betriebsversagen	2 · 10 <sup>-6</sup>		8
Leistungsschalter ohne Abzweig	schließt nicht	3 · 10 <sup>-7</sup>		6
	öffnet nicht	2 · 10 <sup>-7</sup>		11
Abzweig	öffnet nicht oder schließt nicht	1 · 10 <sup>-6</sup>		10
Generatorschalter	öffnet nicht	6 · 10 <sup>-7</sup>		5
Schütz	Verlust der Hauptfunktion 40-60 A 300-460 A	9 · 10 <sup>-7</sup>		10
		1 · 10 <sup>-6</sup>		15
Sicherung	vorzeitige Unterbrechung	1 · 10 <sup>-6</sup>		10
Transformator		1,5 · 10 <sup>-6</sup>		5
Notstromdiesel CMA	Startversagen	2 · 10 <sup>-4</sup>		10
Notstromdiesel CMA	Betriebsversagen	1,5 · 10 <sup>-4</sup>		10

<sup>1)</sup> Ausfallraten pro Stunde    <sup>2)</sup> Ausfallwahrscheinlichkeit pro Anforderung

**Tab. F3, 7-1:**

Ausfallraten und Ausfallwahrscheinlichkeiten für verfahrens- und elektrotechnische Komponenten

In den Literaturstellen /F3, 7-3 bis -9, -28, -30 und -40/ werden Ausfallraten für Pumpen angegeben, ohne daß zwischen Startversagen und Ausfällen im Betrieb unterschieden wird. Die Werte wurden im Verhältnis 1 : 4 auf Start- und Betriebsausfälle aufgeteilt. Dieses Verhältnis ergibt sich aus /F3, 7-34/. Literaturwerte, die als Ausfallwahrscheinlichkeit pro Anforderung angegeben sind, wurden für die Bestimmung der Verteilung nicht herangezogen, weil die zur Umrechnung benötigten Zeiten zwischen den Anforderungen nicht bekannt sind. Aus den Einzelwerten ergibt sich die eingezeichnete Verteilung mit dem Median  $8 \cdot 10^{-6}$  pro Stunde und dem Streufaktor 7. Der Erwartungswert dieser Verteilung ist  $\bar{\lambda} = 1,6 \cdot 10^{-5}$  pro Stunde. Diese Verteilung wurde in den Fehlerbaumanalysen für die Pumpe mit Antrieb verwendet.

Beim Vergleich mit den im Anhang 2 aufgeführten Werten aus der Betriebserfahrung ist zu berücksichtigen, daß in diesen Werten außer dem Antrieb noch der Abzweig und die Ansteuerung enthalten sind, die in den Fehlerbaumanalysen gesondert berücksichtigt werden. Zum Vergleich ist also die Summe der Werte zu verwenden, die in den Fehlerbaumrechnungen für Pumpe, Abzweig und Ansteuerung angesetzt werden. Die Verteilungen für Abzweig und Ansteuerung haben Medianwerte von  $1 \cdot 10^{-6}$  pro Stunde und Streufaktoren von 10 bzw. 3. Nähert man die Verteilung der Summe der drei Ausfallraten wieder mit einer logarithmischen Normalverteilung an, dann erhält man einen Median von  $1 \cdot 10^{-5}$  pro Stunde und einen Streufaktor von 6. Der Erwartungswert beträgt  $2 \cdot 10^{-5}$  pro Stunde.

Nähert man die im Anhang 2 angegebenen Ausfallraten für Startversagen von Pumpen durch eine logarithmische Normalverteilung an, dann erhält man einen Median  $\lambda_{50} = 1,4 \cdot 10^{-5}$  pro Stunde, einen Streufaktor  $K_{95} = 2,8$  und einen Erwartungswert  $\bar{\lambda} = 1,7 \cdot 10^{-5}$  pro Stunde. Damit ergibt sich eine gute Übereinstimmung zwischen den für die Fehlerbaumanalysen verwendeten Daten und den Betriebserfahrungen. Der Erwartungswert, der für die Ergebnisse der Analysen bestimmend ist, weicht nur geringfügig ab, der Wert aus den Betriebserfahrungen ist etwas günstiger. Die Da-

ten aus den Betriebserfahrungen weisen eine deutlich geringere Streuung auf als die für die Analysen verwendeten.

Zum Vergleich mit den aus der Betriebserfahrung ermittelten Ausfallwahrscheinlichkeiten bei Anforderung muß man die in der Analyse verwendete Rate in eine Ausfallwahrscheinlichkeit bei Anforderung umrechnen. Unterstellt man, daß die Anforderung durch einen Störfall zu einem beliebigen Zeitpunkt erfolgen kann, dann liegt im Mittel die letzte Prüfung ein halbes Prüfintervall  $T$  zurück. Der Erwartungswert der Ausfallwahrscheinlichkeit ist damit

$$\bar{p} = \frac{1}{2} \bar{\lambda} T$$

Bei den üblichen 4wöchigen Prüfungen ergibt dies einen Wert von  $7 \cdot 10^{-3}$ . Dieser Wert ist etwa doppelt so groß wie der Erwartungswert, der sich aus den Betriebserfahrungen ergibt. Für Pumpen mit längeren Prüffristen liefert die Analyse entsprechend ungünstigere Werte.

### 7.2.2 Betriebsversagen

Die Ausfallrate für den Ausfall einer in Betrieb befindlichen Pumpe wurde aus den im Anhang 1 eingetragenen Literaturquellen ermittelt. Ein großer Teil /F3, 7-34/ stammt aus eigenen Auswertungen in einem Braunkohlekraftwerk. Die Werte aus den Literaturstellen /F3, 7-3 bis -9, -28, -30 und -40/, bei denen nicht zwischen Betriebs- und Startversagen unterschieden wird, wurden zu 80 % als Betriebsversagen ausgelegt (Abschnitt 7.2.1). Die Verteilung mit dem Median  $\lambda_{50} = 2,5 \cdot 10^{-5}$  pro Stunde und dem Streufaktor  $K_{95} = 15$  hat einen Erwartungswert von  $\bar{\lambda} = 9,7 \cdot 10^{-5}$  pro Stunde. Diese Zahlen sind mit den Betriebserfahrungen, die im Anhang 2 unter der Ausfallart "Pumpe fördert nicht" aufgeführt sind, unmittelbar vergleichbar. Eine aus diesen Werten abgeschätzte logarithmische Normalverteilung hat einen Median  $\lambda_{50} = 2,1 \cdot 10^{-5}$  pro Stunde und einen Streufaktor  $K_{95} = 3,7$ . Ihr Erwartungswert ist  $\bar{\lambda} = 2,9 \cdot 10^{-5}$  pro Stunde.

Die Betriebserfahrung liefert in diesem Fall deutlich günstigere Werte, als sie aufgrund der Literaturlauswertung für die Rechnungen verwendet wurden. Die Medianwerte der beiden Verteilungen unterscheiden sich zwar nur wenig, infolge der wesentlich geringeren Streuung der Betriebserfahrung liegt der Erwartungswert, der für den Vergleich heranzuziehen ist, jedoch um mehr als den Faktor 3 niedriger.

Eine Auswertung von Betriebserfahrungen in französischen Kernkraftwerken /F3, 7-41/ liefert ungünstigere Werte für den Ausfall von Pumpen während des Betriebs. Sie liegen zwischen  $1,2 \cdot 10^{-5}$  pro Stunde und  $4,5 \cdot 10^{-4}$  pro Stunde für unterschiedliche Arten von Pumpen und entsprechen im Erwartungswert etwa der aus der Literatur ermittelten Verteilung. Die Abweichung zu den hier dargestellten Betriebserfahrungen ist darauf zurückzuführen, daß unterschiedliche Pumpen untersucht wurden. Für die Risikostudie wurden die Pumpen in Sicherheitssystemen untersucht, die überwiegend nur einen geringen Anteil der Zeit in Betrieb sind. In /F3, 7-41/ wurden hauptsächlich ständig in Betrieb befindliche Pumpen des Wasser/Dampf-Kreislaufes untersucht, wie Speisewasser- und Hauptkühlwasserpumpen. Das trifft auch für die meisten der in /F3, 7-34/ untersuchten Pumpen zu, die ebenfalls höhere Werte aufweisen. Diesem Umstand ist durch eine stärkere Differenzierung der Daten nach Pumpenarten und Betriebsbedingungen Rechnung zu tragen. Hierauf weist auch bereits die große Streuung der aus der Literatur ermittelten Verteilung hin.

### 7.3 Motorarmatur

Für die Fehlerbaumanalysen werden Ausfallraten zu den Ausfallarten "öffnet nicht" und "schließt nicht" benötigt. Aus der Betriebserfahrung ist bekannt, daß sich diese Raten nicht wesentlich unterscheiden, daher wurde für beide Raten der gleiche Wert verwendet. Einige Literaturstellen unterscheiden nicht zwischen den beiden Ausfallarten. Diese Werte wurden nicht auf die beiden Ausfallarten aufgeteilt, es wurde vielmehr unter-

stellt, daß sie für beide Ausfallarten gelten. Dafür waren zwei Überlegungen maßgebend. Zum einen haben die Armaturen auch im Betrieb oftmals eine der beiden Funktionen auszuüben, so daß sich auch die beobachteten Ausfälle vorwiegend hierauf beziehen. Zum anderen führt ein relativ großer Teil der Ausfälle dazu, daß die Armatur weder öffnet noch schließt.

Die verwendeten Literaturstellen sind Bild F3, A1-3 zu entnehmen. Die ermittelte Verteilung mit dem Median  $\lambda_{50} = 7 \cdot 10^{-6}$  pro Stunde und dem Streufaktor 5 hat einen Erwartungswert von  $\bar{\lambda} = 1,1 \cdot 10^{-5}$  pro Stunde. Zum Vergleich mit den im Anhang 2 aufgeführten Betriebserfahrungen sind hierzu wie in Abschnitt 7.2.1 die Raten für Abzweig und Ansteuerung zu addieren. Beschreibt man die Summe mit einer logarithmischen Normalverteilung, dann erhält man einen Median  $\lambda_{50} = 1,1 \cdot 10^{-5}$  pro Stunde, einen Streufaktor  $K_{95} = 4$  und einen Erwartungswert  $\bar{\lambda} = 1,5 \cdot 10^{-5}$  pro Stunde.

Bei den Betriebserfahrungen sind zu Vergleichszwecken sowohl die Werte für "öffnet nicht" als auch für "schließt nicht" verwendbar. Die zugehörige logarithmische Normalverteilung hat die Parameter  $\lambda_{50} = 1,4 \cdot 10^{-5}$  pro Stunde,  $K_{95} = 3$ ,  $\bar{\lambda} = 1,7 \cdot 10^{-5}$  pro Stunde. Bei etwas geringerer Streuung erhält man nahezu den gleichen Erwartungswert, den die für die Fehlerbaumanalyse verwendete Verteilung aufweist.

Berechnet man aus der in der Studie verwendeten Ausfallrate eine Ausfallwahrscheinlichkeit pro Anforderung, dann erhält man bei monatlicher Prüfung und Zugrundelegung des halben Prüfindervalls (Abschnitt 7.2.1) einen Erwartungswert von  $\bar{p} = 5,4 \cdot 10^{-3}$ . Die im Anhang 2 angeführten Ausfallwahrscheinlichkeiten pro Anforderung sind bis auf einen Wert alle kleiner. Bei längeren Prüfindervallen sind die aus der Fehlerbaumanalyse ermittelten Werte noch höher.

#### 7.4 Magnetventil

Die Verteilung der Ausfallrate für Magnetventile wurde aufgrund der in Bild F3, A1-4 angegebenen Literaturstellen ermittelt. Es handelt sich um nur 6 Werte, die stark streuen. Es ergibt sich ein Median von  $\lambda_{50} = 7 \cdot 10^{-6}$  pro Stunde und ein Streufaktor von  $K_{95} = 20$ . Infolge der großen Streuung liegt der Erwartungswert mit  $\bar{\lambda} = 3,7 \cdot 10^{-5}$  pro Stunde erheblich über dem Median.

Bei den in Kapitel 6 dargestellten Auswertungen von Betriebserfahrungen wurden keine Magnetventile erfaßt, daher liegen von dort keine Vergleichswerte vor. Im Vergleich zu den Werten für andere Armaturentypen wie Motor- und Handarmaturen ist die ermittelte Rate sehr hoch. Plausible technische Gründe gibt es hierfür nicht. Von daher ist anzunehmen, daß die Ausfallrate für Magnetventile durch die Literaturdaten deutlich überschätzt wird.

In dieselbe Richtung deutet ein Vergleich mit den magnetbetätigten Vorsteuerventilen der Frischdampf-Sicherheitsventile. Hierfür wurde aufgrund in der Praxis aufgetretener Anforderungen gesondert eine Ausfallwahrscheinlichkeit abgeschätzt (Abschnitt 7.9). Der ermittelte Erwartungswert ist  $\bar{p} = 7 \cdot 10^{-3}$  pro Anforderung. Legt man die aus der Literatur ermittelte Rate zugrunde, dann würde einer Ausfallwahrscheinlichkeit von  $7 \cdot 10^{-3}$  eine Anforderungshäufigkeit von ca. 1 pro Woche entsprechen, was offensichtlich unrealistisch ist. Pro Jahr wären in einer Anlage bei einer Ausfallrate von  $3,7 \cdot 10^{-5}$  pro Stunde ca. 4 Ausfälle von Vorsteuerventilen für Frischdampf-Sicherheitsventile zu erwarten, tatsächlich wurden über mehrere Jahre keine beobachtet.

Da ein Vergleich nur mit einem Typ von Magnetventilen möglich ist, wurde die aus der Literatur ermittelte Ausfallrate ohne Korrektur übernommen, lediglich für die Vorsteuerarmaturen von Sicherheits- und Entlastungsventilen wurden gesonderte Werte angesetzt. Bei weiterer Auswertung von Betriebserfahrungen ist mit einer verringerten Ausfallrate für Magnetventile zu rechnen.

## 7.5 Pneumatisches Ventil

Die Ausfallrate für pneumatische Ventile wurde aufgrund der in Bild F3, A1-5 angegebenen Literaturstellen ermittelt. Bei einem Median von  $\lambda_{50} = 7 \cdot 10^{-6}$  pro Stunde und einem Streufaktor von  $K_{95} = 23$  ergibt sich ein Erwartungswert von  $\bar{\lambda} = 4,3 \cdot 10^{-5}$  pro Stunde.

Die außerordentlich große Streuung ist vermutlich auf unterschiedliche Einsatzbedingungen zurückzuführen, z.B. können sehr unterschiedliche Anforderungen an die Qualität der Preßluft gestellt werden. Da keine eigenen Auswertungen von Betriebserfahrungen vorliegen, wurde die aus der Literatur ermittelte Rate verwendet. Der Vergleich mit anderen Armaturentypen läßt vermuten, daß die Ausfallrate wesentlich zu hoch ist.

## 7.6 Rückschlagarmatur

### 7.6.1 " ö f f n e t n i c h t "

Die Verteilung wurde aufgrund der in Bild F3, A1-6 angegebenen Literaturstellen ermittelt. Soweit in einzelnen Quellen nicht nach den Ausfallarten "öffnet nicht" bzw. "schließt nicht" unterschieden wurde, wurden die Werte im Verhältnis 35 : 65 auf diese Ausfallarten aufgeteilt. Dieses Verhältnis ergibt sich aus den restlichen Quellen. Es folgt ein Median von  $\lambda_{50} = 8 \cdot 10^{-7}$  pro Stunde, ein Streufaktor von  $K_{95} = 10$  und ein Erwartungswert von  $\bar{\lambda} = 2,1 \cdot 10^{-6}$  pro Stunde.

Die im Anhang 2 angegebenen Betriebserfahrungen zeigen ein erheblich günstigeres Bild. Bei einer Gesamtbeobachtungszeit von ca.  $2,5 \cdot 10^6$  Stunden wurde kein Ausfall beobachtet. Daraus kann eine Ausfallrate von etwa  $3 \cdot 10^{-7}$  pro Stunde abgeschätzt werden. Etwa  $1,5 \cdot 10^6$  Betriebsstunden entfielen auf Rückschlagventile NW 250 des Not- und Nachkühlsystems. Für diese Ventile wurde eine logarithmische Normalverteilung mit dem Median  $\lambda_{50} = 5 \cdot 10^{-7}$  pro Stunde und einem Streufaktor  $K_{95} = 4$  verwendet.

Median und 95%-Fraktile dieser Verteilung stimmen mit dem 50%- bzw. 95%-Wert der  $\chi^2$ -Verteilung überein, die sich für null Ausfälle ergibt. Der Erwartungswert der logarithmischen Normalverteilung ist  $\bar{\lambda} = 7,1 \cdot 10^{-7}$  pro Stunde.

Da eine signifikant günstigere Ausfallrate vom Beobachtungsumfang her nur für diese Population belegbar ist, wurde für andere Rückschlagarmaturen die aus der Literatur ermittelte Rate verwendet. Die Betriebserfahrung weist jedoch darauf hin, daß sie zu hoch angesetzt ist.

#### 7.6.2 " S c h l i e ß t n i c h t "

Auch für die Ausfallart "schließt nicht" liefert die Betriebserfahrung wesentlich günstigere Werte als die verwendete Literatur. Mit den in Bild F3, A1-7 angegebenen Literaturstellen erhält man eine Verteilung mit Median  $\lambda_{50} = 2,5 \cdot 10^{-6}$  pro Stunde, Streufaktor  $K_{95} = 3$  und Erwartungswert  $\bar{\lambda} = 3,1 \cdot 10^{-6}$  pro Stunde. Literaturangaben, bei denen nicht zwischen den Ausfallarten unterschieden wird, wurden entsprechend Abschnitt 7.6.1 zu 65 % der Ausfallart "schließt nicht" zugerechnet.

Aus den Betriebserfahrungen im Anhang 2 ergibt sich 1 Ausfall auf eine Gesamtbeobachtungszeit von ca.  $2,6 \cdot 10^6$  Stunden. Dies führt auf einen um fast eine Zehnerpotenz günstigeren Schätzwert für die Ausfallrate. Für die Rechnungen der Phase A der Studie wurde dies noch nicht berücksichtigt.

#### 7.6.3 I n n e r e L e c k a g e

In Tabelle F3, A1-1 sind einige Literaturwerte für die Ausfallart "innere Leckage" angegeben. Diese Werte wurden jedoch nicht zur Ermittlung der Ausfallrate herangezogen, weil die Dichtheitsanforderungen an eine Armatur je nach ihrer Funktion im System unterschiedlich sein können und die Literaturstellen nicht erkennen lassen, wie der Ausfall definiert ist. Aus /F3, 7-34/



wurde ein Wert von  $1,1 \cdot 10^{-5}$  pro Stunde ermittelt. Als Ausfall wurden alle Fälle gewertet, bei denen eine Instandsetzung infolge zu großer Leckage durchgeführt wurde. Wegen der Unschärfe der Definition der Ausfallart wurde für die Risikostudie ein Medianwert von  $\lambda_{50} = 1,5 \cdot 10^{-5}$  pro Stunde festgelegt und die Unsicherheit durch einen großen Streufaktor von  $K_{95} = 10$  berücksichtigt. Dies führt auf einen Erwartungswert von  $\bar{\lambda} = 3,9 \cdot 10^{-5}$  pro Stunde, der deutlich ungünstiger ist als die Literaturwerte.

Aus der Betriebserfahrung (Anhang 2) erhält man bei gleicher Definition des Ausfalls wie in /F3, 7-34/ zwei Werte von  $2,6 \cdot 10^{-5}$  pro Stunde und  $4,2 \cdot 10^{-6}$  pro Stunde. Sie werden durch den oben bestimmten Wert gut abgedeckt.

#### 7.6.4 R ü c k s c h l a g a r m a t u r m i t M o t o r a n t r i e b

In der Literatur sind zu dieser Komponente kaum Angaben zu finden, die in Tabelle F3, A1-1 angegebenen Werte wurden aus /F3, 7-42/ ermittelt. Es wurden die Streufaktoren angesetzt, die sich für Rückschlagarmaturen ohne Antrieb ergeben. Die Ausfallraten gelten nur für die Armatur und stimmen etwa mit denen für Rückschlagarmaturen ohne Motorantrieb überein. Für die gesamte Komponente sind zu diesen Werten die Raten für den Elektromotor, die Ansteuerung und den Abzweig zu addieren.

In den Fehlerbaumanalysen kommen diese Komponenten bei der Absperrung der Druckspeicher vor. Da der Stempel des Motorantriebs in Bereitschaftsstellung aufgefahren ist, ist die Ausfallart "schließt nicht" von Interesse. Hierfür ergibt sich mit Antrieb, Ansteuerung und Abzweig eine Verteilung mit  $\lambda_{50} = 5 \cdot 10^{-6}$  pro Stunde,  $K_{95} = 4$  und  $\bar{\lambda} = 7,4 \cdot 10^{-6}$  pro Stunde. Zum Vergleich liefert die Betriebserfahrung (Anhang 2) für eine elektrisch absperrbare Rückschlagklappe einen Wert von  $4,3 \cdot 10^{-6}$  pro Stunde für die Ausfallart "Antrieb fährt weder auf noch zu".

Die Ausfallart "innere Leckage" wurde für den Fall, daß die Armatur motorisch zugehalten wird, etwas günstiger bewertet als bei Rückschlagarmaturen ohne Motorantrieb.

### 7.7 Handarmatur

Die Werte für Handarmaturen wurden aus Literaturangaben und Betriebserfahrungen ermittelt. Die zuletzt genannten Werte sind in Bild F3, A1-8 mit (B) gekennzeichnet. Sie stellen einen Zwischenstand der in Kapitel 6 dargestellten Auswertungen dar. Man erhält eine Verteilung mit  $\lambda_{50} = 1,5 \cdot 10^{-6}$  pro Stunde,  $K_{95} = 12$  und  $\bar{\lambda} = 4,7 \cdot 10^{-6}$  pro Stunde.

Zum Vergleich werden nur die Werte für "öffnet nicht" im Anhang 2 herangezogen, weil die Ausfälle für "schließt nicht" zum großen Teil auf dieselben Schäden zurückgehen. Daraus erhält man eine Verteilung mit  $\lambda_{50} = 1,7 \cdot 10^{-6}$  pro Stunde,  $K_{95} = 5,7$  und  $\bar{\lambda} = 3 \cdot 10^{-6}$  pro Stunde. Die Betriebserfahrung liefert bei wesentlich geringerer Streuung einen etwas günstigeren Erwartungswert.

### 7.8 Regelarmatur

Die Verteilungen für die Ausfallarten "fährt nicht auf" und "fährt nicht zu" sind mit den verwendeten Literaturstellen in Bild F3, A1-9 wiedergegeben. Soweit in den Literaturstellen nicht nach den Ausfallarten unterschieden wurde, wurden die Ausfallraten im Verhältnis 1 : 1 auf die Ausfallarten aufgeteilt. In beiden Fällen ergeben sich Verteilungen mit  $\lambda_{50} = 5 \cdot 10^{-6}$  pro Stunde,  $K_{95} = 7$ ,  $\bar{\lambda} = 1 \cdot 10^{-5}$  pro Stunde. Diese Raten wurden in den Fehlerbaumanalysen für die Armatur mit Antrieb verwendet.

Die Werte aus Betriebserfahrungen im Anhang 2 enthalten darüber hinaus den Abzweig und die Regelung. In den Fehlerbaumanalysen der Risikostudie kommt eine Regelarmatur mit Regelung nicht vor.

Die Regelung bleibt in den untersuchten Fällen außer Betracht, weil der Reaktorschutz mit Vorrang eingreift oder die Regelung ohnehin als ausgefallen unterstellt wird, da sie nicht für Störfallbedingungen ausgelegt ist. Damit ist keine unmittelbare Vergleichsmöglichkeit gegeben. Vergleicht man den in der Studie verwendeten Wert trotz der unterschiedlichen Komponentenabgrenzung mit den Werten aus der Betriebserfahrung, dann ergibt sich das folgende Bild: Von den drei Populationen, für die im Anhang 2 Ergebnisse angegeben sind, weist die erste einen deutlich geringeren Wert auf, die zweite erlaubt auf der Basis von null Ausfällen eine Abschätzung, die mit den in der Studie verwendeten Raten gut übereinstimmt, während die dritte einen deutlich höheren Wert liefert.

#### 7.9 Sicherheits- und Entlastungsventile

Die aus der Literatur entnommenen Werte für die Ausfallarten "öffnet nicht", "schließt nicht" und "öffnet unbeabsichtigt" sind in den Tabellen F3, A1-1 und -2 wiedergegeben. Soweit in den Literaturstellen nicht nach Ausfallarten unterschieden wurde, wurden sie im Verhältnis 2 : 6 : 2 auf die drei Ausfallarten aufgeteilt, das sich aus den Daten von /F3, 7-42/ ergibt. Die resultierenden Verteilungen sind in Bild F3, A1-10 dargestellt.

In den Fehlerbaumanalysen der Risikostudie spielen die betrachteten Ausfallarten für die Sicherheitsventile der Frischdampfleitungen sowie für die Entlastungs- und Sicherheitsventile am Druckhalter eine Rolle. Aus bisherigen Betriebserfahrungen ist bekannt, daß das Ausfallverhalten solcher Ventile sehr von Einzelheiten der jeweiligen Auslegung abhängt. Das ergibt sich z.B. aus /F3, 7-43/, wo Ausfälle von Sicherheits- und Entlastungsventilen in amerikanischen Kernkraftwerken untersucht werden. Auch in den Fällen, in denen Abblaseventile am Druckhalter offen blieben (Abschnitt 3.1.2), sind Anlagen eines Herstellers weit überproportional vertreten. Da den Literaturstellen häufig keine Einzelheiten zu Ventiltyp und Ausfallart zu entnehmen sind, bestehen bei den Literaturwerten zu Sicherheits- und Ent-

lastungsventilen relativ große Unsicherheiten hinsichtlich der Übertragbarkeit.

Daher wurden die aus der Literatur ermittelten Verteilungen für die Ausfallarten "öffnet nicht" und "schließt nicht" nicht für die Fehlerbaumanalysen verwendet. Hierfür wurden anhand der bisher aufgetretenen Anforderungen an die Frischdampf-Sicherheitsventile im Kernkraftwerk Biblis Ausfallwahrscheinlichkeiten abgeschätzt. Es zeigt sich, daß diese Abschätzungen relativ gut mit den Erwartungswerten der Literaturdaten übereinstimmen. Die für die Frischdampf-Sicherheitsventile abgeschätzten Werte wurden auch für die anderen Sicherheits- und Entlastungsventile verwendet, für die nicht ausreichende Anforderungen vorlagen, um gesonderte Abschätzungen vorzunehmen. Für die Ausfallart "öffnet unbeabsichtigt" wurde die aus der Literatur ermittelte Rate verwendet. Dies ist angesichts der ausreichenden Übereinstimmung, die sich in den beiden anderen Ausfallarten ergab, gerechtfertigt.

Für die beiden Blöcke des Kernkraftwerks wurden vom Betreiber die folgenden Anforderungszahlen mitgeteilt:

- 20 Ventilprüfungen; bei jeder Prüfung wird jedes der drei Vorsteuerventile gesondert betätigt, d.h., das Hauptventil wird insgesamt dreimal geöffnet. Da diese Anforderungen kurz aufeinanderfolgen, wurden sie als eine gewertet. Aus den Prüfungen folgen damit 60 Anforderungen an Vorsteuerventile und 20 an Hauptventile.
- 40 betriebliche Anforderungen, bei denen in der Regel zwei Sicherheitsventile im Verlauf einer Viertelstunde etwa 10mal öffnen. Auch dieses mehrfache Öffnen wurde jeweils nur als eine Anforderung gewertet. Wieviele Vorsteuerventile jeweils öffnen, wird nicht registriert. Da die Ansprechwerte um etwa 1 bis 2 bar streuen können, wurde unterstellt, daß jeweils nur ein Vorsteuerventil öffnete. Damit erhält man jeweils 80 betriebliche Anforderungen für Haupt- und Vorsteuerarmaturen.

Bei den Prüfungen und betrieblichen Anforderungen wurde kein Versagen beobachtet. Ein Versagen würde unmittelbar bemerkt werden, ebenso ein Ausfall in Offenstellung bei den betrieblichen Anforderungen. Sollte sich dagegen bei einer betrieblichen Anforderung ein Vorsteuerventil nicht öffnen, dann würde dies nicht unbedingt bemerkt; die Hauptarmatur würde durch Öffnen eines redundanten Vorsteuerventils betätigt. Ein Fehler, der zum Nichtöffnen des Ventils führt, würde jedoch bei der nächsten Prüfung entdeckt. Da solche Fehler nicht auftraten, wurden für die Abschätzung unbemerkte Ausfälle in geschlossener Stellung ausgeschlossen.

Aus diesen Angaben wurden die folgenden oberen Abschätzungen abgeleitet:

- Für die Kombination Hauptventil mit einem Vorsteuerventil wurden die Ausfallarten "öffnet nicht" und "schließt nicht" mit einem Erwartungswert von  $1 \cdot 10^{-2}$  angesetzt. Das entspricht dem Schätzwert, den man bei den vorliegenden 100 Anforderungen bei einem Ausfall erhalten würde. Für die Rechnungen wurde eine logarithmische Normalverteilung mit dem Median  $P_{50} = 7 \cdot 10^{-3}$  und dem Streufaktor  $K_{95} = 4$  verwendet. Der Faktor 4 entspricht etwa dem Verhältnis von 95%- und 50%-Wert einer  $\chi^2$ -Verteilung bei null Ausfällen.
- Dieselben Werte wurden für ein Hauptventil mit mehreren Vorsteuerventilen für die Ausfallart "schließt nicht" verwendet, weil unterstellt wird, daß bei der Anforderung jeweils nur ein Vorsteuerventil öffnet.
- Für die Ausfallart "öffnet nicht" ist bei mehreren Vorsteuerventilen ein günstigerer Wert zu erwarten. Wegen der Redundanz der Vorsteuerventile ist praktisch nur die Ausfallwahrscheinlichkeit der Hauptarmatur von Belang. Bei gegebener Anzahl von Anforderungen lassen sich jedoch für Teile einer Komponente keine kleineren Schätzwerte ableiten als für die Komponente insgesamt. Der Tatsache, daß hier ein günstigerer Wert plausibel ist, wurde dadurch Rechnung getragen, daß mit  $7 \cdot 10^{-3}$  der 50%-Wert der  $\chi^2$ -Verteilung für 100 Anforderungen und null Ausfälle als Erwartungswert angesetzt wurde.

Für die Rechnungen wurde eine logarithmische Normalverteilung mit dem Median  $P_{50} = 4 \cdot 10^{-3}$  und dem Streufaktor  $K_{95} = 6$  verwendet. Der größere Streufaktor berücksichtigt, daß sich bei der Summierung von Ausfallraten die Streuung reduziert.

- Für ein einzelnes Vorsteuerventil wurde ein Median  $P_{50} = 4 \cdot 10^{-3}$  und ein Streufaktor  $K_{95} = 6$  angesetzt. Der Erwartungswert von  $\bar{P} = 7 \cdot 10^{-3}$  entspricht dem Schätzwert, den man bei den vorliegenden 140 Anforderungen bei 1 Ausfall erhalten würde.

Aus der in Bild F3, A1-10 dargestellten Literaturlauswertung ergeben sich für die Ausfallarten "öffnet nicht" und "schließt nicht" Erwartungswerte der Ausfallraten von  $\bar{\lambda} = 1,2 \cdot 10^{-6}$  pro Stunde und  $5,2 \cdot 10^{-6}$  pro Stunde. Unterstellt man eine Anforderungshäufigkeit von 1 pro Jahr, was allein schon durch die Prüfungen gegeben ist, dann entspricht dies bei Zugrundelegung des halben Prüflntervalls Ausfallwahrscheinlichkeiten pro Anforderung von  $5 \cdot 10^{-3}$  bzw.  $2,2 \cdot 10^{-2}$ . Angesichts der dargestellten Unsicherheiten der Übertragbarkeit kann dies als gute Übereinstimmung gewertet werden. Dabei ist zu berücksichtigen, daß die Abschätzungen aus der Betriebserfahrung auf null Ausfällen basieren, so daß die tatsächlichen Werte auch deutlich niedriger liegen können.

Wegen der für die beiden betrachteten Ausfallarten ermittelten guten Übereinstimmung erscheint es gerechtfertigt, die Werte für die Ausfallart "öffnet unbeabsichtigt" der Literatur zu entnehmen. Es ergibt sich eine logarithmische Normalverteilung mit dem Median  $\lambda_{50} = 2 \cdot 10^{-6}$  pro Stunde und dem Streufaktor  $K_{95} = 7$ , was einem Erwartungswert von  $\bar{\lambda} = 3,6 \cdot 10^{-6}$  pro Stunde entspricht.

Anzumerken ist, daß die im Anhang 2 angegebenen Zahlen für Sicherheitsventile hier nicht herangezogen werden können. Es handelt sich um Ventile kleiner Nennweite zur Absicherung wasserführender Rohrleitungen. Diese Armaturen sind mit den hier betrachteten nicht vergleichbar.

Die obigen Ausführungen zeigen, daß die weitere Auswertung von Betriebserfahrungen mit Sicherheits- und Entlastungsventilen erforderlich ist. Ein entsprechendes Projekt wurde in der Zwischenzeit in Zusammenarbeit mit dem TÜV Rheinland begonnen. Für die Phase B der Studie werden hieraus Ergebnisse verfügbar sein.

#### 7.10 Rohrleitungen

Die in der Literatur verfügbaren Ausfalldaten von Rohrleitungen weisen im Vergleich zu anderen Komponenten besonders große Unsicherheiten auf. Die Autoren verwenden unterschiedliche, nicht ohne weiteres vergleichbare Schadensdefinitionen. Material, Betriebsbedingungen, Qualitätsanforderungen und andere Parameter sind unterschiedlich und häufig nicht genau bekannt. Die Rohrleitungslänge, auf die sich beobachtete Fehler beziehen, liegt zum Teil nicht eindeutig fest. Das bei anderen Komponenten angewandte Vorgehen, die Streuung der aus verschiedenen Quellen bekannten Daten durch eine Verteilung zu berücksichtigen, ohne eine Wertung der Einzeldaten vorzunehmen, erscheint bei Rohrleitungen daher für eine verlässliche Abschätzung der Ausfallwahrscheinlichkeit nicht geeignet.

Von wesentlicher Bedeutung ist das Versagen von Rohrleitungen in der Risikostudie als auslösendes Ereignis für Kühlmittelverluststörfälle. Hierfür wurde in Abschnitt 3.1.1 eine Abschätzung vorgenommen. Sie verwendet die Ergebnisse einer Reihe dort aufgeführter Autoren, stützt sich für kleine Bruchquerschnitte jedoch im wesentlichen auf die vorliegenden Betriebserfahrungen kommerzieller Leistungsreaktoren. Da keine Kühlmittelverluste der betrachteten Art auftraten, handelt es sich um eine obere Abschätzung. Die Werte für große Bruchquerschnitte basieren auf den diskutierten Literaturstellen und einer Bewertung der relativen Wahrscheinlichkeit von Brüchen unterschiedlichen Querschnitts. Für die Abschätzungen werden mit  $K_{95} = 10$  große Streufaktoren angesetzt.

Außer im Zusammenhang mit Kühlmittelverluststörfällen spielen Versagenswahrscheinlichkeiten von Rohrleitungen in den Störfallablauf- und Fehlerbaumanalysen der Risikostudie eine untergeordnete Rolle. Es genügt jeweils die Angabe einer ungefähren Größenordnung. Daher wurden für die Phase A der Studie keine vertieften Untersuchungen zur Versagenswahrscheinlichkeit von Rohrleitungen durchgeführt. Mit einer für den vorliegenden Zweck ausreichenden Genauigkeit kann aus den in Tabelle F3, A1-1 angegebenen Literaturwerten ein Bereich von etwa  $10^{-11}$  pro Meter und Jahr bis  $10^{-8}$  pro Meter und Jahr entnommen werden. Für die Analysen wurde ein Wert von  $10^{-9}$  pro Meter und Jahr verwendet. Auf die Angabe einer Verteilung wurde wegen der vorhandenen Unsicherheiten verzichtet.

## 7.11 Notstromdiesel

### 7.11.1 Startversagen

Für die Ermittlung der Wahrscheinlichkeit, daß ein Notstromdiesel auf Anforderung nicht startet, bietet die große Anzahl von Dieselstarts bei Funktionsprüfungen in den deutschen Kernkraftwerken eine gute statistische Basis. Die für die Risikostudie verwendeten Werte wurden daher aus diesen Erfahrungen abgeleitet, Angaben aus der Literatur sind nur zum Vergleich in Tabelle F3, A1-1 angegeben.

Betrachtet wird das gesamte Notstromaggregat, d.h. die Dieselmachine mit Ansteuerung, Regelung, Kraftstoffsystem, Anlaßsystem, Kühlung, soweit sie dem Diesel unmittelbar zugeordnet ist, und der Generator. Die Unsicherheiten in der technischen Beurteilung sind im Vergleich zu anderen Komponenten gering. Folgende Punkte sind zu nennen:

- Bei einzelnen Fehlern bestehen Zweifel, ob sie zum Ausfall des Aggregats geführt hätten. In diesen Fällen wurde ein Ausfall unterstellt. Es wurden auch die Fehler berücksichtigt, die den Start des Aggregats nicht verhindern, jedoch zu einem Ausfall nach kurzem Lauf führen würden.



- Die genaue Anzahl des Starts war nicht in allen Fällen zu klären, da außer den regelmäßigen Prüfungen Probestarts, z.B. nach Wartungsarbeiten, und Starts bei Anforderungen zu berücksichtigen sind. Es wurden vergleichbare Verhältnisse unterstellt wie bei den Aggregaten, für die vollständige Angaben vorlagen.
- Die Aggregate unterscheiden sich technisch, z.B. hinsichtlich des Anlaßsystems. Für die Ermittlung der Ausfallwahrscheinlichkeit wurden alle Aggregate herangezogen.

Es ergibt sich bei 24 Ausfällen und ca. 810 Starts ein Erwartungswert von  $\bar{P} = 3 \cdot 10^{-2}$  für die Ausfallwahrscheinlichkeit bei Anforderung. Für die zugehörige Verteilung wurde ein Median von  $\lambda = 2,5 \cdot 10^{-2}$  und ein Streufaktor  $K_{95} = 3$  verwendet. Der Streufaktor wurde aufgrund der Schwankungen zwischen den Werten für die einzelnen Kernkraftwerke abgeschätzt. Die verwendeten Werte stimmen gut mit denen von WASH-1400 überein; in der Literatur werden zum Teil deutlich günstigere Werte angegeben.

#### 7.11.2 Betriebsversagen

Notstromdiesel stehen in Kernkraftwerken normalerweise in Bereitschaft, ihre Betriebszeiten, hauptsächlich aufgrund von Prüfungen, sind im Vergleich zur Bereitschaftszeit kurz. Es ist daher anzunehmen, daß ein Teil der Ausfälle, die innerhalb dieser relativ kurzen Betriebszeiten auftreten, auf Ursachen zurückzuführen ist, die bereits während des Bereitschaftszustandes vorlagen. Ermittelt man daher eine Ausfallrate, indem man die aufgetretenen Fehler auf die akkumulierte Betriebszeit bezieht, dann ist diese Rate nur für kurze Betriebszeiten im Bereich weniger Stunden anwendbar. Eine Übertragung dieser Ausfallrate auf längeren Betrieb, z.B. über einige Tage, erscheint problematisch. Für die Analysen der Risikostudie sind Ausfallraten für einen Zeitraum von ca. 2 Stunden nach Anforderung der Diesel von Bedeutung. Die Ermittlung einer Ausfallrate auf die beschriebene Art ist daher angemessen.

Über einen Zeitraum von 2,5 Jahren wurden 35 Aggregate betrachtet, die in Kernkraftwerken im Einsatz waren, einige nur über einen Teil dieser Zeit. Aus den bekannten Betriebsstunden von 11 Aggregaten ergab sich eine mittlere Betriebszeit von 76 Stunden pro Aggregat und Jahr. Da die Betriebszeiten für die restlichen Aggregate nicht bekannt waren, wurden pessimistisch 50 Stunden pro Aggregat und Jahr zugrunde gelegt. Dies führt zu einer Gesamtbetriebszeit von 3740 Stunden. Es traten 17 Ausfälle während des Betriebes auf; dies ergibt eine Ausfallrate von  $4,5 \cdot 10^{-3}$  pro Stunde. Die Streuung zwischen verschiedenen Anlagen ist gering. Für die Rechnungen wurde eine Verteilung mit dem Median  $\lambda_{50} = 5 \cdot 10^{-3}$  pro Stunde und einem Streufaktor  $K_{95} = 2$  verwendet.

Aus Tabelle F3, A1-2 ist ersichtlich, daß in der Literatur überwiegend günstigere Werte angegeben sind. In /F3, 7-44/ werden auf der Basis einer relativ umfangreichen Statistik für intermittierenden Betrieb Ausfallraten von  $3,5 \cdot 10^{-3}$  pro Stunde und  $1,2 \cdot 10^{-3}$  pro Stunde genannt, für kontinuierlichen Betrieb  $2 \cdot 10^{-3}$  pro Stunde.

### 7.11.3 "Common mode" - Ausfälle

Ausfälle mit gemeinsamer Ursache können zu einem gleichzeitigen Ausfall mehrerer Aggregate führen. Da die vorhandene Redundanz dadurch unwirksam wird, kann die Zuverlässigkeit des Systems durch solche "common mode"-Ausfälle bestimmt werden, auch wenn ihre Wahrscheinlichkeit wesentlich geringer ist als die für den unabhängigen Ausfall einzelner Diesel. Für Notstromdiesel sind "common mode"-Ausfälle zu berücksichtigen, da sowohl in deutschen als auch in ausländischen Anlagen Ausfälle beobachtet wurden, deren Ursachen mehrere Aggregate betrafen.

Von den in der Bundesrepublik aufgetretenen Fällen mit Ausfall von mehr als einem Diesel ist keiner auf die Referenzanlage anwendbar. Sie waren zurückzuführen auf:

- Ausfall der gemeinsamen Kühlwasserversorgung. Die Diesel der Referenzanlage haben jeweils eine unabhängige Kühlwasserversorgung.
- Alterung von Starterbatterien. Die Referenzanlage hat keine elektrischen, sondern Preßluft-Startsysteme, die den einzelnen Dieseln zugeordnet sind.
- Versagen des synchronen Hochlaufens von Aggregaten, die auf eine gemeinsame Schiene speisen. Die Notstromgeneratoren der Referenzanlage speisen auf je eine eigene Schiene.

Weiter traten Fälle auf, bei denen nur ein Diesel ausfiel, jedoch aufgrund von Ursachen, die auch zum Ausfall redundanter Maschinen hätte führen können:

- Bruch der Welle eines Turboladers infolge Materialfehlers,
- unzureichende Kühlung infolge Ablagerung eines Korrosionsschutzmittels.

Die quantitative Bewertung dieser Ereignisse ist schwierig, weil nicht angebbbar ist, mit welcher Wahrscheinlichkeit bei einer Anforderung gleichzeitig mehrere oder gar alle Diesel ausgefallen wären.

Zur Abschätzung der Wahrscheinlichkeit eines Ausfalls mehrerer Notstromdiesel gleicher Ursache wurde daher wie folgt vorgegangen:

- Bezogen auf die vorliegende Anzahl von Starts wird 1 Ausfall aus einer gemeinsamen Ursache angesetzt.
- Es wird unterstellt, daß der Ausfall zur gleichzeitigen Nichtverfügbarkeit aller vier Diesel führt.

Gewertet wird dabei entweder der Start einer einzelnen Maschine oder der gleichzeitige Start mehrerer Maschinen. Mit dieser Definition ergab sich eine Anzahl von ca. 770 Starts<sup>1)</sup>. Dies führt zu einer Wahrscheinlichkeit von  $1,3 \cdot 10^{-3}$  pro Anforderung.

---

<sup>1)</sup> Die Abschätzung wurde im Juni 1978 durchgeführt. In der Zwischenzeit hat sich die Zahl der Starts nahezu verdoppelt. Auf die Referenzanlage anwendbare Ausfälle aus gemeinsamer Ursache traten nicht auf.

Auf ein ähnliches Ergebnis führt eine amerikanische Auswertung von Dieselausfällen /F3, 7-45/. Dort werden bei 2940 Starts sechs Ausfälle als potentielle "Common mode"-Ausfälle betrachtet. In WASH-1400 wird ebenfalls ein Wert von  $1 \cdot 10^{-3}$  verwendet.

Für die Durchführung der Fehlerbaumrechnungen wurde der oben abgeschätzte Wert in eine Ausfallwahrscheinlichkeit je Start und in eine Ausfallrate im Betrieb aufgespalten. Auf die Ergebnisse der Rechnungen hat diese Aufteilung keinen Einfluß, weil sie bei der Betriebszeit von 2 Stunden, wie sie in den Rechnungen betrachtet wird, den oben abgeschätzten Erwartungswert nicht verändert. Es wurden Verteilungen mit den Medianwerten  $p_{50} = 2 \cdot 10^{-4}$  pro Start und  $\lambda_{50} = 1,5 \cdot 10^{-4}$  pro Stunde und jeweils dem Streufaktor 10 verwendet.

#### 7.12 Steuerstäbe

Zur Ermittlung einer Ausfallrate für die Ausfallart "Steuerstab fällt nicht ein" wurden die Betriebserfahrungen mit Steuerstäben in KWU-Druckwasserreaktoren ausgewertet. Diese Steuerstäbe entsprechen sowohl hinsichtlich der Bauart (Antrieb durch magnetischen Klinkenschrittheber) als auch hinsichtlich der Herstellungs- und Prüfverfahren weitgehend denen der Referenzanlage. Der Literatur entnommene Werte sind in Tabelle F3, A1-1 angegeben. Da hier jedoch einerseits Unsicherheiten bezüglich der Übertragbarkeit bestehen, andererseits die Betriebserfahrungen mit KWU-Steuerstäben ausreichende Daten liefern, werden die Werte aus der Literatur für die Zuverlässigkeitsanalyse des mechanischen Systems zur Reaktorschnellabschaltung nicht verwendet.

Die Daten wurden auf Anfrage durch die Betreiber von Kernkraftwerken mit insgesamt vier KWU-Druckwasserreaktoren geliefert und beziehen sich auf Reaktorschnellabschaltungen in einem Lastbereich von 0 bis 100 %. Während die bei Nulllast fehlende Aufwärmespanne im Reaktorkern keinen wesentlichen Einfluß auf die

Fallzeiten der Steuerstäbe hat, bewirkt die bei Nulllast erhöhte Dichte nachweisbar längere Fallzeiten. Die Reaktorschnellabschaltungen bei Nulllast werden daher als vollwertige Funktionsanforderungen betrachtet. Die Betriebszeiten wurden aus den Betriebsstatistiken in /F3, 7-46/ abgeschätzt. Aus den Betriebszeiten und der Anzahl der Steuerstäbe jedes Kernkraftwerkes wurde die Gesamtzahl der Steuerstab-Betriebsstunden zu  $5,1 \cdot 10^6$  Stunden ermittelt. Während der genannten Betriebszeiten wurde bei den betrachteten Reaktorschnellabschaltungen kein Ausfall beobachtet. Nach Abschnitt 6.3.1 ergibt sich damit als Schätzwert für den 50%- bzw. 95%-Wert der Ausfallrate:

$$\lambda_{50} = 1,4 \cdot 10^{-7} \quad \text{pro Stunde}$$
$$\lambda_{95} = 6 \cdot 10^{-7} \quad \text{pro Stunde}$$

Den Werten entspricht ein Unsicherheitsfaktor von  $K_{95} = 4$  und ein Erwartungswert der Ausfallrate von  $\bar{\lambda} = 2 \cdot 10^{-7}$  pro Stunde.

Aus den insgesamt ca. 14 000 Stabeinfällen kann auch eine Ausfallwahrscheinlichkeit pro Anforderung (Reaktorschnellabschaltung) für das Nichteinfallen eines Steuerstabes ermittelt werden:

$$p_{50} = 5 \cdot 10^{-5}$$
$$K_{95} = 4$$
$$p = 7 \cdot 10^{-5}$$

Ob das Ausfallverhalten der Steuerstäbe besser durch eine konstante Ausfallrate oder durch eine konstante Ausfallwahrscheinlichkeit pro Anforderung gekennzeichnet wird, kann derzeit nicht beurteilt werden. In der Zuverlässigkeitsanalyse für das mechanische System zur Reaktorschnellabschaltung wird die konstante Ausfallrate verwendet: Es ergibt sich damit für die Systemfunktion "Reaktorschnellabschaltung" ein höherer Wert der Ausfallwahrscheinlichkeit bei Anforderung, als wenn für den Steuerstab die konstante Ausfallwahrscheinlichkeit zugrunde gelegt wird (Fachband 2).

Neuere Auswertungen zu Steuerstäben im Kernkraftwerk Biblis, Block A (1/77 bis 3/78) und Block B (2/77 bis 3/78) führen bei späteren Ausfällen zu einem nur unwesentlich geänderten Wert für die Null-Ausfallrate:

$$\lambda_{50} = 1,1 \cdot 10^{-7} \text{ pro Stunde}$$

### 7.13 Sonstige Komponenten

Zu den restlichen in Tabelle F3, 7-1 angegebenen Daten ist folgendes anzumerken:

- Elektromotoren

In den Fehlerbaumanalysen sind mit wenigen Ausnahmen die Elektromotoren mit den Betriebsmitteln zusammengefaßt, die von ihnen angetrieben werden, z.B. Pumpen oder Armaturen. In diesen Fällen sind keine gesonderten Daten für Elektromotoren erforderlich. Auch bei der Auswertung der Betriebserfahrungen wurde nicht nach Antrieb und angetriebenem Betriebsmittel differenziert. Die Abschnitte 7.2 und 7.3 zeigen, daß für Pumpen und Motorarmaturen jeweils einschließlich Antrieb gute Übereinstimmung zwischen den für die Rechnungen verwendeten Daten und der Betriebserfahrung besteht. Die Werte für Elektromotoren basieren auf den in Tabelle F3, A1-1 angegebenen Literaturstellen. Soweit dabei nicht zwischen Startversagen und Ausfall im Betrieb unterschieden wurde, wurden diese Summenraten im Verhältnis 30 : 70 auf die beiden Ausfallraten aufgeteilt. Das Verhältnis ergibt sich aus den Auswertungen von /F3, 7-34/. Die sich ergebenden Verteilungen sind in den Bildern F3, A1-11 und -12 dargestellt.

- Umschaltventil

Das eigenmediumbetätigte Umschaltventil in der Hochdruckeinspeiseleitung schaltete innerhalb von 30 Sekunden bei 126 Funktionsprüfungen 12mal nicht um, wie es nach Herstellerrechnungen zur Erfüllung seiner Funktion im Störfall erforderlich ist. Es

ließ sich nicht eindeutig klären, inwieweit diese Fehlfunktion auf das Prüfverfahren zurückzuführen ist bzw. inwieweit sie auch im Störfall zu erwarten wäre. Für die Bestimmung der Ausfallwahrscheinlichkeit wurden alle Fälle mit Umschaltzeiten über 30 Sekunden als Versagen der Umschaltung gewertet. Damit ergibt sich ein Erwartungswert von  $\bar{P} = 9,5 \cdot 10^{-2}$ , für die Rechnung wurde eine Verteilung mit dem Median  $P_{50} = 4 \cdot 10^{-2}$  und einem Streufaktor  $K_{95} = 10$  verwendet. Die Auswirkung von Änderungen an der Armatur konnte in der Auswertung noch nicht berücksichtigt werden. Für spätere Betrachtungszeiten ist mit einer deutlichen Reduzierung der Ausfallwahrscheinlichkeit zu rechnen.

- Frischdampf-Schnellschlußschieber

Die Ausfallrate für die Ausfallarten "öffnet nicht" und "schließt nicht" wurde auf der Basis von 112 Anforderungen in Betrieb ermittelt, wobei kein Ausfall auftrat. Hieraus wurde eine Verteilung mit Median  $P_{50} = 6 \cdot 10^{-3}$  und Streufaktor  $K_{95} = 4$  abgeschätzt. Die Rate gilt für die Armatur ohne die zugehörigen Steuerventile.

- Abzweige

In den Fehlerbäumen werden Abzweige gesondert ausgewiesen, in den Ergebnissen ist jedoch nur die Summe der Raten für den Abzweig und das darüber versorgte Betriebsmittel von Bedeutung. Aus den Betriebserfahrungen wurden ebenfalls nur Werte für diese Summe ermittelt. Aus den Abschnitten 7.2 und 7.3 ist ersichtlich, daß hierfür eine gute Übereinstimmung mit den Betriebserfahrungen besteht. Literaturwerte für Abzweige liegen nicht vor. Die in Tabelle F3, 7-1 angegebenen Werte basieren auf einer technischen Bewertung. Diese Abschätzung, nach der ca. 20 % der Ausfälle von Pumpen oder Motorarmaturen mit Antrieb und Abzweig auf den letzteren entfallen, ist als pessimistisch anzusehen. Hierfür spricht auch der Vergleich mit anderen Betriebsmitteln, wie Leistungsschalter oder Schütze. Die Unsicherheit der Abschätzung wird durch einen Streufaktor  $K_{95} = 10$  berücksichtigt. Abzweige beinhalten u.a. auch eine Sicherung. Sofern in den

Analysen Werte für unbeabsichtigte Unterbrechung wegen Ausfalls der Sicherung benötigt werden, wird hierfür die volle Rate des Abzweiges eingesetzt. Kabelverbindungen sind gegenüber dem Abzweig vernachlässigbar.

- Leistungsschalter

Die Werte für Leistungsschalter wurden aufgrund der in Tabelle F3, A1-1 angegebenen Literaturstellen ermittelt. Soweit es sich nicht klären ließ, wurde unterstellt, daß in diesen Werten der Abzweig nicht enthalten ist. Daten, bei denen nicht zwischen den Ausfallarten "öffnet nicht" und "schließt nicht" unterschieden wurde, wurden diesen Ausfallarten im Verhältnis 30 : 70 zugeordnet, die sich aus /F3, 7-34/ ergeben. Die Verteilungen sind in Bild F3, A1-13 dargestellt.

- Generatorschalter

Die Ausfallrate für die Ausfallart "öffnet nicht" von Generatorschaltern wurde aufgrund einer von der Herstellerfirma BBC zur Verfügung gestellten Betriebsstatistik ermittelt. Dieser Statistik zufolge waren Mitte 1977 in der Bundesrepublik Deutschland insgesamt 50 Schaltergruppen mit einer Gesamtbetriebszeit von 166 Jahren in Kraftwerken im Einsatz. Es trat kein Ausfall an den Generatorschaltern auf, der zu einem Öffnungsversagen führte. Die Verwendung der aus der Gesamtbetriebszeit ermittelten Ausfallrate stellt eine pessimistische Vorgehensweise dar, im Vergleich zur Verwendung der Ausfallwahrscheinlichkeit pro Anforderung, die man aufgrund der durchgeführten 13 000 Lastspiele erhält. Der Grund hierfür ist, daß bei den in der Statistik enthaltenen Generatorschaltern von konventionellen Kraftwerken im allgemeinen wesentlich häufiger Schaltvorgänge durchgeführt werden als bei Kernkraftwerken.

Die Daten für die restlichen in Tabelle F3, 7-1 aufgeführten Komponenten wurden aufgrund der in Tabelle F3, A1-1 angegebenen Literaturstellen ermittelt. Die sich ergebenden Verteilungen sind in den Bildern F3 A1-14 bis -16 wiedergegeben.



## 8. ZUVERLÄSSIGKEITSKENNGRÖSSEN FÜR LEITTECHNISCHE KOMPO- NENTEN

### 8.1 Ausfallratenermittlung durch Literaturlauswertung

#### 8.1.1 Allgemeines

Für einige Komponenten der Leittechnik blieb nur die Möglichkeit der Literaturlauswertung, um genügend gesicherte Ausfallraten angeben zu können, da direkt auswertbare Betriebserfahrungen noch nicht in ausreichender Form vorlagen. Diese Komponenten (Differenzdruck- bzw. Druckmeßumformer und Relais) sind in der Datenliste in Anhang 3 besonders gekennzeichnet. Die Literaturstellen wurden in erster Linie dahingehend ausgewählt, ob die enthaltenen Informationen auswertbar und vor allem glaubhaft sind (z.B. Angaben über die untersuchte Population). Sicherlich kann man bei vielen Komponenten der Leittechnik auf eine jahrelange Erfahrung zurückgreifen. Es erschien jedoch sinnvoll, sich auf kraftwerksspezifische Literatur zu beschränken, da Ausfallarten und Umgebungsbedingungen vergleichbar sein sollten.

Im Gegensatz dazu ist die Ausfallratenermittlung für elektronische Bauelemente, wie z.B. Transistor oder Widerstand, weit weniger problematisch. Die Ausfallraten dieser Bauelemente werden für die Ausfalleffektanalyse von Elektronikarten in leittechnischen Systemen (Abschnitt 8.3) benötigt. Hier kann man auf Literatur zurückgreifen, die gut übereinstimmende Ergebnislisten langjähriger Tests mit sehr großen Bauelementstückzahlen beinhaltet. Die Zuverlässigkeitskenngrößen für diese Bauelemente werden als bekannt vorausgesetzt, sind daher im folgenden nicht weiter behandelt und in der Tabelle der Leittechnikdaten (Anhang 3 nicht gesondert aufgeführt. In Abschnitt 8.2 werden zusätzlich neue Methoden zur Ermittlung von Bauelementausfallraten vorgestellt.

### 8.1.2 Verwendete Auswertemethoden

In WASH-1400 kommen nur wenige Komponentendaten aus der Leittechnik zur Anwendung. Durch anderen Aufbau der Steuerungsebene und durch Zusammenfassungen bei der Fehlerbaumanalyse bedingt, werden nur Ausfallraten für Relais (4 Ausfallarten), Sicherungen und eine allgemeine Ausfallrate für Meßkanäle jeglicher Art benötigt. Die verwendeten Daten wurden, wie die Daten der verfahrenstechnischen Komponenten, aus Literaturquellen und nuklearer Betriebserfahrung gewonnen. Als Basis für die Abschätzung des Medianwertes diente der Wert aus der nuklearen Betriebserfahrung. Der 5%- und der 95%-Wert der angenommenen logarithmischen Normalverteilung wurde so gewählt, daß ca. 90 % der Daten aus der Literatur innerhalb dieses Vertrauensintervalls liegen und der Vertrauensbereich je nach Streuung der Daten eine oder zwei Größenordnungen überstreicht. Die resultierende logarithmische Normalverteilung hat somit Streufaktoren von 3 oder 10.

In Anlehnung an dieses Verfahren wurde die ausgewählte Literatur für die obengenannten Leittechnikdaten ausgewertet. Der Medianwert der angenommenen logarithmischen Normalverteilung wurde entsprechend der Vorgehensweise in Kapitel 5 ermittelt, der Streufaktor analog zu WASH-1400 bewertet. Die Annahme, daß Ausfallraten logarithmisch normalverteilt sind, kann mittels der Eintragung der Summenhäufigkeitskurve der einzelnen Literaturdaten in ein doppeltlogarithmisches Wahrscheinlichkeitsnetz überprüft werden (Bilder F3, A1-17 und -18). Sofern sich eine Gerade durch die einzelnen Punkte legen läßt, kann davon ausgegangen werden, daß eine logarithmische Normalverteilung vorliegt, was auch in den gezeigten Beispielen der Fall ist. Für die nicht bildlich dargestellten Ausfallratenverteilungen kann ein ähnliches Verhalten beobachtet werden, so daß hier ebenfalls eine logarithmisch normalverteilte Ausfallrate unterstellt werden kann. Die für spezielle Ausfallarten benötigten Daten der leittechnischen Komponenten sind prozentual aus den Gesamtausfallraten abgeleitet. Die Anteile konnten ebenfalls aus Literaturwerten ermittelt werden und sind bei den diskutierten Veröffentlichungen in Abschnitt 8.1.3 angegeben.

### 8.1.3 Ausgewertete Literatur

Bei der Ermittlung der Ausfallraten von Differenzdruck- bzw. Druckmeßumformern mit Bartonzelle bzw. Rohrfedermeßwerk und von Relais wurden folgende Literaturquellen ausgewertet:

- Nuclear Plant Reliability Data System, 1976 Annual Report of System and Component Reliability, Hrsg.: ANSI, APPA EEI and USNRC, May 1977 /F3, 8-1/

Durch die umfangreiche und detaillierte Dokumentation dieser Datensammlung konnten zum Teil Ausfallraten für je zwei Populationen angegeben werden, bei Relais z.B. die eine mit 4132 beobachteten Einheiten und die andere mit 409 beobachteten Einheiten. Bei Meßumformern lag die Größe der Population zwischen 568 und 130 Einheiten. Bei einer Population traten keine Ausfälle auf. Da der Beobachtungszeitraum genügend groß war, konnte trotzdem unter Verwendung der  $\chi^2$ -Verteilung eine Ausfallrate berechnet werden:

$$\lambda_{50} = \frac{\chi^2_{50;2}}{T}$$

mit

T: akkumulierte Betriebszeit

Dabei ergaben sich:

Relais	$\lambda_1 = 0,5 \cdot 10^{-6}/h$
	$\lambda_2 = 0,6 \cdot 10^{-6}/h$
Meßumformer mit Bartonzelle	$\lambda_1 = 1,2 \cdot 10^{-6}/h$
	$\lambda_2 = 2,5 \cdot 10^{-6}/h$
Meßumformer mit Rohrfedermeßwerk	$\lambda = 5,3 \cdot 10^{-6}/h$
Ausfallart: mißt zu hohen oder zu niedrigen Druck	66 %

- Green, A.E., and A.J. Bourne: Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, AHSB (S) R 117, UKAEA, 1966 /F3, 8-2/

Als Quelle der Ausfallraten für Meßumformer und Relais wurde die sogenannte "Felderfahrung" angegeben. Dieselben Ausfallratenlisten sind bei allen UKAEA-Quellen zu finden.

Relais	$\lambda = 0,5 \cdot 10^{-6}/h$
Meßumformer mit Bartonzelle	$\lambda = 5 \cdot 10^{-6}/h$

- Earles, D.R., and M.F. Eddins (General Electric): Reliability Physics, Ninth National Symposium on Reliability and Quality Control, San Francisco, 1963 /F3, 8-3/

Dieselben Datentabellen finden sich in: Garrick, B.J., et al.: Reliability Analysis of Nuclear Power Plant Protective Systems, HN 190, Holmes & Narver Inc., 1967 /F3, 8-4/ und in: Earles, D.R.: Reliability Application and Analysis Guide, MI-60-54, The Martin Company, 1961 /F3, 8-5/.

Die Ausfallraten wurden durch Tests unter Laborbedingungen ermittelt.

Relais	$\lambda = 0,25 \cdot 10^{-6}/h$
Meßumformer mit Bartonzelle	$\lambda = 2,2 \cdot 10^{-6}/h$
Meßumformer mit Rohrfedermeßwerk	$\lambda = 3,5 \cdot 10^{-6}/h$

- Headington, W.L., M.E. Stewart and J.O. Zane: Fault Tree Analysis of the PBF Transient Rod Drive System, IDO-17272, Phillips Petroleum Company, Atomic Energy Division, November 1968 /F3, 8-6/

Die Ausfallrate für Relais ist dem "Failure Rate Data Program of Army, Navy, Air Force & Nasa (FARADA)" entnommen.

Relais	$\lambda = 0,87 \cdot 10^{-6}/h$
--------	----------------------------------

- Ausfallratenstatistik, Hrsg. Schoppe und Faeser, Minden, 1973 und 1976 /F3, 8-7/

Die Ausfallrate für Meßumformer mit Bartonzellen wurde im Werk anhand von Reparaturaufträgen ermittelt. Die Rate ist nach Ausfallarten prozentual aufgeteilt.

Meßumformer mit Bartonzelle	$\lambda = 1,5 \cdot 10^{-6}/h$
Ausgang konstant 100 %	20 %
Ausgang konstant 0	40 %
kein definierter Ausgang	19 %
Meßfehler erheblich zu groß	17 %
Sonstiges	4 %

- Balfanz, H.P.: Ausfallratensammlung, IRS-W-8, IRS, 1973 /F3, 8-8/

Die Ausfallrate für Meßumformer entstammt einer internen Mitteilung der Firma General Electric. Es wurden 54 Einheiten beobachtet.

Meßumformer mit Bartonzelle	$\lambda = 4,7 \cdot 10^{-6}/h$
Meßumformer mit Rohrfedermeßwerk	$\lambda = 4,7 \cdot 10^{-6}/h$

- Bartels, G.: Wirtschaftliches Instandhalten von Meß-, Steuer- und Regelanlagen in Chemiebetrieben, Bayer, Leverkusen, 1977 /F3, 8-9/

Es wurde im Rahmen einer rechnerunterstützten Erfassung von Instandhaltungsmaßnahmen in mehreren Bayer-Werken eine Ausfallratenstatistik erstellt, der die Werte für Meßumformer entnommen sind.

Meßumformer mit Bartonzelle oder mit Rohrfedermeßwerk	$\lambda = 8,2 \cdot 10^{-6}/h$
--	---------------------------------

- RADC Reliability Notebook, Vol. II, Rome Air Development Center, New York, 1967 /F3, 8-10/

Die Ausfallrate für Relais wurde in Labortests unter verschiedenen Umwelt- und Streßbedingungen erzielt. Sie setzt sich aus

einer Basisausfallrate und Faktoren zusammen, die Bauart, Belastung, Anzahl der Schaltspiele und Umgebung berücksichtigen.

Relais  $\lambda = 0,74 \cdot 10^{-6}/h$

- Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix III: Failure Data, WASH-1400 (NUREG 75/014), USNRC, 1975 /F3, 8-11/

Es wird u.a. eine Ausfallrate für Relais, aufgeschlüsselt nach fünf Ausfallarten, aufgeführt.

Relais  $\lambda = 0,52 \cdot 10^{-6}/h$

Ausfallarten:

Arbeitskontakt schließt nicht bei vorhandener Erregung	58 %
Ruhekontakt öffnet nicht bei nicht vorhandener Erregung	19 %
Kurzschluß zwischen Arbeits- und Ruhekontakt	2 %
Unterbrechung in der Erregerspule	19 %
Kurzschluß in der Erregerspule	2 %

## 8.2 Betriebserfahrung

Ein wichtiges Verfahren, Zuverlässigkeitsdaten leittechnischer Komponenten zu gewinnen, liegt in der Auswertung der Betriebserfahrung. Es wäre an sich wünschenswert, für die Beurteilung der in kerntechnischen Anlagen eingesetzten leittechnischen Komponenten eine für eine hohe Aussagesicherheit ausreichende Betriebserfahrung zu haben. Da aber nur für einige spezielle Geräte ausreichende Betriebserfahrung vorliegt, muß häufig auf Betriebserfahrung aus ähnlichen Einsatzbedingungen (z.B. chemische Industrie, konventionelle Kraftwerke) oder auf Betriebserfahrung mit ähnlichen Komponenten zurückgegriffen werden. Daher wurde der Lehrstuhl für elektrische Meßtechnik der TU München von der GRS beauftragt, neue Datenquellen zu erschließen und darin enthaltene Betriebserfahrung auszuwerten /F3, 8-12/, um somit diese, bisher nur als grobe Schätzwerte zu bezeichnen-

den Ausfallarten abzusichern. Zusätzlich sollten die Baugruppen-Ausfallraten überprüft werden, die durch theoretische Ausfalleffektanalysen (Abschnitt 8.3) ermittelt worden waren. Die durch den hier zitierten Bericht abgesicherten Ausfallraten sind in Anhang 3 besonders gekennzeichnet.

Die Untersuchungen begannen mit der Auswertung von ca. 250 Veröffentlichungen, die in den letzten fünf Jahren zu den Schlagwörtern Prüftechnik, Qualität, Sicherheit und Wartung erschienen sind. Weiterhin wurden ca. 50 Firmen, die Hersteller oder Anwender leittechnischer Komponenten sind, angesprochen. Informationen, die schon in Datensammlungen der GRS eingeflossen waren, wurden nicht aufgenommen.

Ausfallraten für die in Fehlerbäumen vorkommenden leittechnischen Komponenten wurden weitgehend aus Störungs- und Reparaturprotokollen von Kraftwerken gewonnen, wobei insbesondere wegen der längeren Betriebszeiten und der größeren dort vorliegenden Erfahrungen konventionelle Kraftwerke ausgewertet worden sind. Darüber hinaus wurde untersucht, wieweit die aus Kraftwerken stammenden Daten mit Erfahrungen aus anderen technischen Bereichen übereinstimmen. Hier lagen vor allem Betriebsstatistiken aus dem Bereich der Fernsprechtechnik und der Prozeßsteuerung in der chemischen Industrie vor. Meist waren die in den Kraftwerken geführten Reparaturberichte nicht so detailliert, daß die Versagenswahrscheinlichkeit für eine bestimmte Gerätefunktion direkt angegeben werden konnte. Hierzu war es notwendig, die aus Felderfahrungen ermittelten Geräteausfallraten auf die möglichen Ausfallarten aufzuteilen. Diese Aufteilung war um so korrekter durchzuführen, je besser die Ausfallmöglichkeiten der Geräte bekannt waren, und dann besonders gut möglich, wenn eine Ausfalleffektanalyse vorlag.

Im Rahmen dieser Arbeiten wurden auch, wie schon erwähnt, die Ergebnisse aus theoretischen Ausfalleffektanalysen (siehe Abschnitt 8.3) von Elektronikarten überprüft. Die Auswertung der Betriebserfahrung aus deutschen Kraftwerken zur Ermittlung von Ausfallraten der dort eingesetzten Elektronikarten geschah teilweise beim Betreiber, teilweise beim Gerätehersteller und

teilweise am Lehrstuhl für elektrische Meßtechnik. Insgesamt stützten sich die Ergebnisse auf Daten aus neun konventionellen Kraftwerken mit insgesamt elf ausgewerteten Blöcken und auf Mitteilungen aus zwei Kernkraftwerken. Das ergab eine Testmenge von rund 50 000 Baugruppen bei einer mittleren Einsatz- und Prüfdauer von fünf Jahren. Grundlage für eine gesicherte Ausfallratenermittlung war eine sorgfältig geführte Auflistung aller aufgetretenen Schäden. Die ausgewerteten Berichte hatten zwar einen stark unterschiedlichen Detaillierungsgrad, doch waren für die ausgewerteten Kraftwerke die Betriebszeit und die Zahl der eingesetzten Geräte bekannt.

Am Beispiel einer Baugruppe aus dem gleichen Leittechniksystem wie in der Referenzanlage soll die Auswertung näher erläutert werden. Das hier angesprochene System Simatic P wird seit etwa 1969 in einer großen Anzahl von Kraftwerken eingesetzt. Trotzdem sind bisher keine Auswertungen von Betriebserfahrungen veröffentlicht. Als Quelle für die hier dargelegten Ergebnisse dienen die Schadensberichte aus dem konventionellen Kraftwerk Irching. Insgesamt wurden die Ergebnisse aus allen drei Blöcken des Kraftwerkes mit zusammen 9 000 Baugruppen berücksichtigt. Die Betriebszeiten für die Blöcke (Stand April 1978) lagen zwischen 78 800 und 29 100 Stunden. Aus den Schadens- und Reparaturberichten war keine Trennung in zufällige Fehler und Behandlungsfehler möglich. Aus diesem Grund sind alle Fehler pessimistisch als zufällige gewertet. Tabelle F3, 8-1 zeigt die Auswertung für den Betätigungsbaustein B21B /F3, 8-12/.  $\bar{\lambda}$  ist der Schätzwert für den Erwartungswert der Ausfallrate.  $\lambda_o$  bzw.  $\lambda_u$  sind für den Erwartungswert die oberen bzw. unteren Vertrauensgrenzen mit 90 % Aussagesicherheit, die mit Hilfe der  $\chi^2$ -Verteilung berechnet wurden. N ist die Anzahl der betrachteten Baugruppen, NT die Gesamtbetriebszeit und n die Anzahl der Ausfälle. Im Vergleich zur Betriebserfahrung ( $\lambda = 0,83 \cdot 10^{-6}$  pro Stunde) ergab die Ausfalleffektanalyse /F3, 8-13/ nach Zusammenfassung aller Ausfallarten eine Ausfallrate von  $1 \cdot 10^{-6}$  pro Stunde.



Anlage	N	$\frac{NT}{10^6 \text{ h}}$	n	$\bar{\lambda}$	$\lambda_u$	$\lambda_0$
				in $10^{-6}/\text{h}$		
Irsching 1	79	6,23	6	0,96	0,42	1,89
Irsching 2	79	3,97	1	0,25	0,01	1,19
Irsching 3	106	3,1	4	1,29	0,44	2,95
Zusammen	264	13,30	11	0,83	0,47	1,4

Tab. F3, 8-1:

Beispiel für die Auswertung der Schadensstatistik des Kraftwerks Irsching; Steuerungssystem: Simatic P, Baugruppe: Betätigungsstufe B21B

Für Leitungsanschlüsse (Löt-, Crimp- oder Wrap-Verbindungen) lieferte eine Auswertung von Literatur für Ausfallraten Werte im Bereich von  $\lambda = 1 \cdot 10^{-8}$  bis  $\lambda = 2 \cdot 10^{-7}$  pro Stunde. In WASH-1400 wird bei Leitungsanschlüssen für die Ausfallart P-Schluß ein Wert von  $\lambda_{50} = 3 \cdot 10^{-10}$  pro Stunde und für die Ausfallart Masseschluß ein Wert von  $\lambda_{50} = 1 \cdot 10^{-8}$  pro Stunde angegeben.

Für Quetschverbindungen läßt sich jedoch aus Betriebserfahrung /F3, 8-12/ eine Gesamtausfallrate von  $\lambda_{50} = 1 \cdot 10^{-9}$  pro Stunde angeben. Eine Expertenabschätzung lieferte ebenfalls eine Ausfallrate von  $\lambda = 1 \cdot 10^{-9}$  pro Stunde für nicht steckbare Verbindungen. Dieser Wert wurde auch in der vorliegenden Studie verwendet, wobei eine Aufteilung in einzelne Ausfallarten nicht sinnvoll erschien. Eine zu einem späteren Zeitpunkt durchgeführte Auswertung von Betriebserfahrung zu Klemmkurzschlüssen (Schraub-, Löt- und Klemmanschlüsse) führte zu einer Obergrenze der Ausfallrate von  $\lambda_{95} = 3 \cdot 10^{-9}$  pro Stunde /F3, 8-12/.

Der in der Studie verwendete Wert wurde also, wie die Auswertung der Betriebserfahrung zeigt, pessimistisch abgeschätzt. Die Literaturangaben erscheinen unter Berücksichtigung der Betriebserfahrung als zu pessimistisch.

Für einige neuere Geräte konnte wegen der kurzen Einsatzzeit noch nicht auf Betriebserfahrungen im wünschenswerten Umfang zurückgegriffen werden. Hier war es naheliegend, von den Bauelementen der Baugruppen auszugehen und die Summe der Bauelementausfallraten der Geräte als erste Näherung für die Baugruppenausfallrate zu nehmen bzw. genauer die Bauelementausfallraten für eine Ausfalleffektanalyse zu benutzen. Die Bauelementausfallraten können vorhandenen Ausfallratensammlungen, insbesondere /F3, 8-14/, entnommen werden. Die Anwendung dieser Daten auf den zivilen europäischen Bereich ist jedoch nicht ohne weiteres möglich. So werden in der hier interessierenden Kraftwerkstechnik keine MIL-spezifizierten Bauelemente verwendet, und es ist auch unsicher, welche der in MIL definierten Qualitätsstufen für die industrielle Technik zutreffend sind. Aus diesem Grunde wurde in /F3, 8-12/ versucht, neben der Auswertung von Herstellerangaben die Bauelementausfallraten rückwärts aus den Geräte-Schadensstatistiken zu errechnen. Diese "Feld"-Bauelementausfallraten sind in Tabelle F3, 8-2 beispielhaft den MIL-Bauelementausfallraten gegenübergestellt /F3, 8-12 und -14/.

Bauelement	Ausfallraten in $10^{-9}/h$			
	Geräte- serie A	Geräte- serie B	Geräte- serie C	MIL-HDBK 217B <sup>1)</sup>
Widerstand	0,46	0,4	0,9	15 <sup>2)</sup>
Kondensator	14,2	5,4	2,7	6 <sup>3)</sup>
Transistor	48	130	17	180 <sup>4)</sup>
Diode	3,8	3,0	5,0	120 <sup>5)</sup>

- 1) "quality factor" = 1  
Einsatzart = "ground fixed"  
2) Schichtwiderstände MIL RLR 39017  
3) Kunststofffolienkondensator  
4) npn-Si-Transistor  
5) Si-Universaldiode

Tab. F3, 8-2:  
Ausfallratenvergleich

Aus der Tabelle wird ersichtlich, wie die Bauelemente für den Kraftwerksbereich im Vergleich zu den MIL-Berechnungen liegen. Die rückgerechneten Ausfallraten sind auf jeden Fall zutreffender, da realitätsbezogen, und stellen verbesserte Eingangsdaten für Ausfalleffektanalysen dar. Auf der anderen Seite sind diese "Feld"-Ausfallraten immer noch als pessimistisch zu bezeichnen, da die Daten fast ausschließlich von Komponenten stammen, die nicht in Reaktorschutzqualität (Gerätequalität nach KTA 3501) hergestellt worden sind. Es fehlten weitgehend die Begutachtung und die begleitende Kontrolle durch den TÜV und die Eignungsprüfung, die besonderen Maßnahmen also, die für den Einsatz sicherheitsrelevanter leittechnischer Komponenten vorgeschrieben sind. Es kann unterstellt werden, daß bei diesen Prüfungen Schwachstellen und Frühausfälle entdeckt werden, so daß die tatsächlich in der Reaktorschutztechnik auftretenden Ausfallraten wahrscheinlich noch geringer sind als die in Tabelle F3, 8-2 zusammengestellten Werte.

Bei der durchgeführten Auswertung ist darauf geachtet worden, ob sich eventuell eine zeitliche Änderung der Komponentenausfallraten feststellen ließ. So war z.B. bei dem Kraftwerk mit der längsten analysierten Betriebszeit von 10 Jahren noch kein Ansteigen der Ausfälle ersichtlich.

### 8.3 Ausfallratenermittlung durch Ausfalleffektanalyse

Neben der Auswertung von Betriebserfahrung und Literatur wird zur Ermittlung der Zuverlässigkeitskenngrößen von Leittechnikkomponenten vor allem auch die Ausfalleffektanalyse eingesetzt. Sie liefert universell anwendbare Ergebnisse und soll, da viele in dieser Studie verwendete Geräteausfallraten mit dieser Methode ermittelt wurden, im folgenden ausführlich beschrieben werden.

### 8.3.1 Allgemeines

Die Ausfalleffektanalyse dient zur Ermittlung der Auswirkungen aller möglichen Fehler bzw. Ausfälle auf alle Ein- und Ausgänge eines Gerätes. Sofern sie sorgfältig und vollständig durchgeführt wird, beschreiben die ermittelten Ergebnisse das mögliche Ausfallverhalten des untersuchten Gerätes. Die Analyse kann experimentell, theoretisch oder in Kombination von beiden Methoden durchgeführt werden.

Wesentlich für den Aussagewert der Analyse ist die Auflistung jener Fehler bzw. Ausfälle, die berücksichtigt werden sollen. Bei diskret aufgebauten Geräten werden folgende Vereinbarungen getroffen:

- Der Ausfall jedes beliebigen Bauelementes wird untersucht.
- Unterstellt werden nur die extremen Bauteilfehler: Baustein bewirkt Kurzschluß zwischen zwei Anschlüssen; Baustein bewirkt Unterbrechung eines Anschlusses.
- Die Bauelementausfallraten werden als zeitlich konstant vorausgesetzt.
- Es wird jeweils nur ein einziger Fehler eingebaut bzw. angenommen.
- Bei Bauteilen, die im Inneren komplex aufgebaut sind (z.B. integrierte Schaltungen), werden Unterbrechungen der Ausgänge oder Kurzschlüsse der Ausgänge zu den Versorgungspotentialen (mitunter auch alle einfachen Kurzschlüsse zwischen den einzelnen Ausgängen) unterstellt.
- Treten bei experimentellen Untersuchungen Folgefehler auf, so werden diese vor der Simulation des nächsten Bauteilfehlers beseitigt.
- Es finden nur solche Fehler Berücksichtigung, die nach der Fertigungskontrolle, d.h. im Betrieb, noch vorkommen können (z.B. der Kurzschluß zweier Transistorelektroden, nicht jedoch der Kurzschluß zweier Leiterbahnen auf einer Printplatte).

- Die Ausfalleffekte werden meist mittels Formblättern bewertet, wobei unterschieden wird, ob

das analysierte Gerät zur Auslösung eindeutig oder nicht eindeutig sicherheitsgerichteter Aktionen dient, der Ausfall selbstmeldend oder nicht selbstmeldend ist, der Ausfall gefährlich oder ungefährlich ist, ein aktiver oder passiver Ausfall vorliegt.

In der Regel bleiben unberücksichtigt:

- Änderungs- bzw. Driftausfälle,
- Mehrfachausfälle (z.B. Doppelfehler usw.),
- genauer innerer Aufbau von integrierten Schaltkreisen,
- äußere Störeinflüsse und
- systematische Ausfallursachen.

Es ist davon auszugehen, daß diese Vernachlässigungen um so weniger zulässig sind, je wichtiger die Sicherheitsfunktion des zu analysierenden Gerätes ist. Aus diesem Grunde wurden in gewissen Fällen folgende Einflüsse mit in die Analyse einbezogen:

- Mehrfachfehler, wenn keine oder nur sehr wenige gefährliche Einfachfehler auftreten und deshalb zu erwarten ist, daß ihre Ausfallrate einen merklichen Beitrag zum Gesamtergebnis liefert;
- Änderungsausfälle, wenn z.B. in binär arbeitenden Schaltungen analog arbeitende Teilschaltungen enthalten sind und keine oder nur sehr wenige gefährliche Totalausfälle auftreten;
- innerer Aufbau von integrierten Schaltkreisen, vor allem dann, wenn das Bauteil in irgend eine Richtung unter keinen Umständen ausfallen darf (z.B. bei gefordertem "fail safe"-Verhalten) und
- ungünstige Umgebungseinflüsse, wenn ihr Auftreten nicht ausgeschlossen werden kann.

Ist die Analyse in der beschriebenen Weise durchgeführt, so erhält man die Geräteausfallraten für Einzelfehler durch einfache Addition aller Ausfallraten jener Bauelemente, deren Ausfälle zu der jeweils interessierenden Ausfallart führen. Sollen Mehrfachfehler berücksichtigt werden, so ist zusätzlich die Kennt-

nis von Fehlerentdeckungszeiten erforderlich. Die Ausfallraten der einzelnen Bauelemente können der zahlreich vorhandenen Literatur entnommen werden.

### 8.3.2 Experimentelle Ausfalleffektanalyse

Bei der Durchführung experimenteller Ausfalleffektanalysen werden einem möglichst der laufenden Fertigung entnommenen Gerät nacheinander alle zu berücksichtigenden Fehler eingebaut und mit Hilfe geeigneter Meßgeräte die jeweiligen Ausfallwirkungen ermittelt. Sofern eine detaillierte Analyse normalerweise unzugänglicher Schaltungen notwendig ist (vergossene Module, integrierte Schaltkreise), müssen diese erst diskret aufgebaut werden.

Der Vorteil der experimentellen Analyse liegt in der relativ hohen Aussagesicherheit und Reproduzierbarkeit. Nachteilig wirkt sich aus, daß diese Methode bei der Untersuchung größerer Systeme sehr arbeitsintensiv ist und daher praktisch nur Einzelfehler berücksichtigt werden können. Auch Bauteiltoleranzen lassen sich nicht systematisch berücksichtigen. Bei der Analyse integrierter Schaltungen macht der Aufbau eines diskreten Modells erhebliche Schwierigkeiten, da manche Eigenschaften nur schwer nachgebildet werden können (parasitäre Transistoren, Schaltungskapazitäten).

### 8.3.3 Theoretische Ausfalleffektanalyse

Die Vorhergehensweise bei der theoretischen Ausfalleffektanalyse entspricht grundsätzlich der experimentellen Analyse. Die einzelnen Fehler werden nur rein gedanklich in die Schaltung eingebaut und die Ausfallwirkungen durch Überlegung ermittelt. Häufig führt dieser Weg schneller zum Ergebnis, da kein meßtechnischer Aufwand erforderlich ist. Nachteilig können sich nur gedankliche Fehler auswirken.

Bei sehr komplizierten Schaltungen hat sich eine Kombination aus theoretischer und experimenteller Analyse bewährt. Hierbei wird

die Untersuchung zunächst theoretisch durchgeführt. Dort, wo die Überlegung nicht zu einer eindeutigen Aussage führt, dient das Experiment als Kontrolle.

#### 8.3.4 Ausfalleffektanalyse mit Netzwerk-analyseprogrammen

Die Vorgehensweise bei der Ausfalleffektanalyse mit Netzwerk-analyseprogrammen entspricht weitgehend den beiden zuvor genannten Methoden. Die zu analysierende Schaltung muß zusammen mit den betrachteten Fehlern einem Rechner eingegeben werden. Dieser rechnet dann die Schaltung für jeden einzelnen Fehler mit Hilfe eines Netzwerkanalyseprogrammes durch und druckt das ermittelte Ausfallverhalten aus. Der Vorteil liegt in der hohen Aussage-sicherheit. Schaltungsparameter lassen sich leicht ändern. Dem entgegen stehen die langen Rechenzeiten bei der Analyse komplexer Schaltungen. Ebenso müssen Modelle für nichtlineare Bauelemente erstellt werden.

#### 8.3.5 Anwendung auf leittechnische Komponenten und Geräte

Im folgenden sind die in der Referenzanlage eingesetzten Komponenten und Geräte aufgelistet, deren Ausfallraten mittels einer Ausfalleffektanalyse /F3, 8-13, -15 bis -17/ bestimmt wurden:

- Thermoelement und Umformer
- Drehzahlfühler und Umformer
- Strom-Spannungs-Wandler
- Spannungs-Spannungs-Wandler
- Trennverstärker TTK
- Summierverstärker
- Grenzwertmelder RG 11
- 2v3-Auswahleinheit des Logikteils
- NOR-Gatter im Taktgeber
- Abschlußglied des dynamischen Logikteils
- Binärsignaleingabe
- Taktgeber des Logikteils

- UND-Gatter (Simatic P)
- ODER-Gatter (Simatic P)
- Verzögerungsstufe (analog) - (Simatic P)
- Verzögerungsstufe (digital) - (Reaktorschutzsystem)
- Betätigungsbaustein B22 für Motorarmaturen (Simatic P)
- Betätigungsbausteine B21 und B23 für Leistungsschalter und Schütze (Simatic P)

Die Ausfallraten der oben aufgeführten Komponenten sind in der Tabelle der Basisdaten im Anhang 3 angegeben.

Anhand der in /F3, 8-13/ ausführlich beschriebenen Analyse des Simatic-P-Bausteins V21 soll beispielhaft gezeigt werden, wie die Ausfallrate für eine bestimmte Ausfallart ermittelt wurde. Die quantitative Bewertung der UND-Stufe V21 (Bild F3, 8-1) ist hier für die Ausfallart "P-Potential wird nicht ausgegeben" dargestellt.

Für die Ausfalleffektanalysen wurden folgende Festlegungen getroffen:

- Doppelfehler werden vernachlässigt, da sie zum einen wegen der niedrigen Bauelementausfallraten sehr unwahrscheinlich sind, zum anderen in den meisten Fällen schon Einzelfehler zum Ausfall der Schaltung führen.
- Belastungsfaktoren (K-Faktoren) werden nur auf die Gesamtschaltung, nicht auf die Bauelemente bezogen. Für die K-Faktoren wird auf die in /F3, 8-2/ veröffentlichten Werte zurückgegriffen. Der Gesamtfaktor für die Referenzanlage setzt sich aus folgenden Einzelfaktoren zusammen:

$K_1 = 0,5$  für vibrationsfreien Einbauort und kontrollierte Atmosphäre,

$K_2 = 0,2$  für 40-%-Belastung der Bauelemente, bezogen auf deren Nennleistung,

$K_3 = 1,3$  für eine Umgebungstemperatur am Einbauort der Bauelemente von 40 °C.

Hieraus ergibt sich ein Gesamtbelastungsfaktor von

$K = K_1 \cdot K_2 \cdot K_3 = 0,13$ . Um diesen Faktor wurden die Gesamtausfallraten für jede mögliche Ausfallart vermindert.



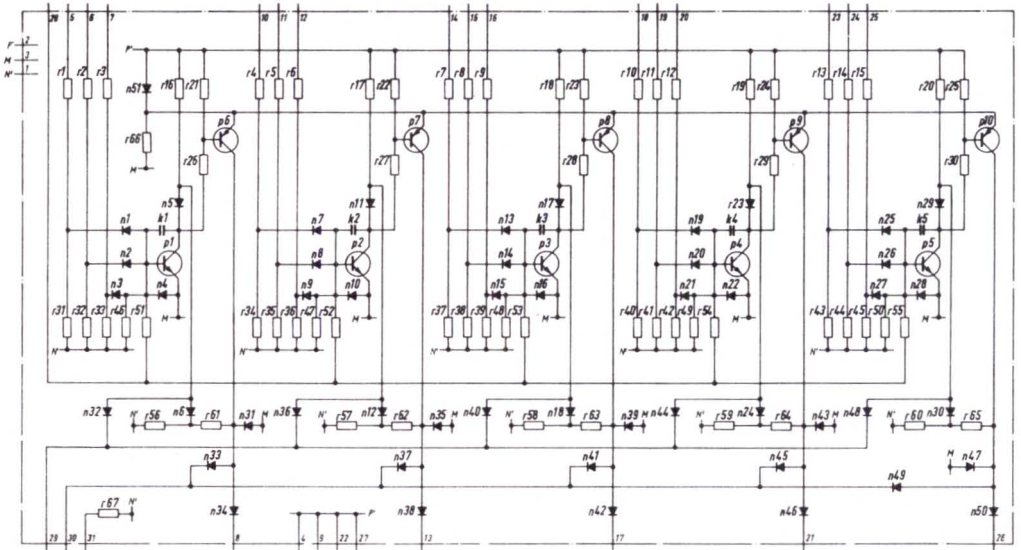
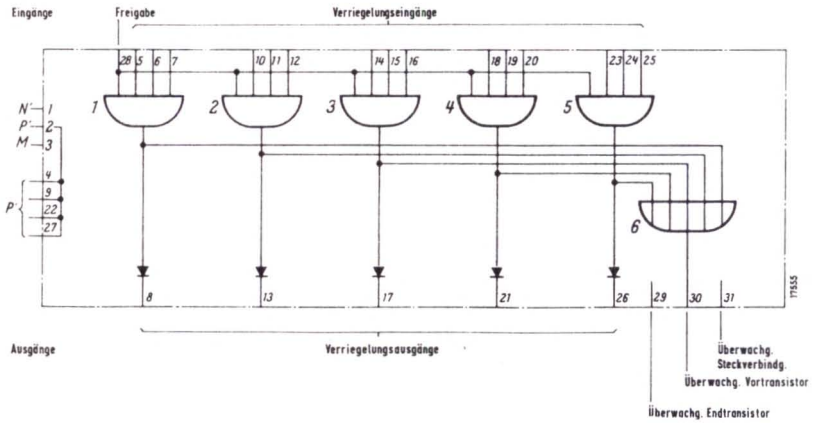


Bild F3, 8-1:  
Schaltplan Simatic-P-Baustein V21 (UND-Stufe)

- In den Ausfallraten ist nur jeweils der Teil der Schaltung berücksichtigt, der auf den entsprechenden Geräteschaltplänen eingezeichnet ist. Das bedeutet, nur die im Baustein auftretenden Ausfälle wurden berücksichtigt, nicht aber Umgebungseinflüsse, wie zum Beispiel auftretende Überspannungen.

Die Ausfalleffektanalyse ergab für die Ausfallart "P-Potential wird nicht ausgegeben" die aus Tabelle F3, 8-3 ersichtliche Aufteilung der Gesamtausfallrate.

Ausfallart	Bauelement / Bezeichnung	Ausfallrate $10^{-6}/h$	Restliche Gatter Ausfallrate $10^{-6}/h$
K	2 Dioden (n4, n31)	0,02	0,02
U	2 Dioden (n34, n51)	0,01	
U	5 Widerstände (r1, r2, r3, r31, r32)	2,45	
K	5 Widerstände (r21, r26, r33, r51, r66)	0,25	0,1
U	2 Transistoren (p1, p6)	0,19	
U	5 Stecker (st5, st6, st7, st8, st28)	0,05	
MK	1 Stecker (st29)	0,001	
		2,97	+ x · 0,12

U = Unterbrechung  
 K = Kurzschluß  
 MK = Masseschluß

Tab. F3, 8-3:

Beispiel für die Aufteilung der Gesamtausfallrate

Unter Berücksichtigung des Belastungsfaktors erhält man eine Ausfallrate von  $\lambda = (0,4 + x \cdot 0,02) \cdot 10^{-6} h^{-1}$ . Hierbei gibt x die Zahl der UND-Gatter auf der gleichen Karte an, die gleichzeitig mit dem betrachteten Gatter leitend werden. x kann alle Werte zwischen 0 und 4 annehmen. Der Fehler ist nicht selbst-meldend. Der Fehlerbaum in Bild F3, 8-2 soll das Zusammenwirken der Bauelementausfälle veranschaulichen.

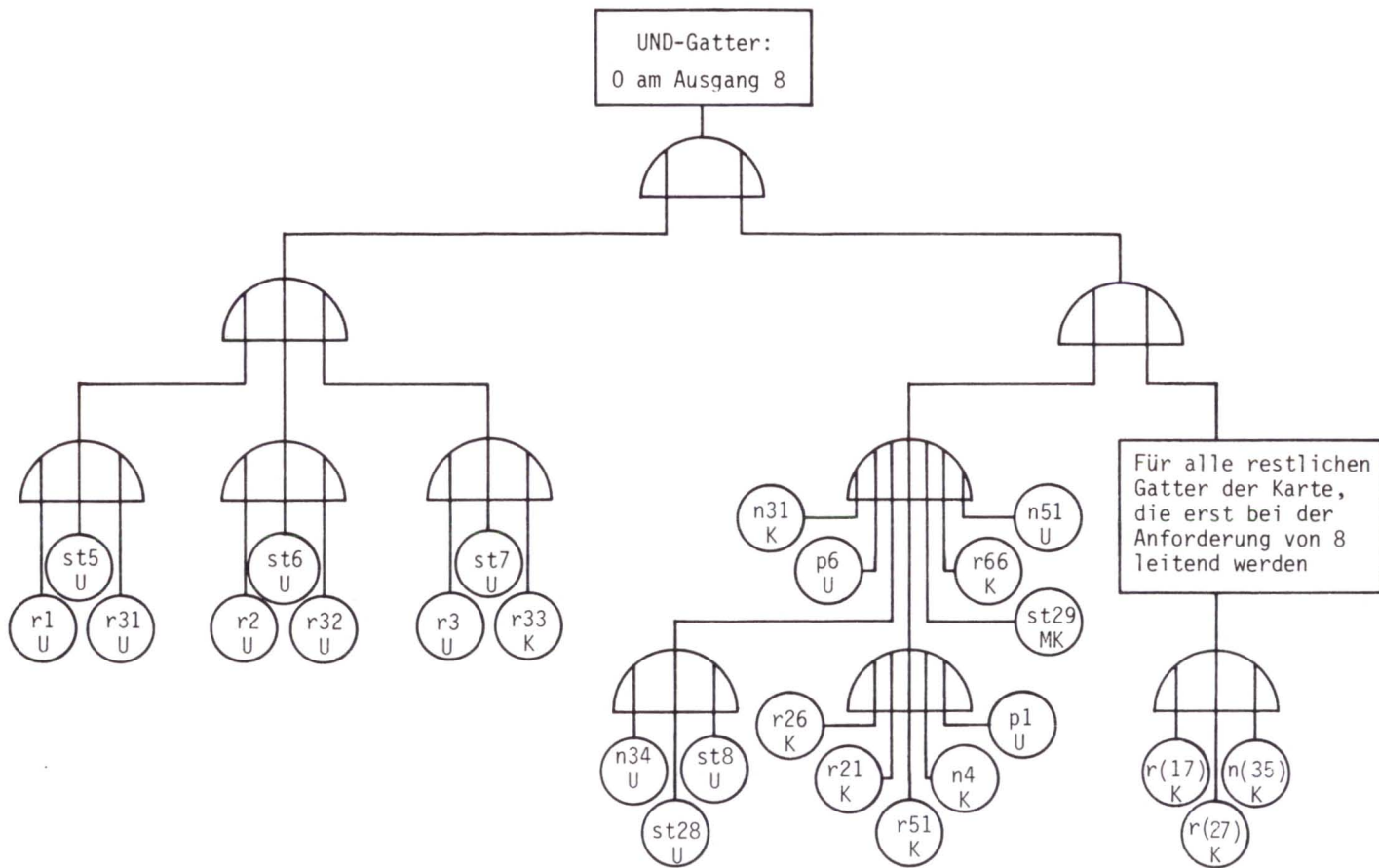


Bild F3, 8-2:

Fehlerbaum Simatic-P-Baustein V21 (UND-Stufe)

### 8.3.6 Ersatzausfallraten für leittechnische Systeme

Die in die Fehlerbaumanalysen miteinbezogenen leittechnischen Systeme setzen sich aus den in Anhang 3 aufgelisteten Geräten und Baugruppen zusammen. Der Einfluß, den Ausfälle einzelner Geräte und Baugruppen innerhalb eines Systems auf die Funktion dieses Systems ausüben, wird durch eine Zuverlässigkeitsanalyse bestimmt. Zuverlässigkeitsanalyse und Quantifizierung des Ausfallverhaltens der jeweils angeforderten Systeme sowie die daraus resultierenden Ersatzausfallraten sind im Fachband 2 beschrieben. Der Anhang des Fachbandes 2 enthält zusätzlich die Liste aller in den Fehlerbaumanalysen verwendeten Ausfallraten der Leittechnik.

### 8.4 Basisdaten zu "common mode"-Ausfällen in der Leittechnik

Die grundsätzliche Methodik zur Behandlung von "common mode"-Ausfällen (CMA) ist ausführlich im Fachband 2 dargestellt. Im folgenden werden daher nur nochmals die verwendeten Nichtverfügbarkeiten für CMA in der Hardware der Leittechnik bzw. CMA aufgrund menschlicher Fehlhandlung zusammenfassend wiedergegeben.

Es werden zwei Arten von CMA unterschieden, einmal sind dies Ausfälle der Hardware selbst, zum anderen sind dies CMA aufgrund menschlicher Fehlhandlungen. Die möglichen Ursachen von CMA werden im Fachband 2 erläutert.

#### ● CM-Ausfälle in der Hardware

In der deutschen Risikostudie wurden Hardware-CMA in der Leittechnik bei Meßumformern und im Relaiseteil des Reaktorschutzsystems unterstellt. Zu denkbaren CMA in anderen Bereichen (z.B. Warte, Verkabelung) liegen bisher keine Hinweise aus der Betriebserfahrung vor, eine sinnvolle Quantifizierung erschien deshalb nicht möglich.

CMA von Meßumformern wurden nur für Druck- bzw. Differenzdruck-, Wasserstands-, Temperatur- und Drehzahlmessungen quantifiziert.

CMA von Spannungsmessungen spielen gegenüber der Wahrscheinlichkeit eines CM-Ausfalls der Notstromdiesel keine Rolle und wurden daher nicht bewertet.

Für Differenzdruck-Meßumformer wurde eine Nichtverfügbarkeit von

$$\begin{aligned}P_{\text{CMA } 50} &= 3,1 \cdot 10^{-4} \\K_{95} &= 4 \\ \bar{P}_{\text{CMA}} &= 5 \cdot 10^{-4} \text{ (gerundet)}\end{aligned}$$

ermittelt. Dieser Wert stellt unseres Erachtens eine Obergrenze für CMA auch der Meßumformer der anderen Meßarten dar, da für diese keinerlei Hinweise auf CMA aus der Betriebserfahrung vorliegen.

Der genannte Wert bezieht sich auf Ausfälle in der Hardware einer Meßkanalgruppe (einer Redundanz). Für CM-Ausfälle gleichartiger Meßumformer in mehreren Strängen wird geschätzt, daß diese in 10 % aller Fälle auftreten werden. Es wurde daher der CM-Ausfall der Meßumformer in zwei oder mehr Strängen durch einen Faktor von 0,1 bewertet.

Der Relaisteil der Reaktorschnellabschaltung und die Relaissteile zur Auslösung der Reaktorschutzsignale wurden unterschiedlich bewertet (Fachband 2). Wegen der hohen sicherheitstechnischen Bedeutung der Reaktorschnellabschaltung wurde für deren Relaissteile eine sehr pessimistische Methode gewählt. Für dieses System wurde die CMA-Wahrscheinlichkeit aus Betriebserfahrung ermittelt. Es ergab sich:

$$\begin{aligned}P_{\text{CMA } 50} &= 1,2 \cdot 10^{-6} \\K_{95} &= 4,5 \\ \bar{P}_{\text{CMA}} &= 1,8 \cdot 10^{-6}\end{aligned}$$

Der Relaiseteil der Reaktorschutzsignale ist in je zwei Redundanzen zueinander diversitär aufgebaut. Für die nichtdiversitären Relaiserteile zweier Redundanzen ergibt sich ein Wert von:

$$\begin{aligned} P_{\text{CMA } 50} &= 1,1 \cdot 10^{-4} \\ K_{95} &= 3 \\ \bar{P}_{\text{CMA}} &= 1,3 \cdot 10^{-4} \end{aligned}$$

Die Wahrscheinlichkeit eines CM-Ausfalls von zueinander diversitären Redundanzen läßt sich daraus zu

$$\begin{aligned} P_{\text{CMA } 50} &= 1,2 \cdot 10^{-8} \\ K_{95} &= 4,5 \\ \bar{P}_{\text{CMA}} &= 1,8 \cdot 10^{-8} \end{aligned}$$

ermitteln.

● CM-Ausfälle aufgrund menschlicher Fehlhandlung

Die Bewertung von CM-Ausfällen aufgrund menschlicher Fehlhandlung wurde in Anlehnung an WASH-1400 durchgeführt. Die deutsche Betriebserfahrung weist einen derartigen CM-Ausfall in einem Betriebssystem nach. Bei menschlichen Handlungen, die mehrfach hintereinander durchzuführen sind, sind im allgemeinen Abhängigkeiten zu berücksichtigen. Derartige Kopplungen wurden in den Analysen berücksichtigt, wenn gleichartige oder vom physikalischen Meßprinzip ähnliche Meßkanalgruppen mehrerer Stränge ohne größere Zeitabstände gewartet, geprüft oder justiert werden. Für CM-Ausfälle als Folge menschlicher Fehlhandlungen wurde ein Beitrag von

$$\begin{aligned} P_{\text{CMA } 50} &= 0,8 \cdot 10^{-3} \\ K_{95} &= 3 \\ \bar{P}_{\text{CMA}} &= 1 \cdot 10^{-3} \end{aligned}$$

zur Nichtverfügbarkeit einer Meßkanalgruppe ermittelt. In den Fällen, in denen eine starke Kopplung zwischen den CM-Ausfällen

mehrerer Stränge angesetzt wird, ergibt sich die Nichtverfügbarkeit zu:

$$\begin{aligned}P_{\text{CMA } 50} &= 1,3 \cdot 10^{-4} \\K_{95} &= 3 \\ \bar{P}_{\text{CMA}} &= 1,8 \cdot 10^{-4}\end{aligned}$$

Bei mittlerer Kopplung der CM-Ausfälle mehrerer Stränge ergibt sich die Nichtverfügbarkeit zu:

$$\begin{aligned}P_{\text{CMA } 50} &= 2,3 \cdot 10^{-5} \\K_{95} &= 3,5 \\ \bar{P}_{\text{CMA}} &= 3,2 \cdot 10^{-5}\end{aligned}$$

Diese Basisdaten wurden für die Bewertung der Anregekanalgruppen der verschiedenen Reaktorschutzsignale sowie in der Zuverlässigkeitsanalyse der Reaktorschnellabschaltung verwendet (Fachband 2).

## 9. BASISDATEN ZUR BEWERTUNG MENSCHLICHER FEHLHANDLUNGEN

Wie im Fachband 2 eingehend dargestellt, lehnt sich die Vorgehensweise zur Bewertung menschlicher Fehlhandlungen eng an die Vorgehensweise in WASH-1400 an. Das der Bewertung zugrunde liegende Datenmaterial wurde daher weitgehend aus WASH-1400 /F3, 9-1/ übernommen, lediglich in einigen speziellen Fällen wurde auf die Vorgehensweise der AIPA-Studie /F3, 9-2/ zurückgegriffen. Im folgenden werden die Daten, die die Grundlage der Bewertungen waren, und das in der AIPA-Studie verwendete Bewertungsmodell dargestellt.

### ● Basisdaten nach WASH-1400 (Tabelle F3, 9-1)

Bei der Bewertung menschlicher Handlungen wurden diese Basisdaten durch Multiplikation mit geeigneten Faktoren (Fachband 2) modifiziert, um Einflüsse von Gefahrenmeldungen, personeller Redundanz usw. zu berücksichtigen. Soweit nichts anderes angegeben ist, beinhalten die Wahrscheinlichkeiten keine unangemessenen Zeitbeschränkungen oder Streßbelastungen bei Störfällen.

### ● Vorgehensweise in der AIPA-Studie

In der AIPA-Studie wird bei der Ermittlung der Wahrscheinlichkeit für menschliches Fehlverhalten die zur Verfügung stehende Zeit und die für den Eingriff erforderliche Zeit berücksichtigt. Dies ist wichtig für die Bewertung menschlichen Fehlverhaltens bei Störfällen, bei denen Eingriffe durch das Personal vorgesehen sind.

Zur Berechnung der Wahrscheinlichkeit  $p$ , mit der innerhalb der zur Verfügung stehenden Zeit  $t$  die erforderliche Handlung nicht erfolgt, wird eine Exponentialverteilung zugrunde gelegt, bei der die Zeit MTOR berücksichtigt wird, die zur Durchführung der Handlung erforderlich ist, d.h.

$$p(t) = \exp. (-t/MTOR)$$



Operator-Handlung	Wahrscheinlichkeit
Fehlhandlung innerhalb der ersten 60 Sekunden nach dem Beginn einer extremen Streßsituation (z.B. bei einem großen Leck in einer Hauptkühlmitteleitung)	$\sim 1$
Fehlhandlung 5 Minuten nach Eintritt einer extremen Streßsituation	0,9
Fehlhandlung 30 Minuten nach Eintritt einer extremen Streßsituation	$10^{-1}$
Fehlhandlung mehrere Stunden nach Eintritt einer extremen Streßsituation	$10^{-2}$
Fehlhandlung allgemein (z.B. falsche Ablesung einer Anzeige und deshalb Betätigung eines falschen Schalters)	$3 \cdot 10^{-3}$
Unterlassungsfehler allgemein, wobei in der Warte keine Anzeige über den Zustand der nichtbetätigten Komponente vorhanden ist (z.B. wenn ein von Hand zu betätigendes Prüfventil nach Abschluß von Wartungsarbeiten nicht wieder in die für den Betrieb richtige Stellung gebracht wird)	$10^{-2}$
Unterlassungsfehler derart, daß während eines Arbeitsablaufes eine Handlung trotz schriftlicher Anweisungen vergessen wird; dies gilt nicht, wenn es am Ende des Arbeitsablaufs geschieht wie im vorherigen Fall	$3 \cdot 10^{-3}$
Nichtentdeckung eines vorausgehenden Fehlers bei einer Kontrolle oder bei einem Kontrollgang Anmerkung: Bei ständiger Meldung des Fehlers auf einer Meldeeinrichtung trifft diese hohe Fehlerwahrscheinlichkeit nicht zu.	$10^{-1}$
Nichtentdeckung einer falschen Armaturenstellung u.ä. bei einem Kontrollrundgang in der Anlage, falls für die Kontrolle keine Checkliste verwendet wird	0,5
Fehlhandlung allgemein bei sehr hoher Streßbelastung, wenn schnell gefährliche Handlungen durchzuführen sind	0,2 - 0,3
Wiederholte Fehlhandlung unter extrem hohem Zeitdruck. Bei jedem Versuch $n$ , die ursprüngliche Fehlhandlung zu korrigieren, verdoppelt sich die ursprüngliche Fehlerwahrscheinlichkeit $P_0$ . Anmerkung: Die Fehlhandlungswahrscheinlichkeit verdoppelt sich so lange, bis die Fehlerwahrscheinlichkeit $P = 1$ erreicht oder die verfügbare Zeit abgelaufen ist.	$p = 2^{(n-1)}P_0$

Tab. F3, 9-1:

Medianwerte der Wahrscheinlichkeiten für menschliche Fehlhandlung

Durch Erhöhung von MTOR gegenüber der bei Proben benötigten Zeit kann auf einfache Weise berücksichtigt werden, daß das Personal bei Störfällen erhöhtem Streß unterliegt.

In der AIPA-Studie wird vorgeschlagen, für die Zeit MTOR eine logarithmische Normalverteilung zugrunde zu legen, wodurch die Streuung der Wahrscheinlichkeit  $p$  berücksichtigt werden kann. Diese Vorgehensweise wurde auch in der deutschen Risikostudie angewandt.

Die aus den Basisdaten ermittelten Wahrscheinlichkeiten der einzelnen Handmaßnahmen, die für die Fehlerbaumanalyse benötigt werden, sind im Fachband 2 erläutert.

10. SCHRIFTTUM

- /F3, 3-1/ Pipe Failure Data  
in: Reactor Safety Study, An Assessment of Accident  
Risks in U.S. Commercial Nuclear Power Plants  
WASH-1400 / NUREG 75/014, App. III, October 1975
- /F3, 3-2/ Bush, S.H.:  
Reliability of Piping in Light-Water Reactors  
Nuclear Safety 17 (1976) No. 5, p. 568-579
- /F3, 3-3/ Boesebeck, K., und F.H. Heuser:  
Ausfallraten für Rohrleitungen und Druckbehälter  
Anhang A7 in: Kritischer Bericht zur Reaktorsicher-  
heitsstudie (WASH-1400)  
IRS-I-87/MRR-I-65, April 1976
- /F3, 3-4/ Phillips, C.A.G., and R.G. Warwick:  
A Survey of Defects in Pressure Vessels Built to  
High Standards of Construction and its Relevance  
to Nuclear Primary Circuit Envelops  
AHSB (S) R 162, UKAEA, 1968
- /F3, 3-5/ Smith, T.A., and R.G. Warwick:  
The Second Survey of Defects in Pressure Vessels  
Built to High Standards of Construction and its  
Relevance to Nuclear Primary Circuits  
SRD R 30, UKAEA, 1974
- /F3, 4-1/ Schadensstatistische Auswertungen zum Versagen me-  
chanisch beanspruchter Bauteile konventioneller  
Druckbehälter  
Forschungsvorhaben RS 217  
TÜV-Arbeitsgemeinschaft Kerntechnik West, Juni 1978

- /F3, 4-2/ Statusbericht: Reaktordruckbehälter, Band 2: Ausführliche Darstellung der Technik von Reaktordruckbehältern (Stand: Dezember 1973)  
Hrsg.: Institut für Reaktorsicherheit der Technischen Überwachungs-Vereine, Dezember 1976
- /F3, 4-3/ RSK-Leitlinien für Druckwasserreaktoren  
2. Ausgabe, 24. Januar 1979  
Gesellschaft für Reaktorsicherheit (GRS) mbH, 1979
- /F3, 4-4/ Analysis of Pressure Vessel Statistics from Fossil Fuelled Power Plant Service and Assessment of Reactor Vessel Reliability in Nuclear Power Plant Service  
WASH-1318, July 1974
- /F3, 4-5/ Marshall, W., et al.:  
An Assessment of the Integrity of PWR Pressure Vessels  
UKAEA, October 1976
- /F3, 7-1/ U.S. Nuclear Operating Experience  
in: Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,  
Appendix III: Failure Data, Table III 2-1: Data Assessment Tabulation  
WASH-1400 / NUREG 75/014, App. III, 1975
- /F3, 7-2/ Nuclear Plant Reliability Data System  
1976 Annual Report of System and Component Reliability,  
Joint Publication of ANSI (N 18-20), APPA EEI and USNRC, May 1977
- /F3, 7-3/ Green, A.E., and A.J. Bourne:  
Reliability Considerations for Automatic Protective System  
Nuclear Engineering 10 (1965) No. 8, p. 303

- /F3, 7-4/ Eames, A.R.:  
Reliability Assessment of Protective System  
Nuclear Engineering 11 (1966) No. 3, p. 188
- /F3, 7-5/ Green, A.E., and A.J. Bourne:  
Safety Assessment with Reference to Automatic  
Protective Systems for Nuclear Reactors  
AHSB (S) R 117, UKAEA, 1966
- /F3, 7-6/ Green, A.E.:  
Reliability Prediction  
ASHB (S) R 164, UKAEA, 1969
- /F3, 7-7/ Bourne, A.J.:  
Reliability Assessment of Technological Systems  
System Reliability Service, UKAEA, October 1971
- /F3, 7-8/ Farmer, F.R.:  
Siting Criteria - A New Approach  
inhaltsgleich mit: Reactor Safety and Siting: A Pro-  
posed Risk Criterion Nuclear Safety 8 (1966/67)  
No. 6, p. 539
- /F3, 7-9/ Earles, D.R.:  
Reliability Application and Analysis Guide  
MI-60-54 (Rev.1), The Martin Company, July 1961;  
Datenaufstellung in HN-190 (Kap. C 5) abgedruckt
- /F3, 7-10/ Garrick, B.J., et al.:  
Reliability Analysis of Nuclear Power Plants Pro-  
tective System  
HN-190, Holmes & Narver, Inc., May 1967
- /F3, 7-11/ Garrick B.J., et al.:  
Collection of Reliability Data at Nuclear Power  
Plants  
HN-199, Holmes & Narver, Inc., December 1968

- /F3, 7-12/ Anyakora, S.N., G.F.M. Engel and F.P. Lees:  
Some Data on the Reliability of Instruments in the  
Chemical Plant Environment  
The Chemical Engineer (1971) No. 255,  
p. 396
- /F3, 7-13/ Shopsky, W.E.:  
Review of Available Failure Rates for ECCS Compo-  
nents  
Letter to D.F. Paddleford, 20.10.1972
- /F3, 7-14/ Davies, F.M.:  
A Worked Example on the Use of Reliability Anal-  
ysis Techniques, Decay Heat Removal  
Lecture No. 58, Reactor Assessment, Section I  
Safety and Reliability Directorate (SRD)
- /F3, 7-15/ Bourne, A.J., E.R. Snaithe and D. Fletcher (CEGB):  
Reliability Analysis of Electrical Supply Systems  
for Nuclear Power Stations  
ENEA/CSNI Meeting of Specialists on the Reliabili-  
ty of Electrical Supply Systems and Related Elec-  
tro-Mechanical Components for Nuclear Reactor Safe-  
ty, Ispra, June 27-28, 1968
- /F3, 7-16/ Mize, G., and J. Eßmann (IRS):  
Reliability Analysis of the Emergency Power Supply  
System  
ENEA/CSNI Meeting of Specialists on the Reliabili-  
ty of Electrical Supply Systems and Related Elec-  
tro-Mechanical Components for Nuclear Reactor Safe-  
ty, Ispra, June 27-28, 1968
- /F3, 7-17/ Hake, G. (AECL):  
AECL's Requirements for Station Power Supplies  
ENEA/CSNI Meeting of Specialists on the Reliabili-  
ty of Electrical Supply Systems and Related Elec-  
tro-Mechanical Components for Nuclear Reactor Safe-  
ty, Ispra, June 27-28, 1968

- /F3, 7-18/ Tashjian, B.M.:  
Sensitivity Analysis of a Two-out-of Four Coincidence Logic Reactor Protective Systems  
IEEE Transactions on Nuclear Science, NS-18,  
February 1971, p. 455
- /F3, 7-19/ Salvatori, R.:  
Systematic Approach to Safety Design and Evaluation  
IEEE Transactions on Nuclear Science, NS-18,  
February 1971, p. 495
- /F3, 7-20/ Headington, W.L., M.E. Stewart and J.O. Zane:  
Fault Tree Analysis of the PBF Transient Rod Drive System  
IDO-17272, Phillips Petroleum Company, Atomic Energy Division, November 1968
- /F3, 7-21/ Bourne, A.J., G. Hensley, A.R. Eames et al.:  
Reliability Assessment of the S.G.H.W.R. Liquid Shutdown System  
AHSB (S) R 144, UKAEA, 1968
- /F3, 7-22/ Otway, H.J., R.K. Lohrding and M.E. Battat:  
A Risk Estimate for an Urban-Sited Reactor  
Nuclear Technology 12 (1971) No. 2, p. 173
- /F3, 7-23/ Antocisco, S., G. Tenaglia and A. Valeri (CNEN):  
A Theoretical Reliability Assessment of a Fire Protection System  
Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Reactor Safety  
Risø Report No. 214, February 1970, p. 22

- /F3, 7-24/ Bastl, W., H. Gieseler (LRA) and H.A. Maurer (CEC):  
The Reliability of Emergency Core Cooling Systems of Light Water Nuclear Power Plants  
Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Reactor Safety  
Risø Report No. 214, February 1970, p. 91
- /F3, 7-25/ Huppmann, H. (Allianz):  
Häufigkeit und Ursachen von Schäden an Bauteilen großer Dampfturbinen  
Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Reactor Safety  
Risø Report No. 214, February 1970, p. 171
- /F3, 7-26/ Hennings, U. (BBK):  
Auslegung und Anordnung einer Reaktor-Beschickungsanlage aufgrund von Zuverlässigkeitsbetrachtungen  
Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Reactor Safety  
Risø Report No. 214, February 1970, p. 213
- /F3, 7-27/ Ehrentreich, J., and H. Maurer:  
Reliability Considerations for Mechanical Components of Control Rod Drive Systems of Gas-Cooled Power Reactors Operated in the European Community  
Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Reactor Safety  
Risø Report No. 214, February 1970, p. 481
- /F3, 7-28/ Sexton, I.B.:  
Failure Rate Estimate of Some Nuclear and Conventional Power Plant Components  
AI-67-TDR-15-REV, Atomics International, 1968



- /F3, 7-29/ IEEE Guide to the Collection and Presentation of Electrical, Electronical and Sensing Component, Reliability Data for Nuclear Power Generating Stations  
IEEE Standard 500-1977
- /F3, 7-30/ Interne Mitteilung  
KWU Erlangen, 18.10.1971
- /F3, 7-31/ van Zylstra, E.H.:  
Recommended Component Failure Rates for Reliability Analysis
- /F3, 7-32/ Interne Mitteilung, betrifft: Untersuchungen für verschiedene Ventiltypen  
RWE Essen, 1975
- /F3, 7-33/ VDEW Störungs- und Schadensstatistik 1972  
Hrsg.: Vereinigung Deutscher Elektrizitätswerke (VDEW), Frankfurt/Main, 1975
- /F3, 7-34/ Hömke, P., und H. Krause:  
Eigene Auswertung des Modellfalles IRS-RWE (unveröffentlicht)
- /F3, 7-35/ Earles, D.R., and M.F. Eddins (General Electric):  
Reliability Physics  
9th National Symposium on Reliability and Quality Control, San Francisco, 1963
- /F3, 7-36/ Ausfallratenstatistik  
Hrsg.: Schoppe und Faeser, Minden, 1973 und 1976
- /F3, 7-37/ Balfanz, H.P.:  
Ausfallratensammlung  
IRS-W-8, Dezember 1973

- /F3, 7-38/ Bartels, G.:  
Wirtschaftliches Instandhalten von Meß-, Steuer-  
und Regelanlagen in Chemiebetrieben  
Bayer Leverkusen, 1977
- /F3, 7-39/ RADC Reliability Notebook, Volume II  
Rome Air Development Center, New York, 1967
- /F3, 7-40/ Shopsy, W.E.:  
Review of Available Failure Rates for ECCS Compo-  
nents  
Letter to D.F. Paddleford, 20.10.1972
- /F3, 7-41/ Dorey, J., and B. Gachot:  
Pump Reliability Data Derived from Electricité de  
France Operating Experience  
Symposium on Inservice Data Reporting and Analysis,  
ANS Winter Meeting, San Francisco, December 1978
- /F3, 7-42/ Nuclear Plant Reliability Data System  
1976 Annual Report of System and Component Relia-  
bility,  
Joint Publication of ANSI (N 18-20), APPA EEI and  
USNRC, May 1977
- /F3, 7-43/ Technical Report on Operating Experience with BWR  
Pressure Relief Systems  
NUREG-0462, July 1978
- /F3, 7-44/ Parisian, R.W.:  
How Reliable are Today's Prime Movers Power  
January 14, 1970
- /F3, 7-45/ Crooks, J.L., and G.S. Vissing:  
Diesel Generator Operating Experience at Nuclear  
Power Plants  
OOE-ES-002, USAEC, June 1974

- /F3, 7-46/ Betriebserfahrungen mit Kernkraftwerken in der Bundesrepublik Deutschland  
Atom und Strom 22 (1976) Nr. 3, S. 68
- /F3, 8-1/ Nuclear Plant Reliability Data System  
1976 Annual Report of System and Component Reliability,  
Joint Publication of ANSI (N 18-20), APPA EEI and USNRC, May 1977
- /F3, 8-2/ Green, A.E., and A.J. Bourne:  
Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors  
AHSB (S) R 117, UKAEA, 1966
- /F3, 8-3/ Earles, D.R., and M.F. Eddins (General Electric):  
Reliability Physics  
9th National Symposium on Reliability and Quality Control, San Francisco, 1963
- /F3, 8-4/ Garrick, B.J., et al.:  
Reliability Analysis of Nuclear Power Plants Protective System  
HN-190, Holmes & Narver, Inc., May 1967
- /F3, 8-5/ Earles, D.R.:  
Reliability Application and Analysis Guide  
MI-60-54 (Rev. 1), The Martin Company, July 1961;  
Datenaufstellung in HN-190 (Kap. C 5) abgedruckt
- /F3, 8-6/ Headington, W.L., M.E. Stewart and J.O. Zane:  
Fault Tree Analysis of the PBF Transient Rod Drive System  
IDO-17272, Phillips Petroleum Company, Atomic Energy Division, November 1968
- /F3, 8-7/ Ausfallratenstatistik  
Hrsg.: Schoppe und Faeser, Minden, 1973 und 1976

- /F3, 8-8/ Balfanz, H.P.:  
Ausfallratensammlung  
IRS-W-8, Dezember 1973
- /F3, 8-9/ Bartels, G.:  
Wirtschaftliches Instandhalten von Meß-, Steuer-  
und Regelanlagen in Chemiebetrieben  
Bayer Leverkusen, 1977
- /F3, 8-10/ RADC Reliability Notebook, Vol. II  
New York: Rome Air Development Center, 1967
- /F3, 8-11/ Reactor Safety Study, An Assessment of Accident  
Risks in U.S. Commercial Nuclear Power Plants,  
Appendix III: Failure Data  
WASH-1400 / NUREG 75/014, App. III, 1975
- /F3, 8-12/ Schrüfer, E., H. Hammerschmidt, G. Lebelt et al.:  
Ausfallraten ausgewählter Bauelemente und Geräte  
der Leittechnik  
EMT 1/79  
München: Technische Universität München
- /F3, 8-13/ Nickau, E.:  
Abschätzung der Ausfallraten von digitalen Bau-  
steinen der Simatic-P-Baureihe  
MRR-I-28, September 1974
- /F3, 8-14/ Military Standardization Handbook, Reliability Pre-  
diction of Electronic Equipment  
MIL-HDBK-217B, U.S. Department of Defense,  
September 1974
- /F3, 8-15/ Nickau, E.:  
Abschätzung der Zuverlässigkeit von Steuerketten  
der Betätigungsebene  
MRR-121, April 1973

- /F3, 8-16/ Goßner, S.:  
Theoretische Untersuchung des Ausfallverhaltens  
eines dynamischen Grenzwertmelders  
MRR-143, Februar 1975
- /F3, 8-17/ Goßner, S.:  
Experimentelle Bestimmung des Betriebs- und Aus-  
fallverhaltens eines Trennverstärkers  
MRR-123, August 1973
- /F3, 9-1/ Reactor Safety Study, An Assessment of Accident  
Risks in U.S. Commercial Power Plants,  
Appendix III: Failure Data  
WASH-1400 / NUREG 75/014, App. III, 1975
- /F3, 9-2/ Fleming, K.N., P.H. Raabe, G.W. Hannaman et al.:  
HTGR Accident Initiation and Progression Analysis,  
Status Report, Volume II: AIPA Risk Assessment  
Methodology  
GA-A 13617, Vol. II, General Atomic, October 1975

11. STICHWORTVERZEICHNIS

A

Arbeitsauftrag 54, 60  
ATWS-Störfälle 25

Ausfall

- Änderungs- bzw. Drift- 106
  - aktiver 106
  - "common mode" 37, 87
  - Früh- 38, 40
  - Hauptspeisewassersystem 25, 61
  - Mehrfach- 106, 109
  - nicht selbstmeldender 106
  - Notstromdiesel 61
  - passiver 106
  - Reaktorschnellabschaltung 25
  - selbstmeldender 106
  - Sicherheitsventile 61
  - Steuerstäbe (Nichteinfahren) 61
  - Umleitstation 61
  - unabhängiger 37
  - Verschleiß- 40
  - Zufalls- 38
- Ausfallart 37, 41, 43, 46
- leittechnische Komponenten 95
- Ausfalleffektanalyse 40, 43, 94, 100, 101, 103, 104
- Elektronikarten (leittechnische Systeme) 94, 100
  - experimentelle 107
  - mit Netzwerkanalyseprogramm 108
  - theoretische 107
- Ausfallrate 37, 46, 47, 52, 56, 57, 59, 62, 69
- Abzweige 92
  - "Badewannen"-Kurve 38
  - Differenzdruckmesser 96
  - Differenzdruck- und Druckmeßumformer 94, 96
  - Elektromotoren 91
  - Elektronikarten 100
  - elektronische Bauelemente 94, 103, 105, 107, 112
  - Ermittlung durch Ausfalleffektanalyse 104
  - Frischdampfschnellschlußschieber 92
  - Generatorschalter 93
  - Handarmaturen 79
  - Leistungsanschlüsse 102
  - Leistungsschalter 93
  - Magnetventile 75
  - Meßkanäle 95
  - Motorarmaturen 73
  - nicht steckbare Verbindungen 102
  - Notstromdieselbetriebsversagen 86
  - Notstromdieselstartversagen 85
  - pneumatische Ventile 76
  - Pumpenbetriebsversagen 72
  - Pumpenstartversagen 69
  - Regelarmaturen 79
  - Relais 94, 95, 96
  - Rohrleitungen 84
  - Rückschlagarmaturen
    - innere Leckage 77
    - Öffnen 76
    - Schließen 77
    - mit Motorantrieb 78
  - Schätzformel 59
  - Sicherheits- und Entlastungsventile 80
  - Sicherungen 95
  - Steuerstäbe 89
  - Umschaltventile 91
- Ausfallverhalten 37, 41, 59
- Zeitabhängigkeit 39
- Ausfallwahrscheinlichkeit 36, 48, 52, 56, 57, 59, 62, 96, 101

- Erwartungswert 72
- Teilstränge 63
- Verteilung 62
- Vertrauensintervall 62

B

- Belastungsfaktor 109, 111  
Beobachtungsumfang 52  
Betriebserfahrungen 14, 18, 21, 23, 24, 26, 36, 38, 40, 43, 46, 52, 61, 67, 69, 94, 99, 100, 102, 114
- Beobachtungsumfang 62
- Betriebsjahre 94  
Betriebszeit 38

C

- "common mode"-Ausfall 37, 87
- Hardware 112
  - Leittechnik 112
  - menschliche Fehlhandlungen 112
  - Meßumformer 112
  - Notstromdiesel 88
  - Relais (Reaktorschutzsystem) 112, 115

D

- Daten
- Streubreite 43, 45
- Datenbank
- Auslegung und Betrieb 53
- Druckhalter
- kleines Leck 22
- Druckhalterabblaseventil
- Kühlmittelverlust 22
  - Öffnen 23, 61

E

- Eintrittshäufigkeit
- auslösender Ereignisse 13
  - Kühlmittelverluststörfälle 17, 22
- Expertenurteil 46

F

- "fail safe"-Verhalten 106  
Fehlbedienung (Komponenten) 37  
Fehler
- selbstmeldende 59
- Fehlerbaumanalyse 36, 37, 43, 45, 47, 52, 57, 59, 63, 71, 73, 79, 80, 85, 92, 95, 100, 112
- Fehlerentdeckung 59  
Fehlerentdeckungszeit 107  
Fehlhandlungswahrscheinlichkeit
- Operator 117
- Freischaltbücher 54  
Funktionsprüfung 53
- Prüfanweisung 53
  - Prüfprotokoll 53

H

- Hauptkühlmittelleitung
- großes Leck 13
  - mittleres Leck 13
  - kleines Leck 13, 18, 20
  - sehr kleines Leck 13, 20

- I
- Instandhaltungsarbeiten 54
  - maßnahmen 66
  - Instandsetzungs- und Wartungszeiten 36
- K
- Komponenten
  - verfahrens- und elektrotechnische 69
- Komponentenausfall
  - unentdeckter 67
- Konservativität 46, 101, 102
- Korrekturfaktoren 44
- Kühlmittelverluststörfall 13, 18, 21, 84
- L
- Leckage
  - absperzbare 14
- Leittechnische Komponenten
  - Fehlerbaumanalyse 100
  - Schadensfälle im konventionellen Bereich 99
- Leittechnische Systeme 94
  - Ersatzausfallraten 112
- Literaturdaten 40
  - Zuverlässigkeitskenngrößen 44, 69, 71
    - Gewichtung 44
    - Stichprobe 44, 61
- Logarithmische Normalverteilung 48, 69
  - Dichtefunktion 49, 50
  - Erwartungswert 49
  - Fraktile 49
  - "maximum-likelihood"-Schätzfunktion 50
  - Medianwert 49
  - Mittelwert 49
  - Parameterschätzung 50
  - Standard- 49
  - Streufaktor 50, 95
  - Streuung 49
  - Verteilungsfunktion 50
  - Vertrauensbereich 95
  - Vertrauensintervall 95
- M
- Medianwert 95
- Menschliche Fehlhandlung (Operator) 117
- N
- Nichtverfügbarkeit 52, 54
  - Teilstränge 66
  - Zeit 60
- Notstromfall 24
- P
- Prüfintervall 36
- Pumpen
  - Startversagen 69
- R
- Reaktordruckbehälter
  - Auslegung 29
  - Bauprüfung 32
  - Betriebsüberwachung 32
  - Bruchmechanik 34
  - Bruchstücke, geschoßartige 34
  - Einhängeprobe 33
  - Erstdruckprüfung 32
  - Fehlerstellen 30
  - Fertigung 31
  - Grundwerkstoff 31
  - Konstruktion 29
  - Membranspannung 29
  - Neutronenbestrahlung 33
  - Prüfungen, wiederkehrende 31, 32
  - Prüfungen, zerstörungsfreie 30, 32
  - Qualitätssicherung 29
  - Ribbildung 31
  - Überhitzungsbereich 31
  - Ultraschallprüfung 32
  - Unterschiede zum konventionellen Druckbehälter 28, 34
  - Verformung, plastische 34
  - Versagen 26
  - Versagenshäufigkeit 33
  - Wärmeeinflußzone 31
  - Werkstoffwahl 30
  - Zähigkeit, integrale 31, 33
  - Zerknall, katastrophaler 33
- Reaktorschnellabschaltung 61, 89, 114, 116
- Reaktorschutzqualität 104
- Reaktorschutzsignal 116
- Reparaturzeit 52, 54, 60, 64
  - maximal zulässige 36
- S
- Schichtbuch 54
- SIMATIC P (Leittechnisches System) 101, 109
  - "stand by"-Komponenten 37
- Störberichte 61
- Störfallaufanalyse 85
- Strefaktoren 41
- Summenhäufigkeitskurve
  - Literaturdaten 95
- T
- Three Mile Island (TMI) 22
- Transiente 22, 24, 61
- U
- Überlastung (Komponenten) 37
- V
- Verfügbarkeit 36
- Volumenregelsystem 14, 20
- W
- Wahrscheinlichkeitsnetz
  - doppeltlogarithmisches 95
- Wartungs- und Instandhaltungsarbeiten 59
  - Dokumentation 61
  - Not- und Nachkühlssysteme 60
  - nukleare Zwischen- und Nebenkühlwasserkreisläufe 60
- WASH-1400 43, 86, 89, 95, 115
- Wiederkehrende Prüfungen 53
  - Gebäudeabschluß, lufttechnische Anlagen 58
  - Notstromanlage 58
  - Not- und Nachkühlssysteme 58
  - nukleare Zwischen- und Nebenkühlwasserkreisläufe 58
  - Prüfintervall 57, 64, 72
  - Prüfprotokoll 54, 60
  - Prüfrücksetzung 55
  - Prüfschritt 54
  - Prüfumfang 54
  - Prüfungsstörablaufprotokoll 54
  - Prüfvorbereitung 55, 58
  - Systemprüfung 55
- Wirksamkeitsanforderungen 13

Z

- Zuverlässigkeitsanalyse 44
- Zuverlässigkeitskenngrößen 36, 40, 43, 52, 63
  - Betriebserfahrungen 94
  - elektronische Bauelemente 94
  - Korrekturfaktoren 95
  - leittechnische Komponenten 94, 99
  - Literaturdaten 94
  - verfahrens- und elektrotechnische Komponenten 69



Zusammenstellung von Zuverlässigkeitskenngrößen

## Anmerkung:

In den Tabellen sind z.T. mehrere Literaturstellen zu einer Spalte zusammengefaßt, z.B. Vorträge, die auf einer Tagung gehalten wurden und daher im Tagungsbericht zusammen abgedruckt sind. In den Schrifttumshinweisen ist in solchen Fällen z.B. /F3, A1-15 bis -17/ angegeben. In den Bildern wird der gleiche Sachverhalt mit einem Schrägstrich zwischen den Ziffern, z.B. (15/17) gekennzeichnet. Stammen mehrere unabhängige Werte aus der gleichen Quelle, z.B. (34), dann sind diese Fälle in den Bildern wie folgt vermerkt: (34,1), (34,2) usw. In Bild F3, A1-8 werden die Werte aus Betriebserfahrungen durch den Hinweis (B) von Literaturwerten, z.B. (2), (13) usw. unterschieden.

INHALT

	Seite
Tabellen:	
F3, A1-1: Zusammenstellung der aus der Literatur entnommenen Zuverlässigkeitskenngrößen	A1-5
F3, A1-2: Zur Festlegung der Verteilungen verwendete Werte der Zuverlässigkeitskenngrößen aus der Literatur . . . . .	A1-9
Bilder . . . . .	A1-13
F3, A1-1: Pumpe, Startversagen	
F3, A1-2: Pumpe, Betriebsversagen	
F3, A1-3: Motorarmatur, öffnet oder schließt nicht	
F3, A1-4: Magnetventil, öffnet oder schließt nicht	
F3, A1-5: Pneumatisches Ventil, öffnet oder schließt nicht	
F3, A1-6: Rückschlagarmatur, öffnet nicht	
F3, A1-7: Rückschlagarmatur, schließt nicht	
F3, A1-8: Handarmatur, öffnet oder schließt nicht	
F3, A1-9: Regelarmatur	
F3, A1-10: Sicherheits- und Entlastungsventil	
F3, A1-11: Elektromotor, Startversagen	
F3, A1-12: Elektromotor, Betriebsversagen	
F3, A1-13: Leistungsschalter	
F3, A1-14: Dichtung, Leckage	
F3, A1-15: Schütz, Verlust der Hauptfunktion	
F3, A1-16: Transformator	
F3, A1-17: Meßumformer mit Bartonzelle	
F3, A1-18: Relais	
Schrifttum . . . . .	A1-33

Tabelle F3, A1-1

Zusammenstellung der aus der Literatur entnommenen  
Zuverlässigkeitskenngrößen

**Zum Verständnis der folgenden 7 Tabellen bitte  
die Falttafel auf Seite A1-7 (8) ausklappen.**

A1-7 (1)

/F3, A1-1/ Betriebserfahrung nuklear (US)	/F3, A1-2/	/F3, A1-3 bis -8/	/F3, A1-9/	/F3, A1-10/	/F3, A1-11/
1,0 E-3/A	5,3 E-6	6,8 E-4	1,4 E-5	1,0 E-5	8,5 E-5
3,0 E-6	1,0 E-5			5,0 E-6	1,0 E-4
1,0 E-3/A	4,5 E-6			1,0 E-5	9,5 E-6
1,0 E-3/A	3,1 E-6	3,0 E-5	1,1 E-5		
1,0 E-4/A	5,2 E-6	2,9 E-5 2,1 E-4 1,1 E-4		1,0 E-7	5,7 E-5
1,0 E-4/A	6,8 E-8 3,2 E-6		5,0 E-6		1,4 E-5
	1,5 E-6 3,7 E-6			1,0 E-6	
	1,4 E-6 1,0 E-7			1,0 E-7	
3,0 E-5/A	5,6 E-7	1,5 E-5			
	6,3 E-6 7,6 E-6 6,0 E-6	3,0 E-5	8,5 E-6		6,8 E-5
	1,2 E-5 6,8 E-6 6,6 E-6			6,8 E-5	
1,0 E-5/A	8,9 E-7	5,0 E-7	5,7 E-6		
1,0 E-5	1,1 E-6	2,0 E-6			
	2,9 E-6				
3,0 E-10/m		2,0 E-7			
3,0 E-9/m		2,0 E-7			
1,0 E-6		5,0 E-7	5,0 E-8		
3,0 E-2/A	2,4 E-5	1,0 E-3			
1,0 E-3	1,8 E-4				
5,0 E-5/A bis 3,0 E-4/A					
3,0 E-4/A	2,6 E-6 1,8 E-6 1,4 E-6	1,0 E-5	3,0 E-7		8,5 E-6
1,0 E-6	1,6 E-6 8,8 E-6 3,0 E-6			8,5 E-6	
	7,7 E-7 1,0 E-7	3,0 E-6	2,5 E-7		
1,0 E-3/A	2,0 E-7 8,7 E-7 3,9 E-7	2,0 E-6	1,4 E-7		
1,0 E-3/A	2,0 E-7 2,9 E-7 3,2 E-7				
2,0 E-6	7,8 E-7	9,0 E-6	1,0 E-6	5,0 E-6	
		5,0 E-6	5,0 E-7		
1,0 E-6/A					

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet

A1-7 (2)

/F3, A1-12/ Chemische Industrie	/F3, A1-13/	/F3, A1-14/	/F3, A1-15 bis -17/		/F3, A1-18 bis -19/
	1,5 E-5 1,7 E-5				
	8,6 E-6 8,2 E-6				
4,8 E-5					
3,4 E-5	3,2 E-6				
	1,2 E-6				
	2,0 E-6 2,4 E-6				
3,4 E-5		3,4 E-6			
	1,6 E-5				
	4,0 E-7	3,7 E-12/m			
	4,0 E-7	3,7 E-12/m			
			1,0 E-4	1,0 E-2/A	
	6,0 E-6	3,7 E-6			
	3,2 E-6				
	6,0 E-7		2,0 E-7		3,6 E-6
	1,3 E-6		4,6 E-6 9,0 E-7	4,0 E-7 1,9 E-6	
	2,6 E-6				

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet

A1-7 (3)

/F3, A1-20/	/F3, A1-21/	/F3, A1-22/	/F3, A1-23 bis -27/		/F3, A1-28/
			4,5 E-6		1,4 E-5 2,9 E-6
		5,7 E-7			
7,5 E-6			1,5 E-6		3,4 E-6
	9,6 E-6		1,8 E-7		
7,5 E-6			1,5 E-6 1,8 E-6	1,2 E-5 4,3 E-6	1,5 E-6 3,0 E-5 2,0 E-6
			1,0 E-7		5,0 E-6 2,3 E-6
					1,1 E-7
			1,8 E-6		1,4 E-5 3,4 E-6 2,0 E-6
			4,6 E-7		1,1 E-5
		5,7 E-9	6,0 E-9/m		
			6,0 E-9/m		
			1,4 E-6		
		5,0 E-2/A		1,2 E-5	6,6 E-6 7,4 E-6 1,1 E-5 2,2 E-6 3,0 E-7 2,0 E-7

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet

A1-7 (4)

/F3, A1-29/	/F3, A1-30/		/F3, A1-31/		
			FARADA	Nuc1. Eng.	AIEE
	4,5 E-5 1,9 E-5	7,5 E-6 6,5 E-5			
1,0 E-5/A	2,6 E-6		1,4 E-5	4,6 E-6	
1,6 E-5/A					
2,8 E-6/A					
			5,0 E-6	5,0 E-6	
	2,1 E-6				
			1,4 E-5		
8,0 E-3/A					
1,3 E-4					
4,5 E-7 9,3 E-7	7,1 E-7				
8,5 E-7 1,2 E-6	1,1 E-6	2,0 E-6 3,6 E-6 3,7 E-6	1,2 E-6 2,7 E-5	4,3 E-6	3,0 E-7 4,3 E-6
1,3 E-7					
1,0 E-6/A					
3,3 E-4/A					
8,8 E-7					
1,3 E-8				5,0 E-7	
1,0 E-5/A					

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet

A1-7 (5)

/F3, A1-31/ Zylstra	/F3, A1-32/	/F3, A1-33/	/F3, A1-47/	/F3, A1-48/	/F3, A1-49 bis -51/ Betriebserfahrung TOV
			1,0 E-3/A		
3,1 E-6			1,0 E-3/A		
	6,9 E-7				
1,6 E-7 2,2 E-7					
1,6 E-6 2,2 E-6					
	1,1 E-5 8,2 E-6				
	1,1 E-5 2,0 E-6 8,2 E-6				
3,0 E-6		2,3 E-7			
	1,5 E-7				
		7,5 E-7			
1,2 E-6					
1,2 E-6					
					4,7 E-3/A 5,0 E-3/A 1,3 E-2/A
					2,6 E-3 3,7 E-3 1,6 E-2
				1,2 E-5/A	
1,0 E-5					
		8,5 E-8 1,7 E-7			
		2,4 E-7			
5,0 E-7					

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet



A1-7 (6)

/F3, A1-49 bis -51/ Betriebserfahrung USAEC/FNke	/F3, A1-52/ Eigenauswertung nuklear		/F3, A1-53/ konventionell		(WASH-1400, App. III/Smith) nuklear
	GEAP 4574		nuklear	konventionell	
	1,9 E-7 7,0 E-8	3,4 E-10/m	8,4 E-8	2,3 E-9	6,5 E-7
		3,4 E-10/m	1,5 E-6	6,8 E-8	1,9 E-6
7,0 E-2/A 4,0 E-2/A					8,7 E-3/A

Anmerkung: alle Ausfallraten in 1/h; Ausfallwahrscheinlichkeiten pro Anforderung durch /A gekennzeichnet



A1-7 (8)

Ausfallart	Komponente
Startversagen	Pumpe
Betriebsversagen	
öffnet nicht oder schließt nicht	Motorarmatur
öffnet nicht oder schließt nicht	Magnetventil
öffnet nicht oder schließt nicht	pneumatisches Ventil
öffnet nicht	Rückschlagarmatur
schließt nicht	
innere Leckage	
öffnet nicht oder schließt nicht	Handarmatur
fährt nicht auf	Regelarmatur
fährt nicht zu	
öffnet nicht	Entlastungsventil
öffnet fälschlich	
schließt nicht	
Bruch	Rohrleitung > 3"
Bruch	Rohrleitung < 3"
Leckage	Dichtung
Startversagen	Notstromdiesel
Betriebsversagen	
fällt nicht ein	Steuerstab
Startversagen	Elektromotor
Betriebsversagen	
	Schütz
schließt nicht	Leistungsschalter
öffnet nicht	
	Transformator
vorzeitige Unterbrechung	Sicherung
keine Auslösung	

Tabelle F3, A1-2

Zur Festlegung der Verteilungen verwendete Werte  
der Zuverlässigkeitskenngrößen aus der Literatur

**Zum Verständnis der folgenden 5 Tabellen bitte  
die Falttafel auf Seite A1-11 (6) ausklappen.**

A1-11 (1)

/F3, A1-1/ Betriebs erfahrung nuklear (US)	/F3, A1-2/	/F3, A1-3 bis -8/	/F3, A1-9/	/F3, A1-10/	/F3, A1-11/
	5,3 E-6	1,3 E-4	2,7 E-6	1,0 E-5	8,5 E-5
3,0 E-6	1,0 E-5	5,5 E-4	1,1 E-5	5,0 E-6	1,0 E-4
	4,5 E-6			1,0 E-5	9,5 E-6
	3,1 E-6	3,0 E-5	1,1 E-5		
	5,2 E-6	2,9 E-5 1,1 E-4 2,1 E-4		1,1 E-7	5,6 E-5
	6,8 E-8 3,2 E-6		1,8 E-6		4,9 E-6
	1,5 E-6 3,7 E-6		3,2 E-6	1,0 E-6	9,1 E-6
	1,5 E-6		1,8 E-6		
	1,0 E-6		3,2 E-6		
	1,0 E-5				
	5,6 E-7	1,5 E-5			
	6,0 E-6 6,3 E-6 7,6 E-6	1,5 E-5	4,3 E-6		6,8 E-5
	6,6 E-6 6,8 E-6 1,2 E-5	1,5 E-5	4,3 E-6		6,8 E-5
	8,9 E-7	5,0 E-7	1,0 E-6		
1,0 E-5	1,1 E-6	2,0 E-6	1,2 E-6		
	2,9 E-6		3,4 E-6		
1,0 E-6		5,0 E-7	5,0 E-8		
	1,4 E-6 2,6 E-6 1,8 E-6	3,0 E-6	9,1 E-8		8,5 E-6
1,0 E-6	1,6 E-6 8,8 E-6 3,0 E-6	7,0 E-6	2,1 E-7		8,5 E-6
	2,0 E-7 8,7 E-7 3,9 E-7	1,4 E-6	9,8 E-8		
	2,0 E-7 3,2 E-7 2,9 E-7	6,0 E-7	4,2 E-8		
	1,0 E-7 7,7 E-7	3,0 E-6	2,5 E-6		
2,0 E-6	7,8 E-7	9,0 E-6	1,0 E-6	5,0 E-6	

Anmerkung: alle Ausfallraten in 1/h

A1-11 (2)

/F3, A1-12/ Chemische Industrie	/F3, A1-13/	/F3, A1-14/	/F3, A1-15 bis -17/	/F3, A1-18 bis -19/	/F3, A1-20/
	2,9 E-6 3,2 E-6				
	1,2 E-5 1,4 E-5				
	8,2 E-6 8,6 E-6				7,5 E-6
4,8 E-5					
3,4 E-5	3,2 E-6				7,5 E-6
	4,2 E-7				
	7,8 E-7				
	2,0 E-6 2,4 E-6				
1,7 E-5					
1,7 E-5		3,4 E-6			
	2,9 E-6				
	3,6 E-6				
	9,5 E-6				
	1,8 E-6	1,1 E-6			
	4,2 E-6	2,6 E-6			
	4,2 E-7		1,4 E-7		
	1,8 E-7		6,0 E-8	3,6 E-6	
	3,2 E-6				
	1,3 E-6		4,6 E-6 4,0 E-7 9,0 E-7 1,9 E-6		

Anmerkung: alle Ausfallraten in 1/h

A1-11 (3)

/F3, A1-21/	/F3, A1-22/	/F3, A1-23 bis -27/		/F3, A1-28/	/F3, A1-29/
		4,5 E-6		5,5 E-7 2,7 E-6	
	5,7 E-7			2,3 E-6 1,2 E-5	
		1,5 E-6		3,4 E-6	
9,6 E-6		1,8 E-7			
		1,5 E-6 1,5 E-6	1,8 E-6 4,3 E-6 1,2 E-5	2,0 E-6 3,0 E-5	
		1,0 E-7		8,1 E-7 1,8 E-6	
				1,5 E-6 3,2 E-6	
				1,1 E-7	
		9,0 E-7		1,0 E-6 1,7 E-6 7,0 E-6	
		9,0 E-7		1,0 E-6 1,7 E-6 7,0 E-6	
		4,6 E-7		2,0 E-6	
				2,5 E-6	
				6,5 E-6	
		1,4 E-6			
			3,6 E-6	6,0 E-8 2,0 E-6 9,1 E-8 2,2 E-6 6,7 E-7 3,3 E-6	4,5 E-7 9,3 E-7 7,1 E-7
			8,4 E-6	1,4 E-7 1,5 E-6 2,1 E-7 4,6 E-6 7,7 E-6 5,2 E-6	8,5 E-7 1,2 E-6 1,1 E-6
					1,3 E-7
					8,8 E-7

Anmerkung: alle Ausfallraten in 1/h

A1-11 (4)

/F3, A1-30/		/F3, A1-31/				
		FARADA	Nucl. Eng.	AIEE	Zylstra	
8,6 E-6	1,4 E-6					
3,6 E-6	1,2 E-5					
3,6 E-5	6,1 E-6					
1,5 E-5	5,3 E-5					
2,6 E-6		1,4 E-5	4,6 E-6		3,1 E-6	
		1,8 E-6	1,8 E-6		1,6 E-7 2,2 E-7	
		3,2 E-6	3,2 E-6		1,6 E-6 2,2 E-6	
1,1 E-6						
1,1 E-6						
		2,5 E-6			7,0 E-7	
		3,1 E-6			1,5 E-7	
		8,3 E-6			2,3 E-6	
6,0 E-7	1,1 E-6	3,6 E-7	1,3 E-6	9,1 E-8	1,3 E-6	3,0 E-6
1,1 E-6		8,2 E-6				
8,4 E-7	2,6 E-6	1,9 E-5	3,0 E-6	2,1 E-7	3,0 E-6	7,0 E-6
2,5 E-6		1,4 E-6				

Anmerkung: alle Ausfallraten in 1/h



A1-11 (5)

/F3, A1-32/	/F3, A1-33/	/F3, A1-34/			
		vgl. F3, A1-1 und -2			
		3,5 E-5 6,4 E-5			
6,9 E-7					
		2,7 E-6			
		5,0 E-6			
8,2 E-6 1,1 E-5		3,2 E-5			
2,0 E-6 8,2 E-6 1,1 E-5		3,2 E-5			
2,3 E-7					
7,5 E-7					
		2,6 E-6			
		6,0 E-6			
	6,0 E-8 1,2 E-7	2,0 E-6			
	5,1 E-8 2,6 E-8	8,7 E-7			
		2,0 E-6 1,1 E-5			
	2,4 E-7				

Anmerkung: alle Ausfallraten in 1/h

A1-11 (6)

Ausfallart	Komponente
Startversagen	Pumpe
Betriebsversagen	
öffnet nicht oder schließt nicht	Motorarmatur
öffnet nicht oder schließt nicht	Magnetventil
öffnet nicht oder schließt nicht	pneumatisches Ventil
öffnet nicht	Rückschlagarmatur
schließt nicht	
öffnet nicht	Rückschlagarmatur mit Motorantrieb (ohne Motor)
schließt nicht	
innere Leckage	
öffnet nicht oder schließt nicht	Handarmatur
fährt nicht auf	Regelarmatur
fährt nicht zu	
öffnet nicht	Entlastungsventil
öffnet fälschlich	
schließt nicht	
Leckage	Dichtung
Startversagen	Elektromotor
Betriebsversagen	
schließt nicht	Leistungsschalter ohne Abzweig
öffnet nicht	
Verlust der Hauptfunktion	Schütz
	Transformator

Bilder F3, A1-1 bis -18

Ausfallratenverteilungen für verfahrens-,  
elektro- und leittechnische Komponenten

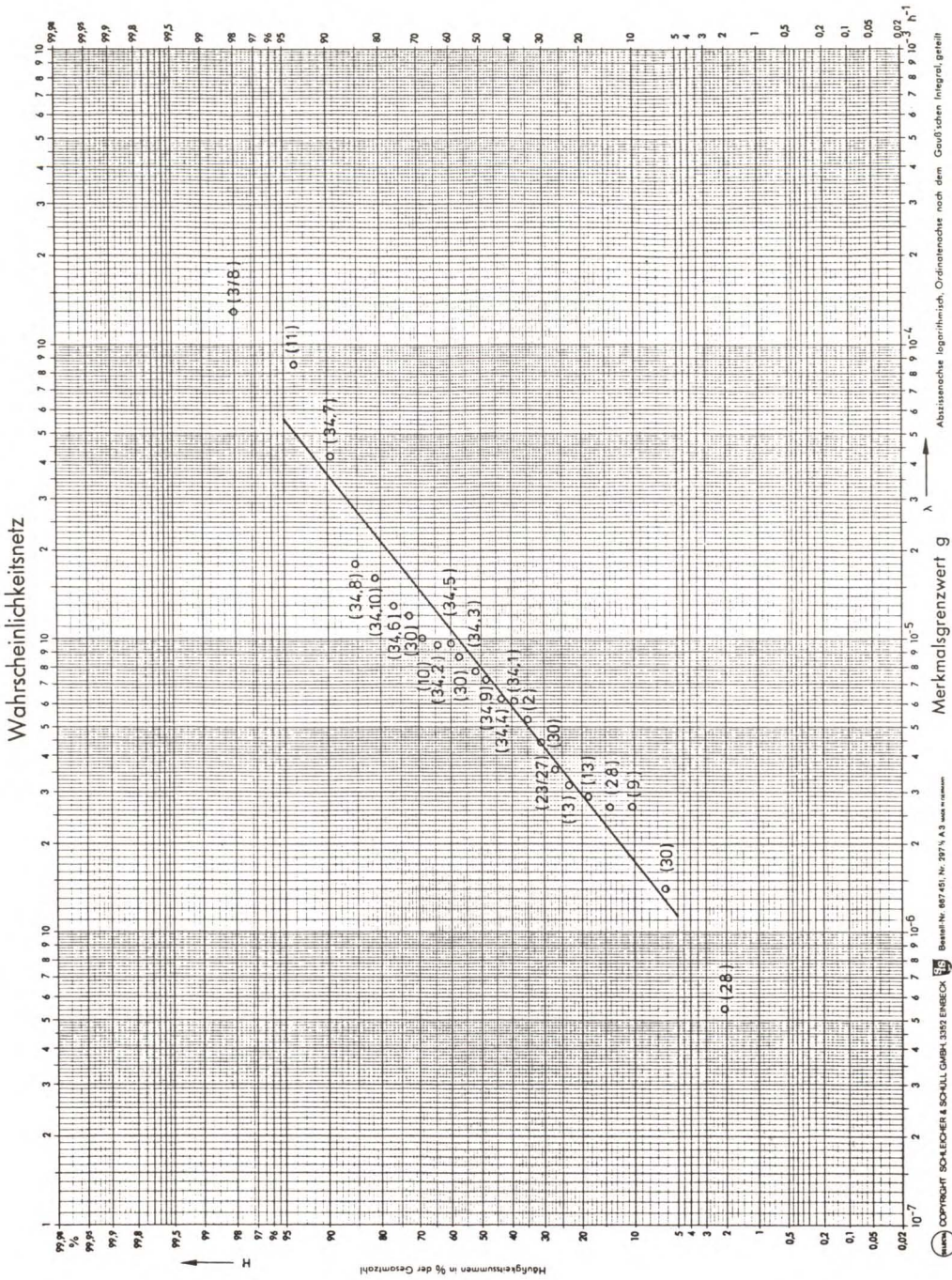
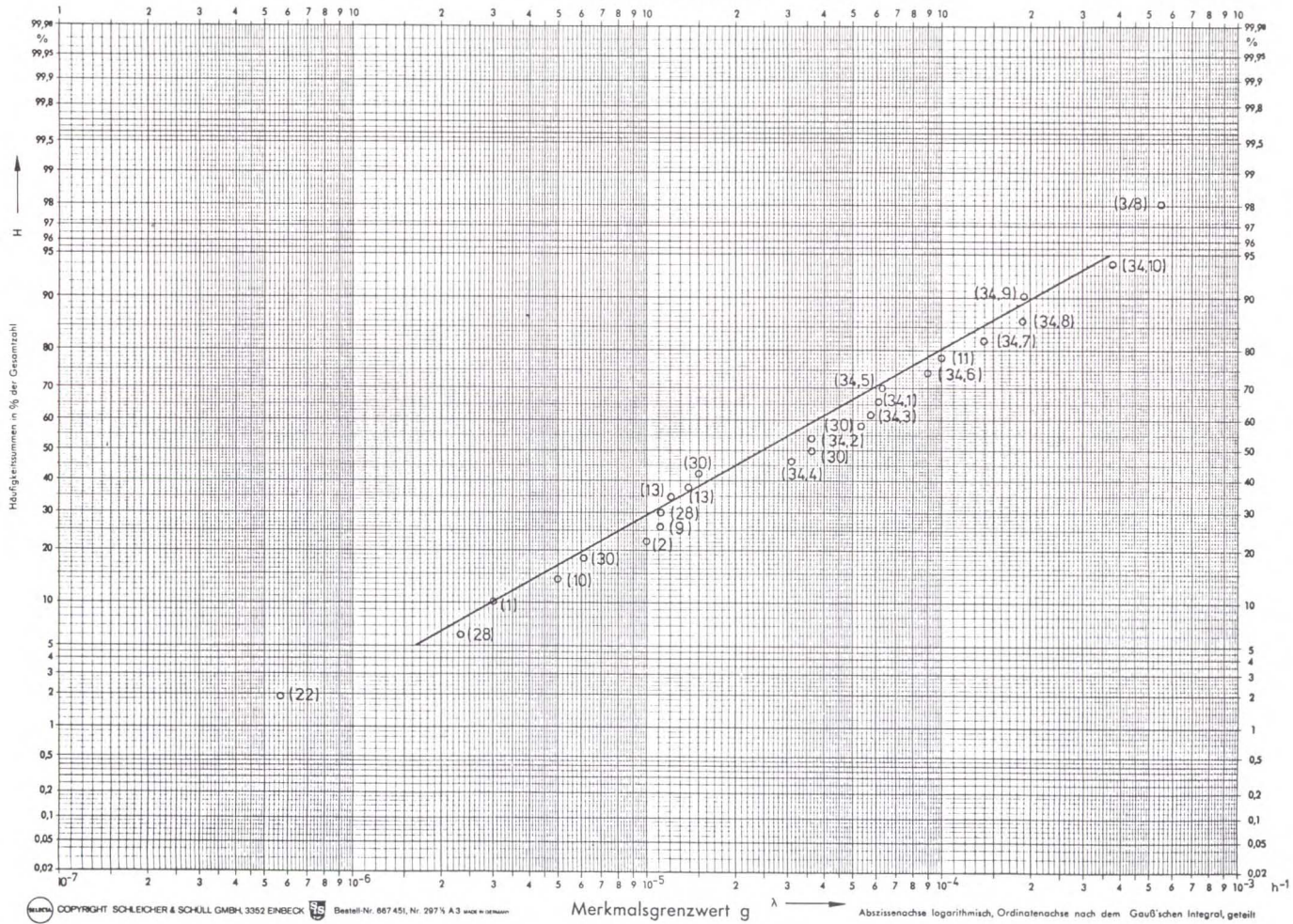


Bild F3, A1-1: Pumpe, Startversagen

# Wahrscheinlichkeitsnetz

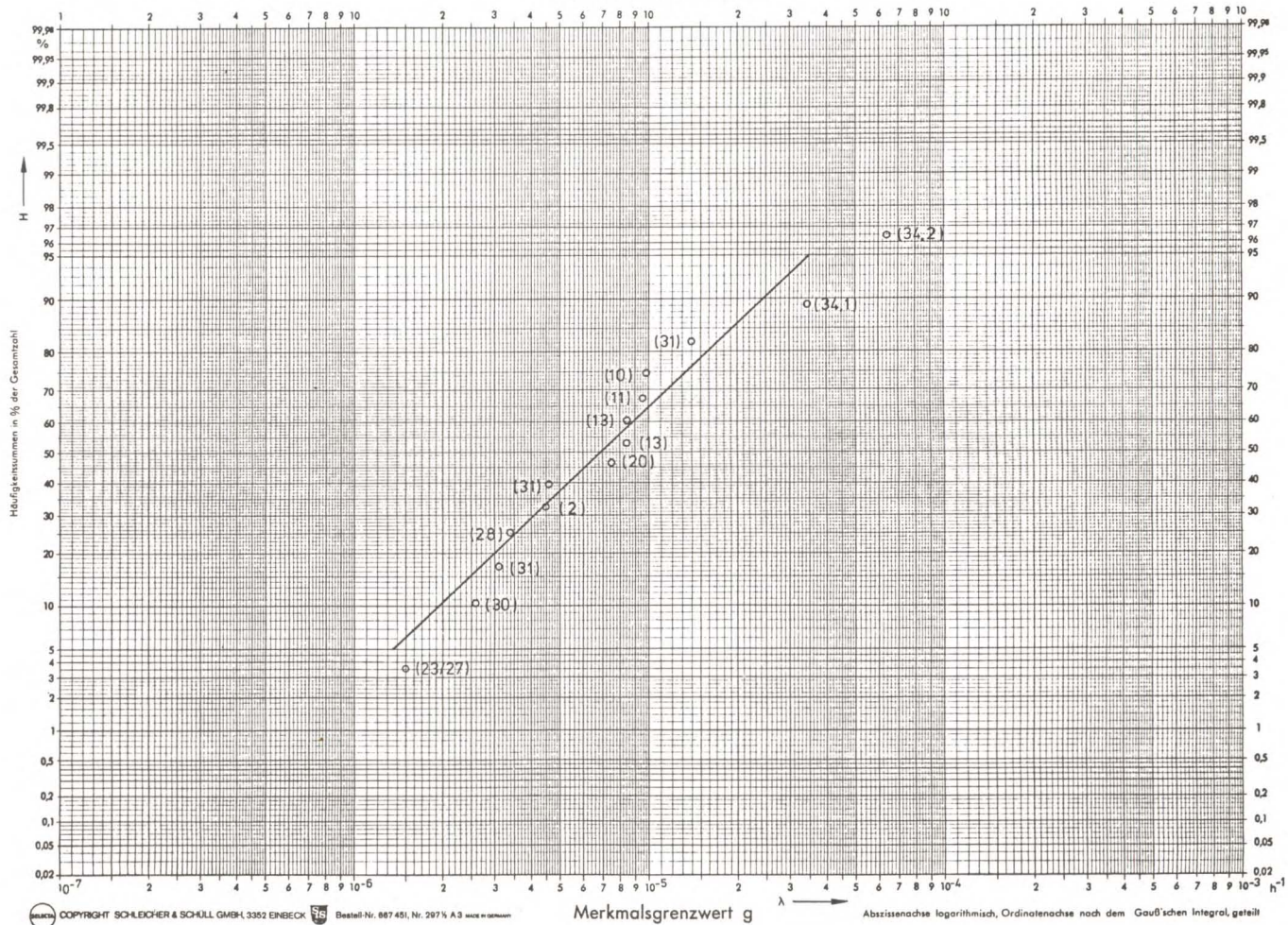


A1-16

Bild F3, A1-2: Pumpe, Betriebsversagen

COPYRIGHT SCHLEICHER & SCHÜLL GMBH, 3352 EINBECK Bestell-Nr. 667 451, Nr. 297 % A 3  $\lambda$   $\text{h}^{-1}$  Abzissennachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral, geteilt

# Wahrscheinlichkeitsnetz



COPYRIGHT SCHLEICHER & SCHÜLL GMBH L3352 EINBECK Bestell-Nr. 887 451, Nr. 297 % A3 nach DIN 52611
 Abszissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral geteilt

Bild F3, A1-3: Motorarmatur, öffnet oder schließt nicht

A1-17

# Wahrscheinlichkeitsnetz

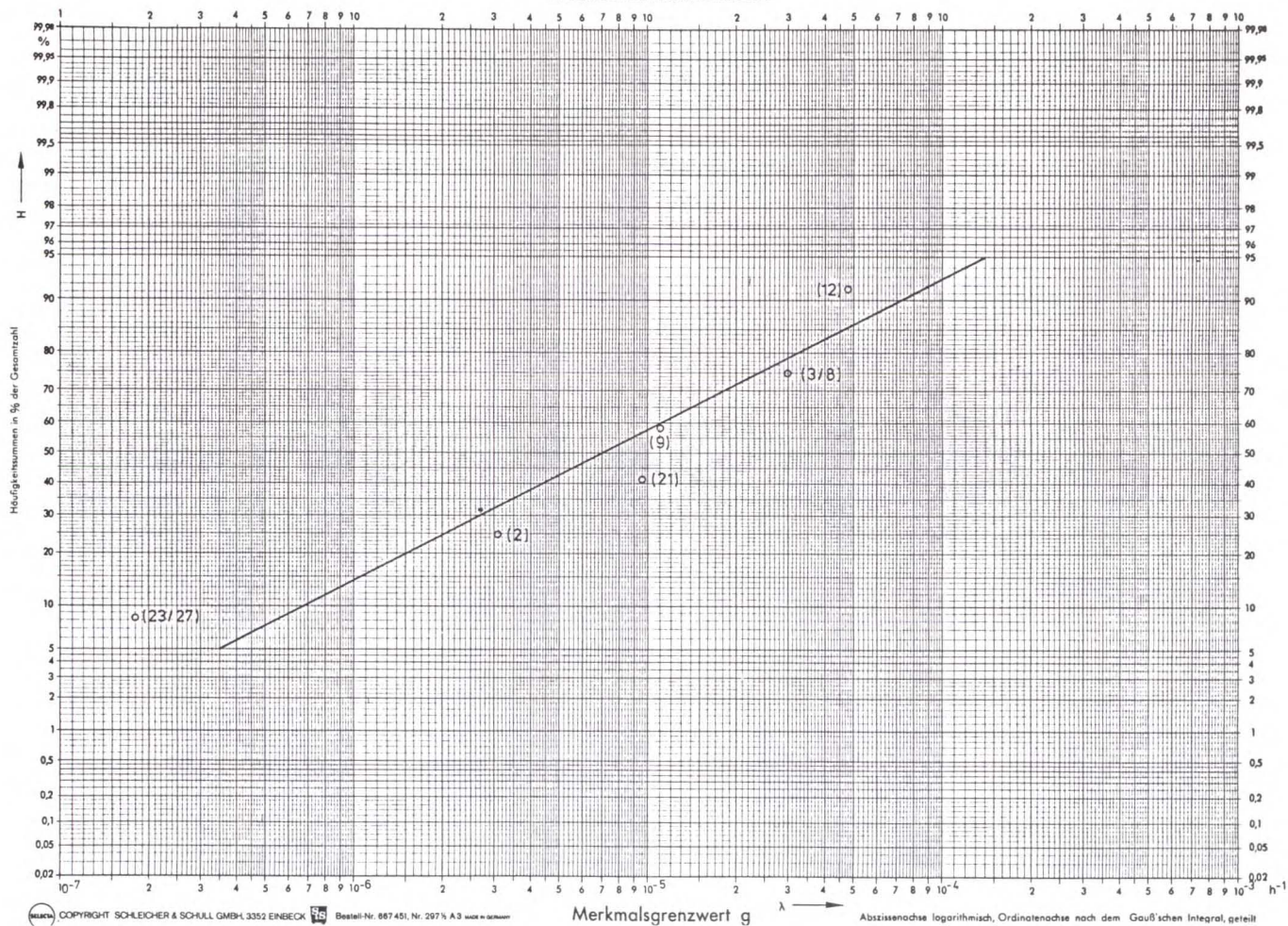
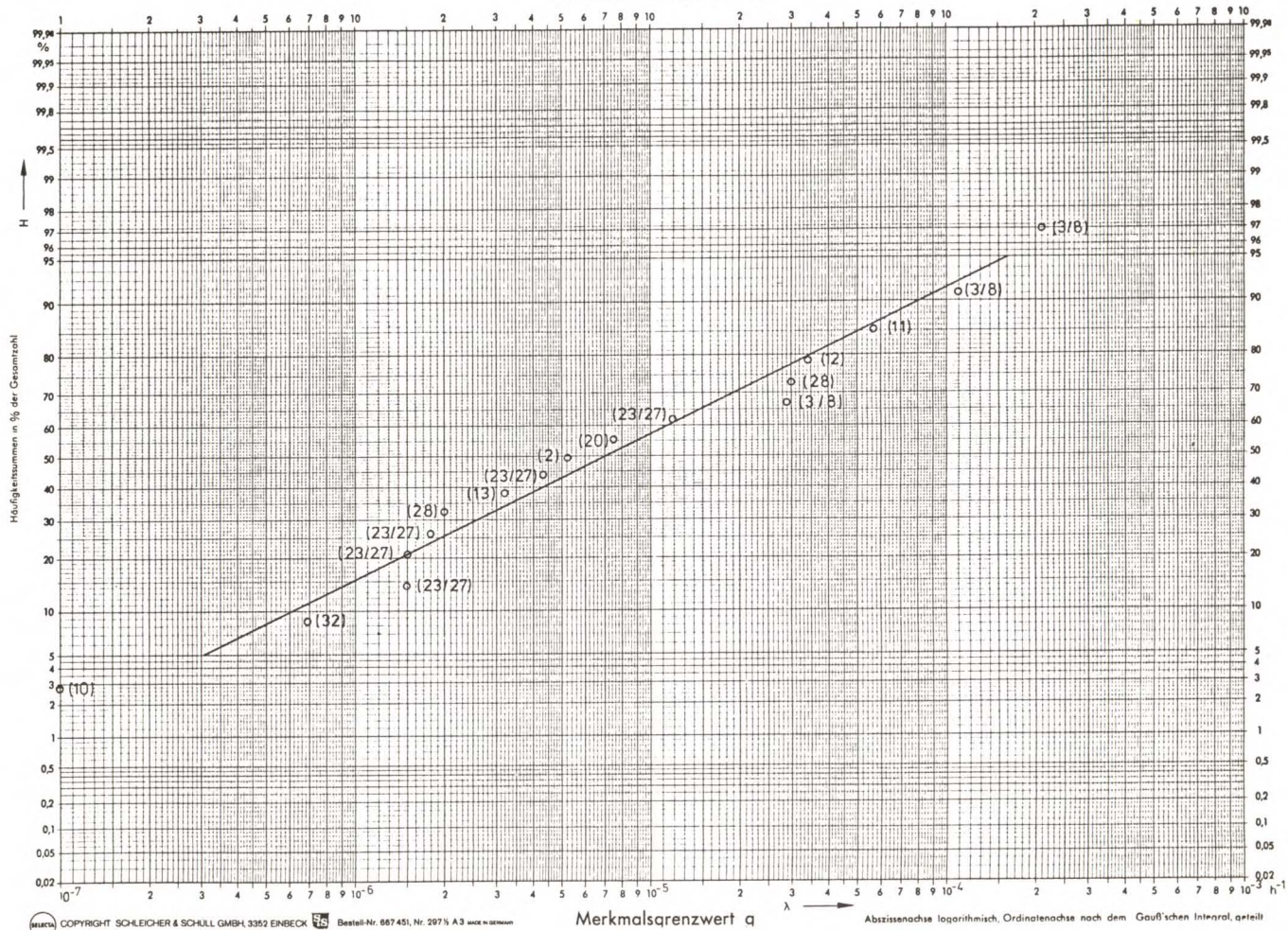


Bild F3, A1-4: Magnetventil, öffnet oder schließt nicht

# Wahrscheinlichkeitsnetz



Merkmalsgrenzwert  $\lambda$  Abszissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral, Anteil

Bild F3, A1-5: Pneumatisches Ventil, öffnet oder schließt nicht



# Wahrscheinlichkeitsnetz

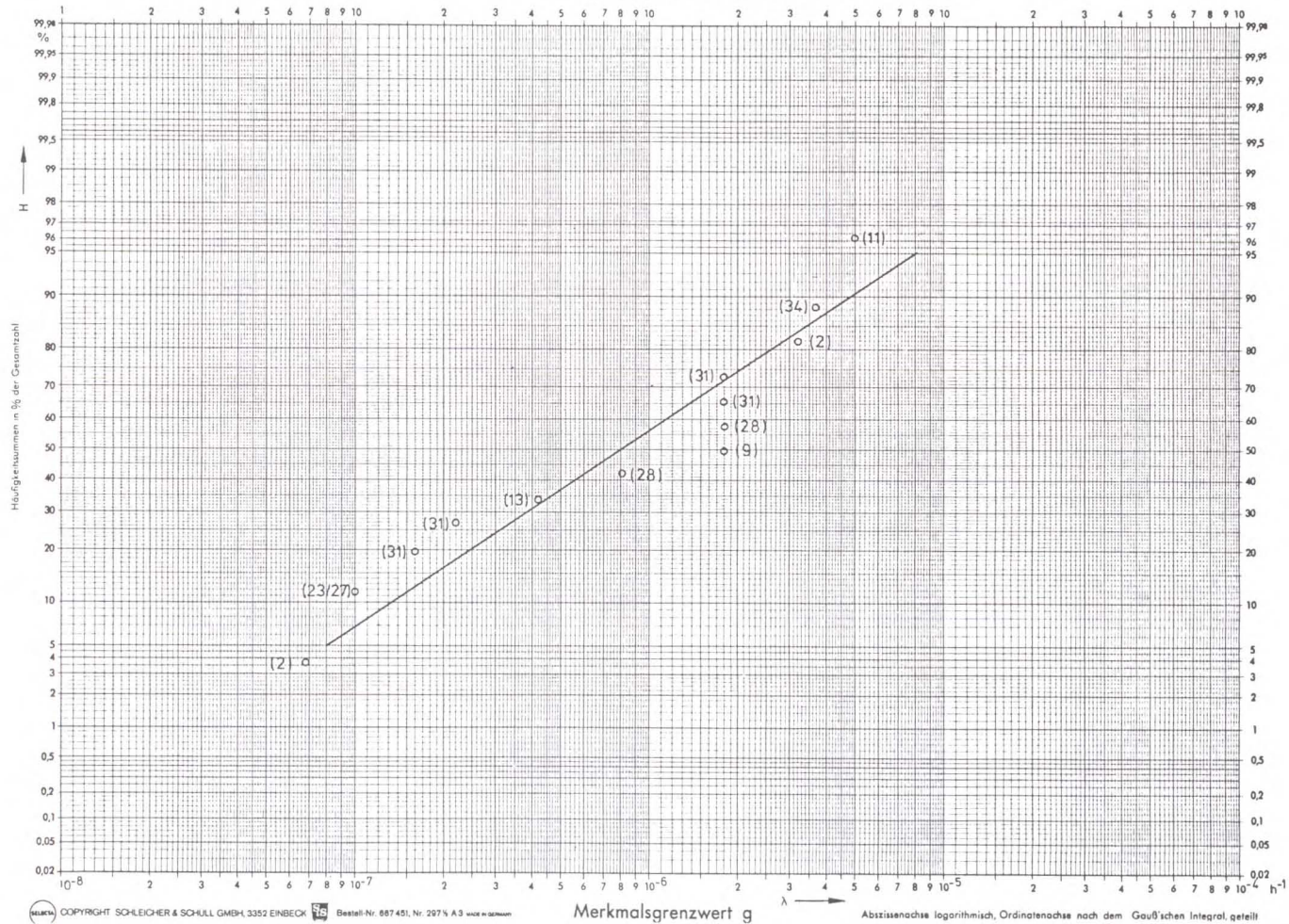
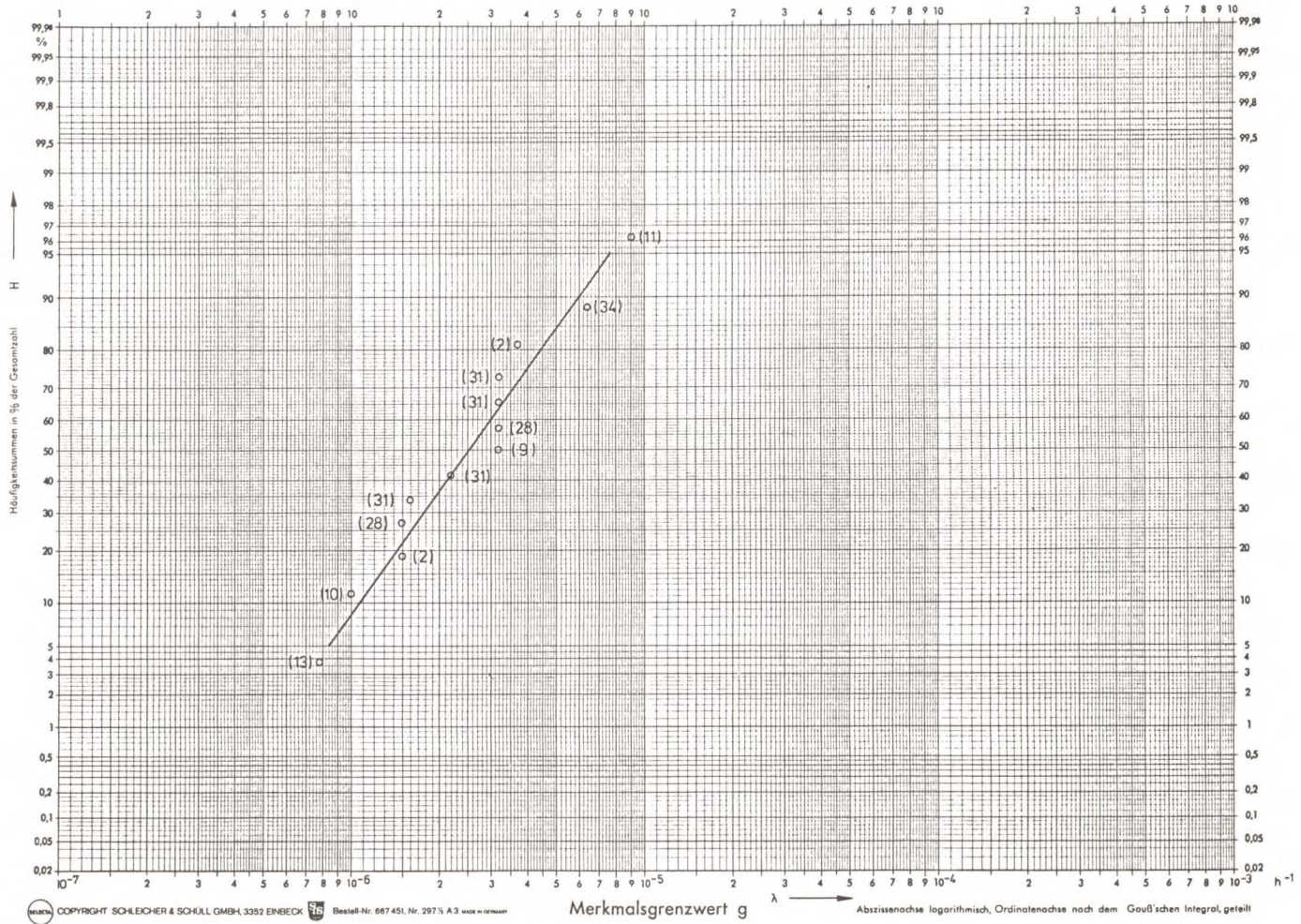


Bild F3, A1-6: Rückschlagarmatur, öffnet nicht

# Wahrscheinlichkeitsnetz



COPYRIGHT SCHLEICHER & SCHÜLL GMBH, 3352 EINBECK 
 Bestell-Nr. 867451, Nr. 297 % A3 siehe in Formeln

Merkmalsgrenzwert  $g$   $\lambda$   $\rightarrow$  Abszissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral, geteilt  $h^{-1}$

Bild F3, A1-7: Rückschlagarmatur, schließt nicht

# Wahrscheinlichkeitsnetz

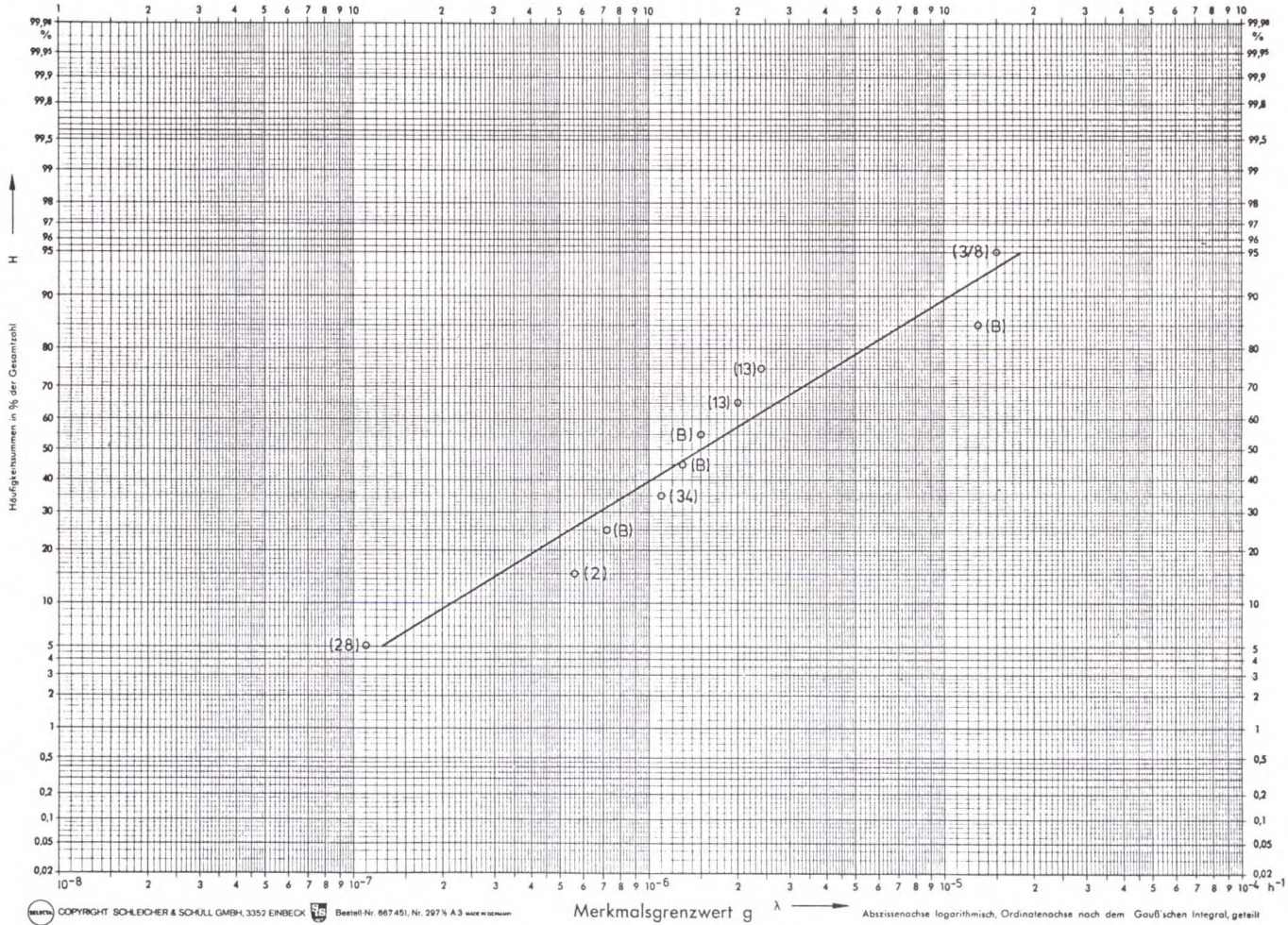
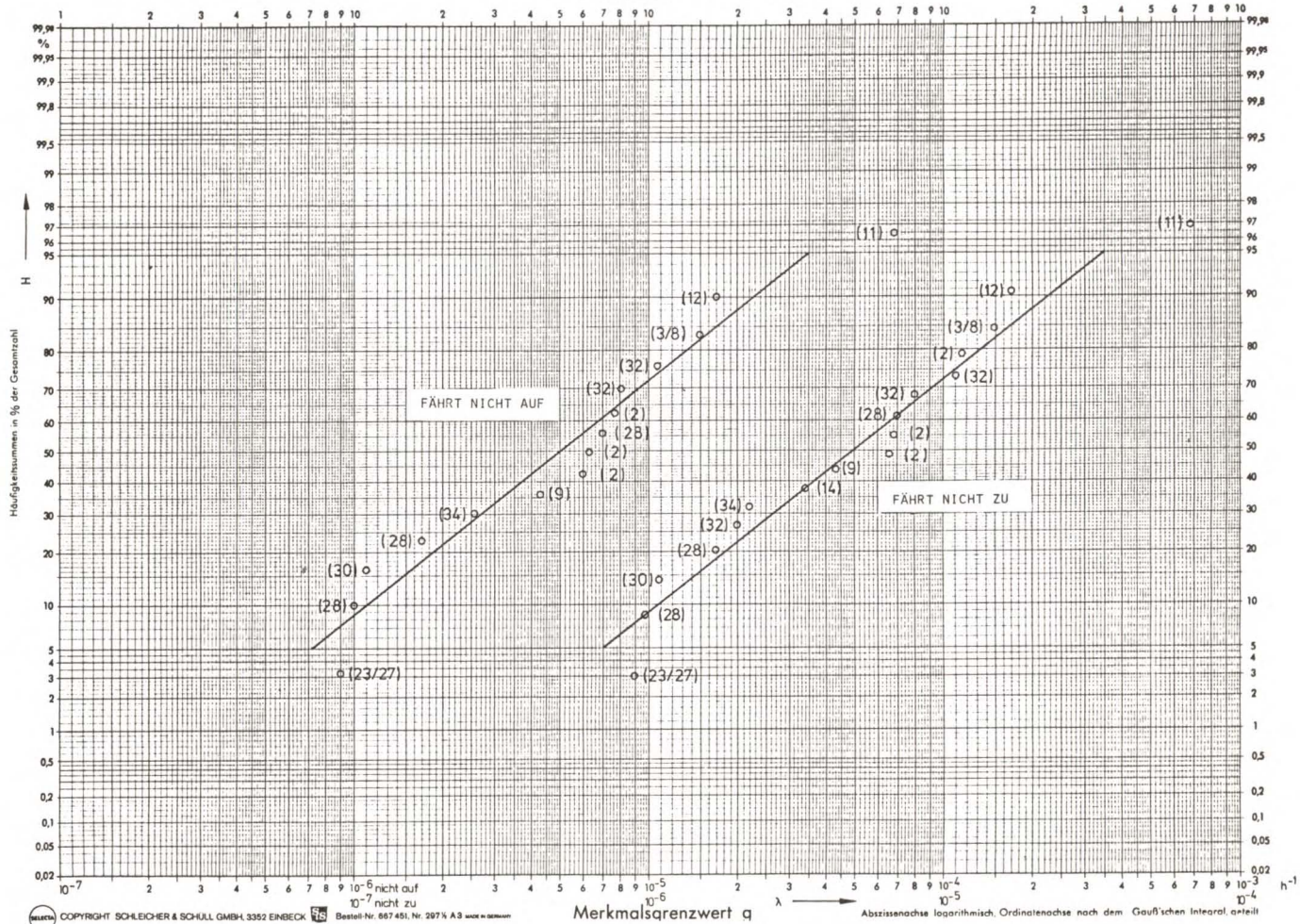


Bild F3, A1-8: Handarmatur, öffnet oder schließt nicht

# Wahrscheinlichkeitsnetz



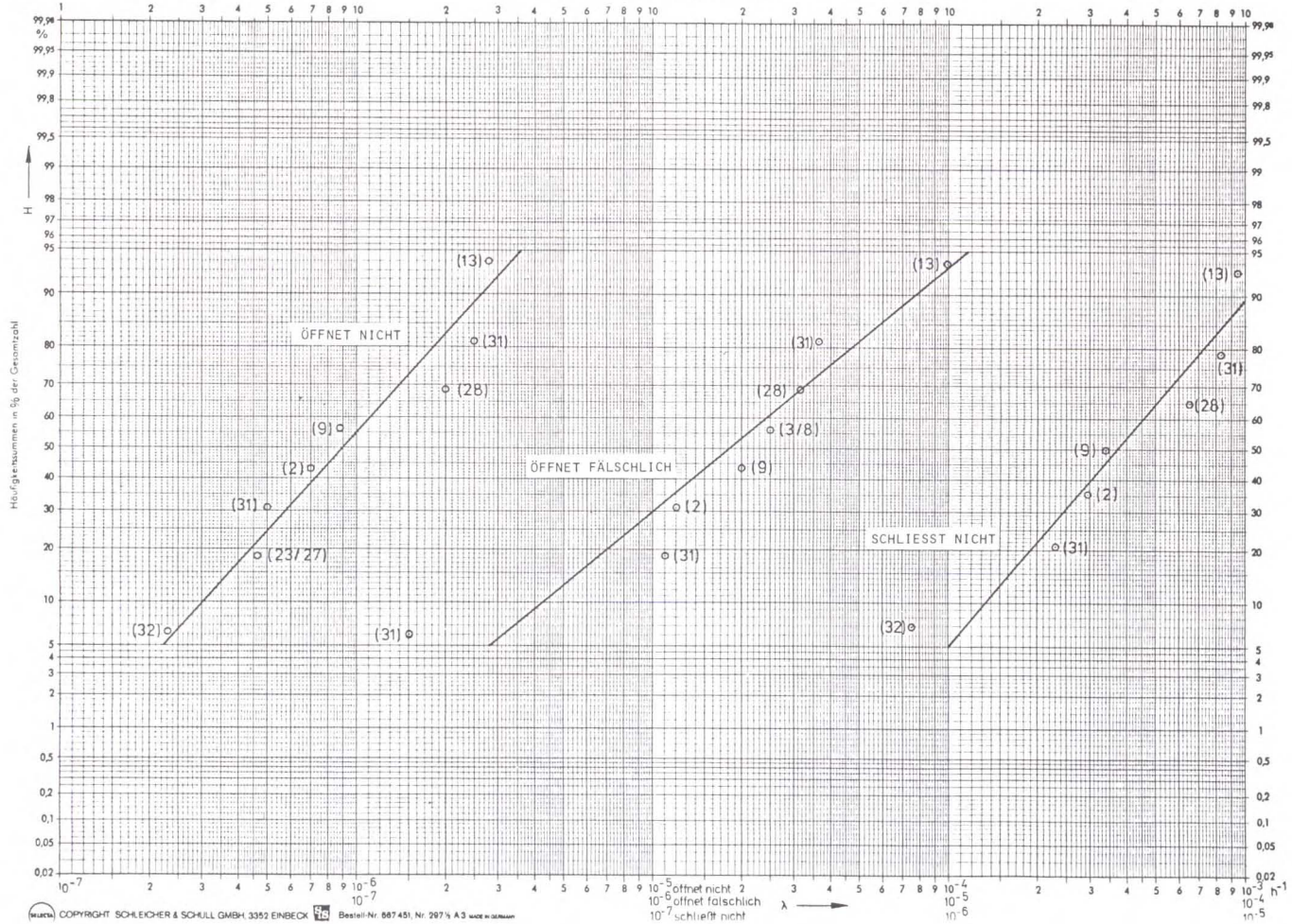
A1-23

COPYRIGHT SCHLEICHER & SCHÜLL GMBH, 3352 EINBECK Best.-Nr. 667 451, Nr. 297 N A3

Merkmalgrenzwert  $q$   $\lambda$  Abzissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral verteilt

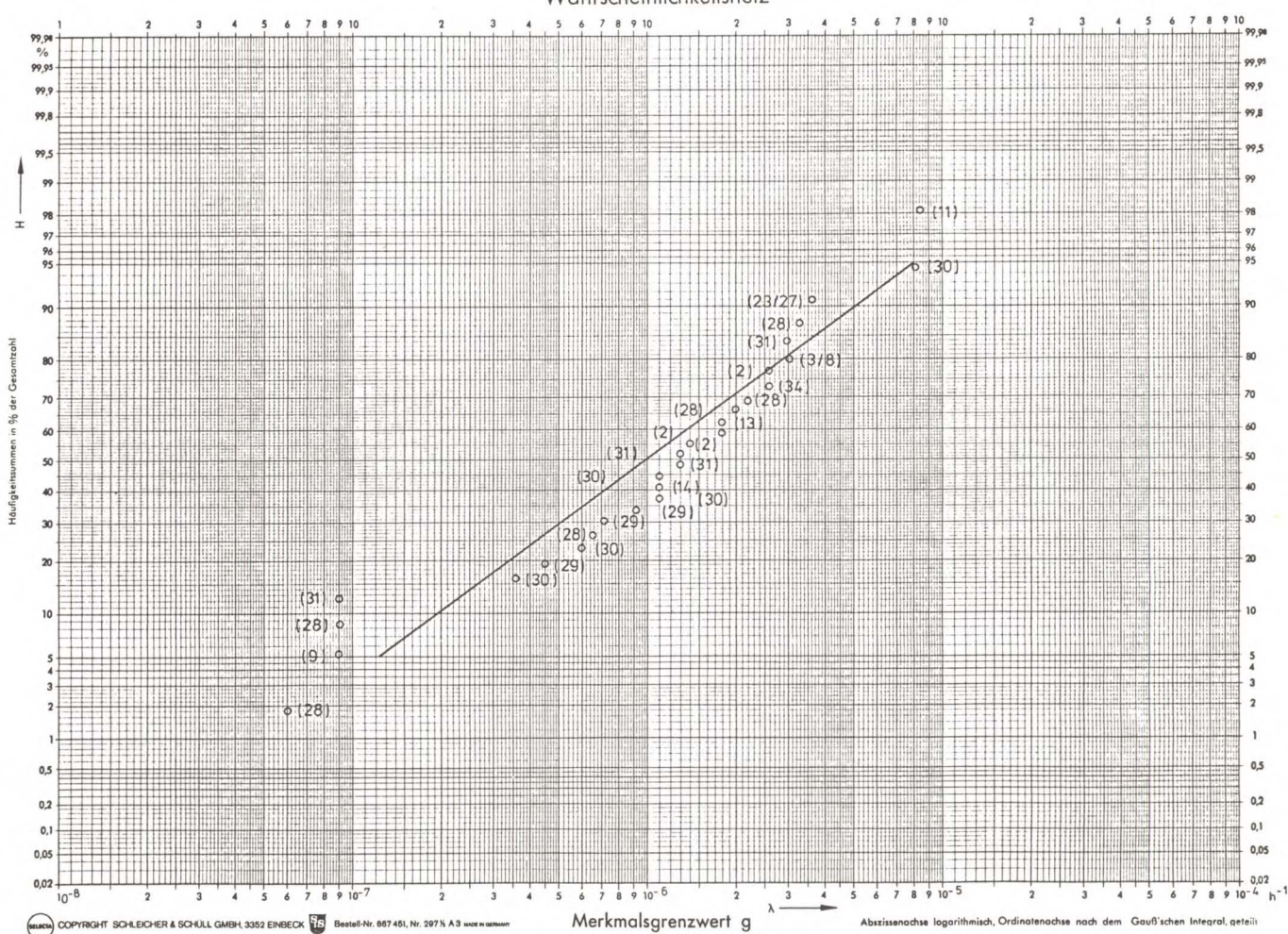
Bild F3, A1-9: Regelarmatur

# Wahrscheinlichkeitsnetz



A1-24

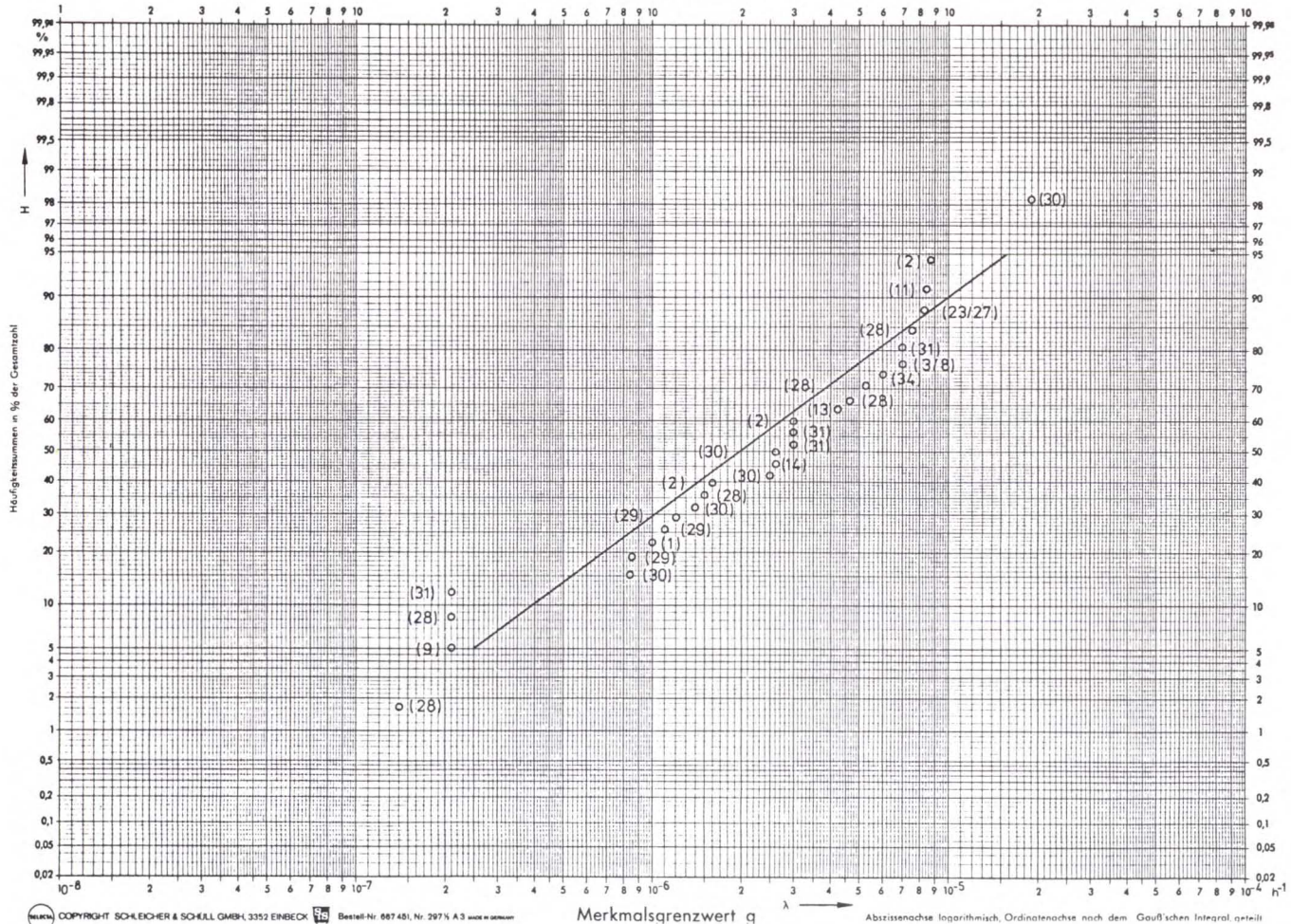
Bild F3 A1-10: Sicherheits- und Entlastungsventil



A1-25

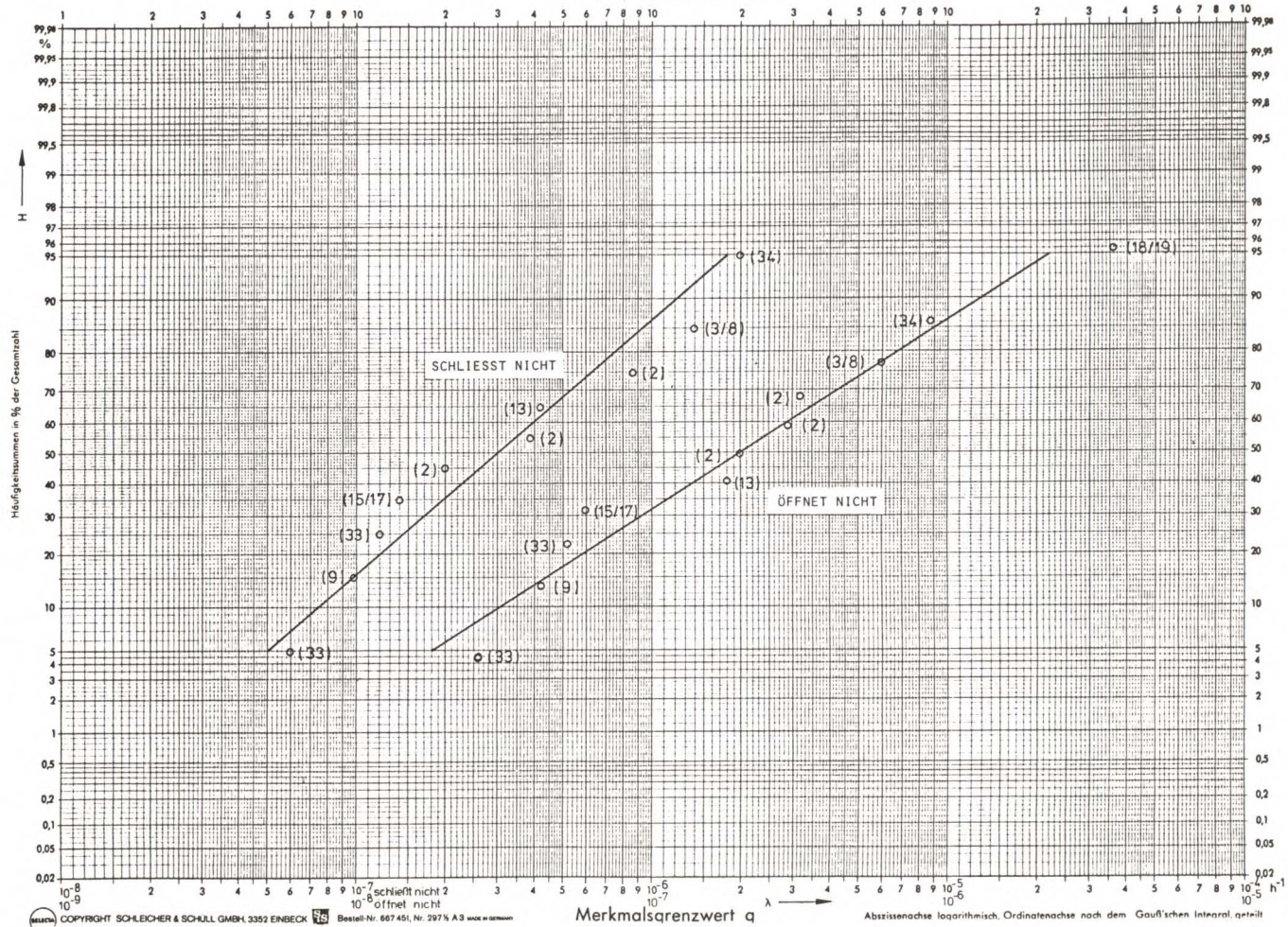
Bild F3, A1-11: Elektromotor, Startversagen

# Wahrscheinlichkeitsnetz



A1-26

Bild F3, A1-12: Elektromotor, Betriebsversagen



Copyright Schleicher & Schull GmbH, 3352 Ennack, Bestell-Nr. 667 451, Nr. 297% A3 www.sschleicher.de  
 Merkmalsgrenzwert  $q$   
 Abszissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral  $q$ -teil

Bild F3, A1-13: Leistungsschalter



# Wahrscheinlichkeitsnetz

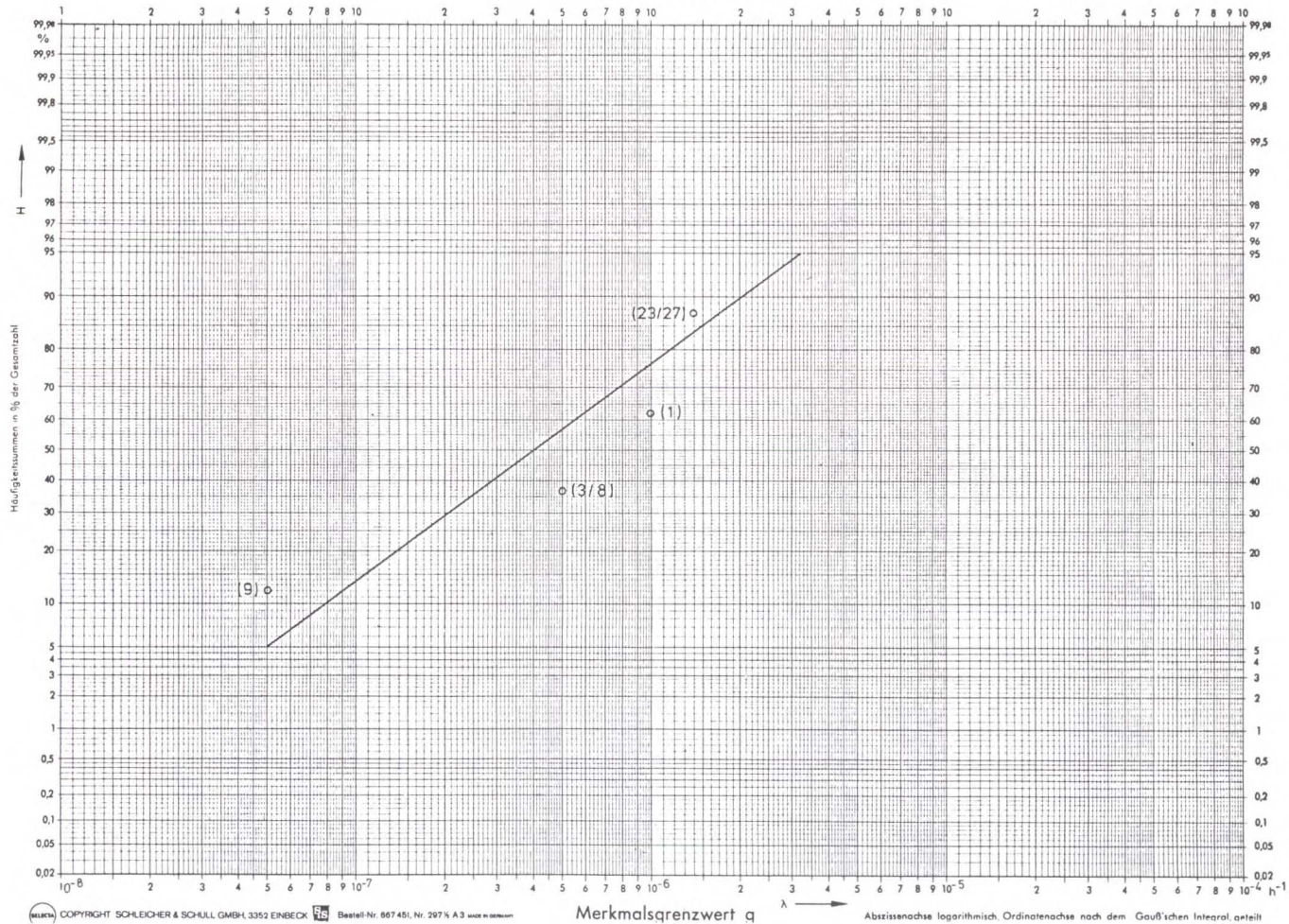
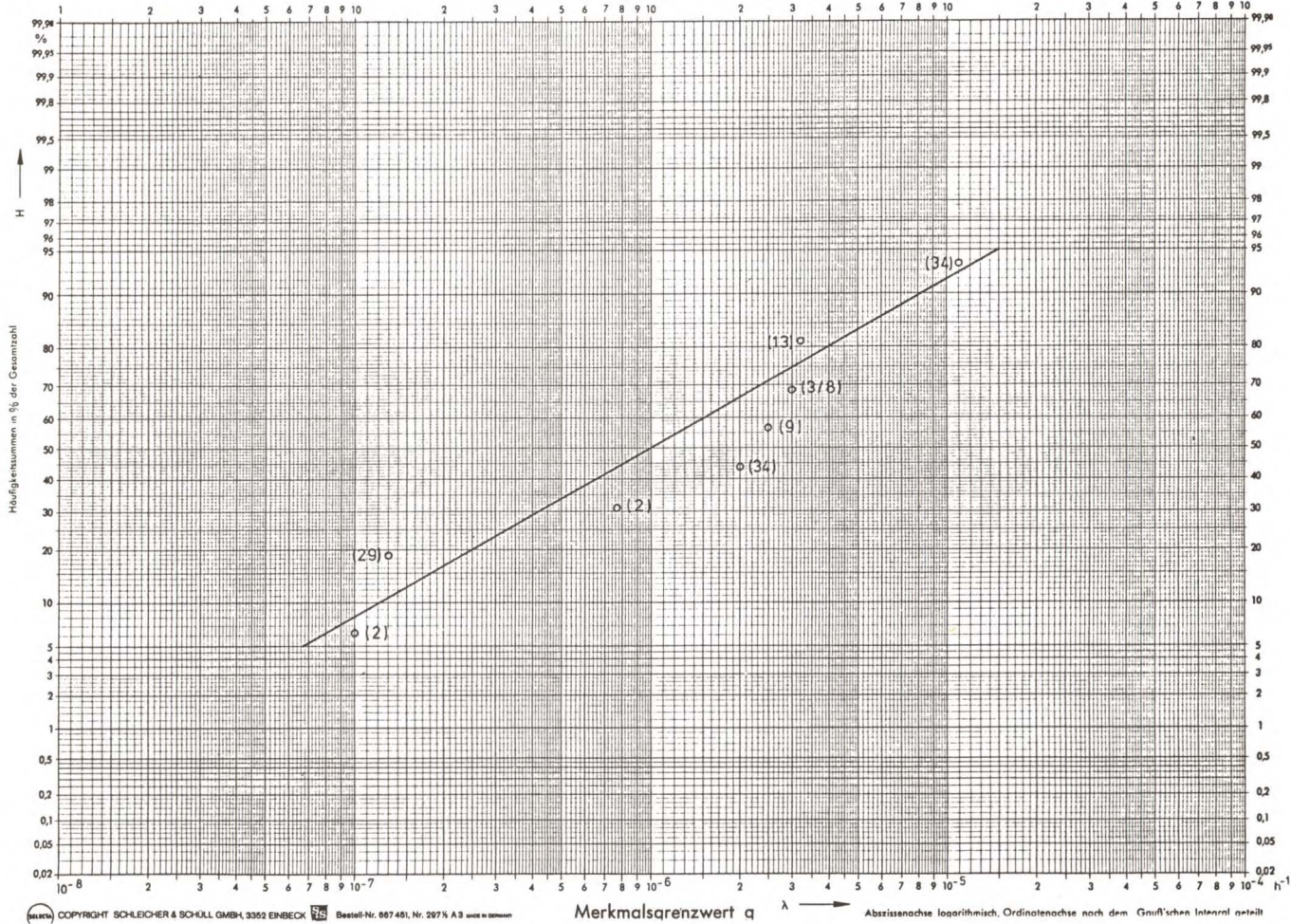


Bild F3, A1-14: Dichtung, Leckage



Häufigkeitssummen in % der Gesamtzahl

H

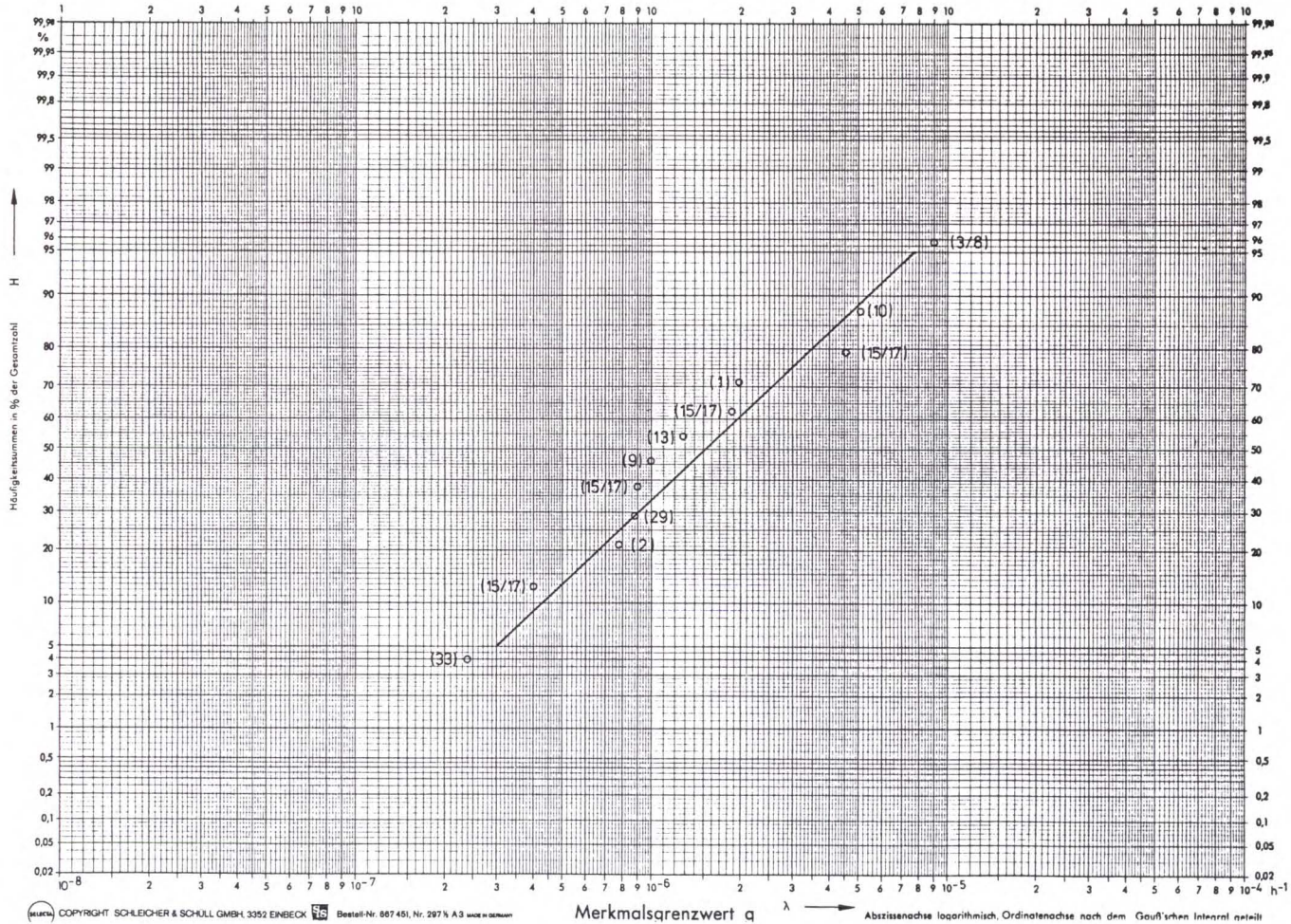
COPYRIGHT SCHLEICHER & SCHÜLL GMBH, 3352 EINBECK Best.-Nr. 067 451, Nr. 297 % A3 nach DIN 55304

Merkmalsgrenzwert  $a$   $\lambda$

Abzissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral geteilt

Bild F3, A1-15: Schütz, Verlust der Hauptfunktion

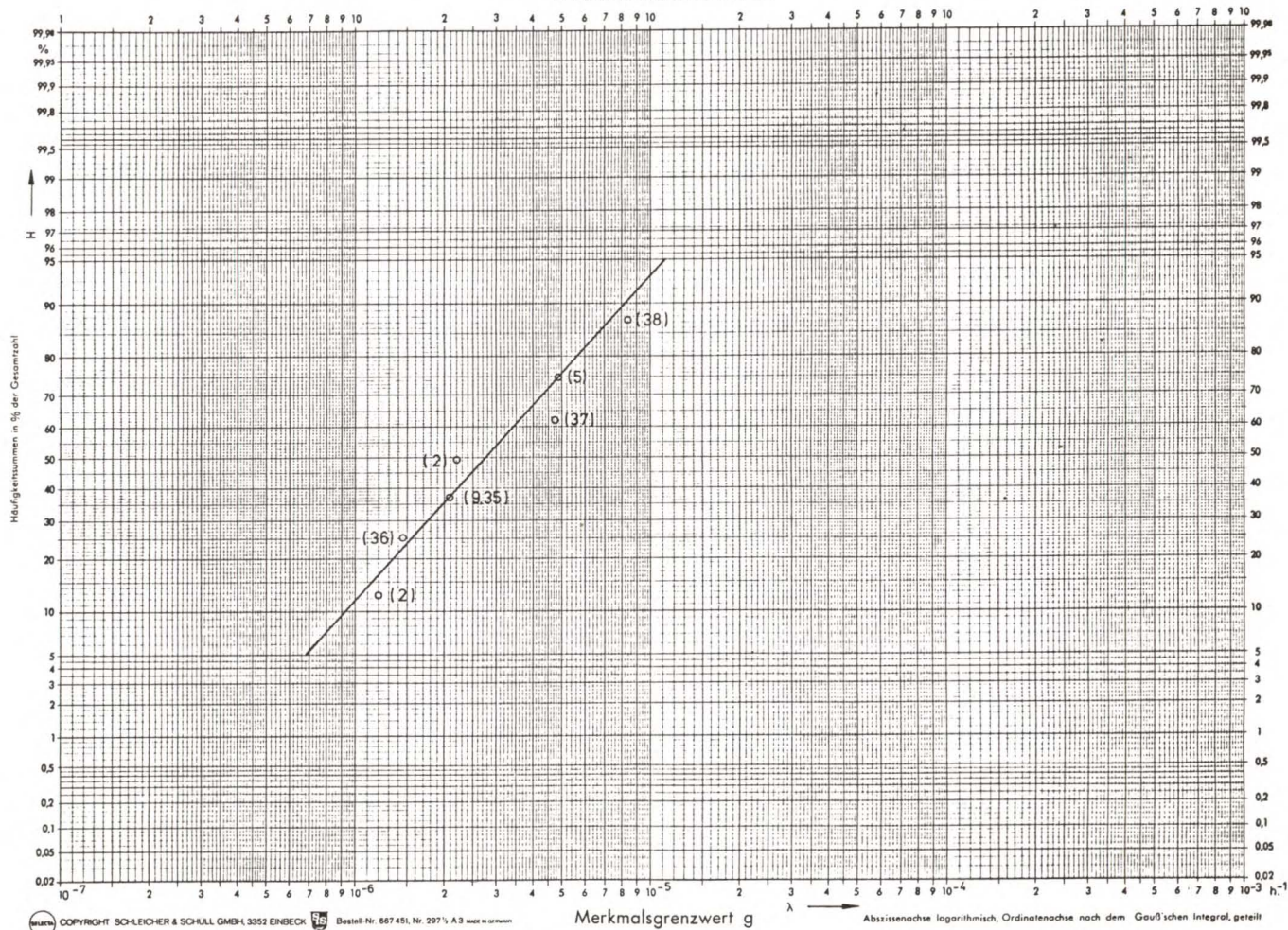
# Wahrscheinlichkeitsnetz



A1-30

Bild F3, A1-16: Transformator

Wahrscheinlichkeitsnetz



COPYRIGHT SCHLEICHER & SCHÜLL GMBH, 3352 ENBECK

Bestell-Nr. 867 451, Nr. 297 1, A 3 made in Germany Merkmalsgrenzwert  $\lambda$  Abszissenachse logarithmisch, Ordinatenachse nach dem Gauß'schen Integral geteilt

Bild F3, A1-17: Meßumformer mit Bartonzelle

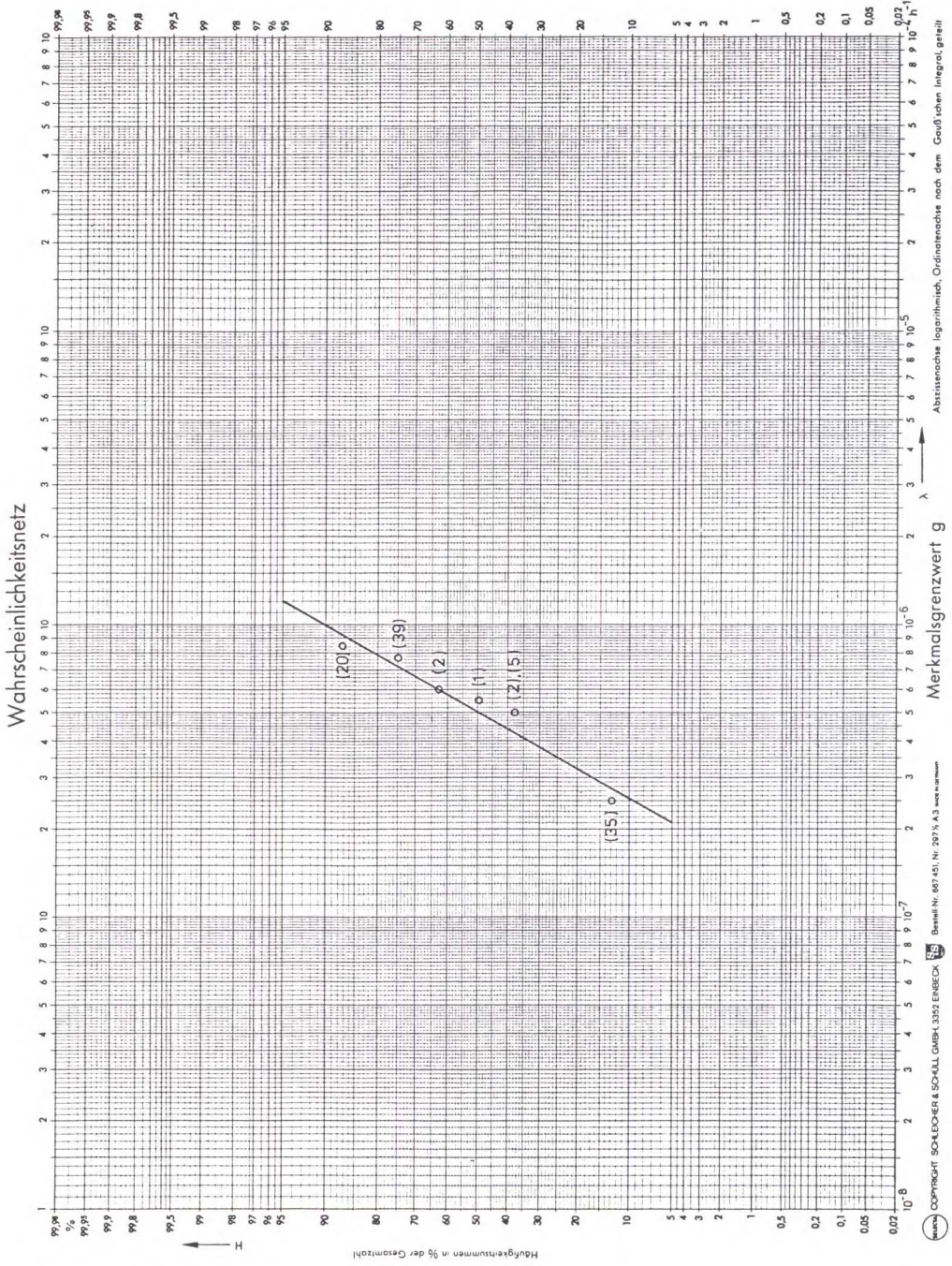


Bild F3, A1-18: Relais

Schrifttum

- /F3, A1-1/ U.S. Nuclear Operating Experience  
in: Reactor Safety Study, An Assessment of Accident  
Risks in U.S. Commercial Nuclear Power Plants,  
Appendix III: Failure Data, Table III 2-1: Data  
Assessment Tabulation  
WASH-1400 / NUREG 75/O14, App. III, 1975
- /F3, A1-2/ Nuclear Plant Reliability Data System  
1976 Annual Report of System and Component Relia-  
bility,  
Joint Publication of ANSI (N 18-20), APPA EEI and  
USNRC, May 1977
- /F3, A1-3/ Green, A.E., and A.J. Bourne:  
Reliability Considerations for Automatic Protec-  
tive System  
Nuclear Engineering 10 (1965) No. 8, p. 303
- /F3, A1-4/ Eames, A.R.:  
Reliability Assessment of Protective System  
Nuclear Engineering 11 (1966) No. 3, p. 188
- /F3, A1-5/ Green, A.E., and A.J. Bourne:  
Safety Assessment with Reference to Automatic  
Protective Systems for Nuclear Reactors  
AHSB (S) R 117, UKAEA, 1966
- /F3, A1-6/ Green, A.E.:  
Reliability Prediction  
ASHB (S) R 164, UKAEA, 1969
- /F3, A1-7/ Bourne, A.J.:  
Reliability Assessment of Technological Systems  
System Reliability Service, UKAEA, October 1971

- /F3, A1-8/ Farmer, F.R.:  
Siting Criteria - A New Approach  
inhaltsgleich mit: Reactor Safety and Siting:  
A Proposed Risk Criterion  
Nuclear Safety 8 (1966/67) No. 6, p. 539
- /F3, A1-9/ Earles, D.R.:  
Reliability Application and Analysis Guide  
MI-60-54 (Rev.1), The Martin Company, July 1961;  
Datenaufstellung in HN-190 (Kap. C 5) abgedruckt
- /F3, A1-10/ Garrick, B.J., et al.:  
Reliability Analysis of Nuclear Power Plants Pro-  
tective System  
HN-190, Holmes & Narver, Inc., May 1967
- /F3, A1-11/ Garrick B.J., et al.:  
Collection of Reliability Data at Nuclear Power  
Plants  
HN-199, Holmes & Narver, Inc., December 1968
- /F3, A1-12/ Anyakora, S.N., G.F.M. Engel and F.P. Lees:  
Some Data on the Reliability of Instruments in the  
Chemical Plant Environment  
The Chemical Engineer (1971) No. 255,  
p. 396
- /F3, A1-13/ Shopsy, W.E.:  
Review of Available Failure Rates for ECCS Compo-  
nents  
Letter to D.F. Paddleford, 20.10.1972
- /F3, A1-14/ Davies, F.M.:  
A Worked Example on the Use of Reliability Anal-  
ysis Techniques, Decay Heat Removal  
Lecture No. 58, Reactor Assessment, Section I  
Safety and Reliability Directorate (SRD)

- /F3, A1-15/ Bourne, A.J., E.R. Snaith and D. Fletcher (CEGB):  
Reliability Analysis of Electrical Supply Systems  
for Nuclear Power Stations  
ENEA/CSNI Meeting of Specialists on the Reliability  
of Electrical Supply Systems and Related Electro-Mechanical Components for Nuclear Reactor Safety, Ispra, June 27-28, 1968
- /F3, A1-16/ Mieke, G., and J. Eßmann (IRS):  
Reliability Analysis of the Emergency Power Supply  
System  
ENEA/CSNI Meeting of Specialists on the Reliability  
of Electrical Supply Systems and Related Electro-Mechanical Components for Nuclear Reactor Safety, Ispra, June 27-28, 1968
- /F3, A1-17/ Hake, G. (AECL):  
AECL's Requirements for Station Power Supplies  
ENEA/CSNI Meeting of Specialists on the Reliability  
of Electrical Supply Systems and Related Electro-Mechanical Components for Nuclear Reactor Safety, Ispra, June 27-28, 1968
- /F3, A1-18/ Tashjian, B.M.:  
Sensitivity Analysis of a Two-out-of Four Coincidence Logic Reactor Protective Systems  
IEEE Transactions on Nuclear Science, NS-18,  
February 1971, p. 455
- /F3, A1-19/ Salvatori, R.:  
Systematic Approach to Safety Design and Evaluation  
IEEE Transactions on Nuclear Science, NS-18,  
February 1971, p. 495



- /F3, A1-20/ Headington, W.L., M.E. Stewart and J.O. Zane:  
Fault Tree Analysis of the PBF Transient Rod Drive  
System  
IDO-17272, Phillips Petroleum Company, Atomic  
Energy Division, November 1968
- /F3, A1-21/ Bourne, A.J., G. Hensley, A.R. Eames et al.:  
Reliability Assessment of the S.G.H.W.R. Liquid  
Shutdown System  
AHSB (S) R 144, UKAEA, 1968
- /F3, A1-22/ Otway, H.J., R.K. Lohrding and M.E. Battat:  
A Risk Estimate for an Urban-Sited Reactor  
Nuclear Technology 12 (1971) No. 2, p. 173
- /F3, A1-23/ Antocisco, S., G. Tenaglia and A. Valeri (CNEN):  
A Theoretical Reliability Assessment of a Fire  
Protection System  
Proceedings of the Meeting of Specialists on the  
Reliability of Mechanical Components and Systems  
for Reactor Safety  
Risø Report No. 214, February 1970, p. 22
- /F3, A1-24/ Bastl, W., H. Gieseler (LRA) and H.A. Maurer  
(CEC):  
The Reliability of Emergency Core Cooling Systems  
of Light Water Nuclear Power Plants  
Proceedings of the Meeting of Specialists on the  
Reliability of Mechanical Components and Systems  
for Reactor Safety  
Risø Report No. 214, February 1970, p. 91
- /F3, A1-25/ Huppmann, H. (Allianz):  
Häufigkeit und Ursachen von Schäden an Bauteilen  
großer Dampfturbinen  
Proceedings of the Meeting of Specialists on the  
Reliability of Mechanical Components and Systems  
for Reactor Safety  
Risø Report No. 214, February 1970, p. 171

- /F3, A1-26/ Hennings, U. (BBK):  
Auslegung und Anordnung einer Reaktor-Beschickungs-  
anlage aufgrund von Zuverlässigkeitsbetrachtungen  
Proceedings of the Meeting of Specialists on the  
Reliability of Mechanical Components and Systems  
for Reactor Safety  
Risø Report No. 214, February 1970, p. 213
- /F3, A1-27/ Ehrentreich, J., and H. Maurer:  
Reliability Considerations for Mechanical Compo-  
nents of Control Rod Drive Systems of Gas-Cooled  
Power Reactors Operated in the European Community  
Proceedings of the Meeting of Specialists on the  
Reliability of Mechanical Components and Systems  
for Reactor Safety  
Risø Report No. 214, February 1970, p. 481
- /F3, A1-28/ Sexton, I.B.:  
Failure Rate Estimate of Some Nuclear and Conven-  
tional Power Plant Components  
AI-67-TDR-15-REV, Atomics International, 1968
- /F3, A1-29/ IEEE Guide to the Collection and Presentation of  
Electrical, Electronical and Sensing Component,  
Reliability Data for Nuclear Power Generating  
Stations  
IEEE Standard 500-1977
- /F3, A1-30/ Interne Mitteilung  
KWU Erlangen, 18.10.1971
- /F3, A1-31/ van Zylstra, E.H.:  
Recommended Component Failure Rates for Reliabili-  
ty Analysis  
May 1969

- /F3, A1-32/ Interne Mitteilung, betrifft: Untersuchungen für  
verschiedene Ventiltypen  
RWE Essen, 1975
- /F3, A1-33/ VDEW Störungs- und Schadensstatistik 1972  
Hrsg.: Vereinigung Deutscher Elektrizitätswerke  
(VDEW), Frankfurt/Main, 1975
- /F3, A1-34/ Hömke, P., und H. Krause:  
Eigene Auswertung des Modellfalles IRS-RWE  
(unveröffentlicht)
- /F3, A1-35/ Earles, D.R., and M.F. Eddins (General Electric):  
Reliability Physics  
9th National Symposium on Reliability and Quality  
Control, San Francisco, 1963
- /F3, A1-36/ Ausfallratenstatistik  
Hrsg.: Schoppe und Faeser, Minden, 1973 und 1976
- /F3, A1-37/ Balfanz, H.P.:  
Ausfallratensammlung  
IRS-W-8, Dezember 1973
- /F3, A1-38/ Bartels, G.:  
Wirtschaftliches Instandhalten von Meß-, Steuer-  
und Regelanlagen in Chemiebetrieben  
Bayer Leverkusen, 1977
- /F3, A1-39/ RADC Reliability Notebook, Volume II  
Rome Air Development Center, New York, 1967
- /F3, A1-40/ Shopsy, W.E.:  
Review of Available Failure Rates for ECCS Compo-  
nents  
Letter to D.F. Paddleford, 20.10.1972

- /F3, A1-41/ Dorey, J., and B. Gachot:  
Pump Reliability Data Derived from Electricité de  
France Operating Experience  
Symposium on Inservice Data Reporting and Analysis,  
ANS Winter Meeting, San Francisco, December 1978
- /F3, A1-42/ Nuclear Plant Reliability Data System  
1976 Annual Report of System and Component Relia-  
bility,  
Joint Publication of ANSI (N 18-20), APPA EEI and  
USNRC, May 1977
- /F3, A1-43/ Technical Report on Operating Experience with BWR  
Pressure Relief Systems  
NUREG-0462, July 1978
- /F3, A1-44/ Parisian, R.W.:  
How Reliable are Today's Prime Movers Power  
January 14, 1970
- /F3, A1-45/ Crooks, J.L., and G.S. Vissing:  
Diesel Generator Operating Experience at Nuclear  
Power Plants  
OOE-ES-002, USAEC, June 1974
- /F3, A1-46/ Betriebserfahrungen mit Kernkraftwerken in der  
Bundesrepublik Deutschland  
Atom und Strom 22 (1976) Nr. 3, S. 68
- /F3, A1-47/ Pugh, M.C.:  
Probability Approach to Safety Analysis  
TRG Report 1949 (R), UKAEA, 1969
- /F3, A1-48/ ATWS: A Reappraisal, Part II, Evaluation of Societal  
Risks Due to Reactor Protection System Failure,  
Vol. 3: PWR Risk Analysis  
EPRI NP-265, August 1976

- /F3, A1-49/ Sommer, P., K.-R. Hartung, H. Scholz et al.:  
Ermittlung der Ausfallraten von Diesellaggregaten  
und Elektronikarten zur Bestimmung der Ausfall-  
wahrscheinlichkeit von Sicherheitssystemen  
Qualität und Zuverlässigkeit 22 (1977) Nr. 5, S. 97
- /F3, A1-50/ Helmich, M.J.:  
Maintenance and Operation of Nuclear Diesel Gene-  
rator Systems  
Paper 77-DGP-14, Energy Technology Conference and  
Exhibit, Houston, Texas, September 18-22, 1977
- /F3, A1-51/ Balfanz, H.P., K. Kotthoff und G. Volmer:  
Störfallablaufanalyse, Methodenkritik und Wahr-  
scheinlichkeitsbewertung am Beispiel des Notstrom-  
falles von deutschen DWR-Anlagen  
Anhang A3 in: Kritischer Bericht zur Reaktorsicher-  
heitsstudie (WASH-1400)  
IRS-I-87/MRR-I-65, April 1976
- /F3, A1-52/ Bush, S.H.:  
Reliability of Piping in Light Water Reactors  
Nuclear Safety 17 (1976) No. 5, p. 568
- /F3, A1-53/ Boesebeck, K., und F.W. Heuser:  
Ausfallraten für Rohrleitungen und Reaktordruck-  
behälter  
Anhang A7 in: Kritischer Bericht zur Reaktorsicher-  
heitsstudie (WASH-1400)  
IRS-I-87/MRR-I-65, April 1976
- /F3, A1-54/ Duma, D.W., and R.F. Saxe:  
An Analysis of Control-Rod-System Malfunctions in  
Nuclear Power Reactors  
Nuclear Safety 14 (1973) No. 4, p. 315

/F3, A1-55/ Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants  
NUREG/CR-1331, EGG-EA-5079, February 1980

Zuverlässigkeitskenngrößen aus der Auswertung von Betriebs-  
erfahrungen in Kernkraftwerken

Anmerkung:

Jede Zeile repräsentiert eine Population der betrachteten  
Komponentenart. Werte zu Ausfallraten sind untereinander sta-  
tistisch unabhängig, ebenso Werte zu Ausfallwahrscheinlich-  
keiten (Abschnitt 6.3).

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$	
Pumpe	startet nicht	3	3,8 E-5	-	
		1	1,3 E-5	-	
		0	9,0 E-6	-	
		5	2,3 E-5	-	
		1	4,7 E-6	-	
		2	1,9 E-5	-	
		2	1,4 E-5	-	
		2	-	8,1 E-3	
		9	-	1,9 E-3	
		5	-	2,7 E-3	
		1	-	4,0 E-4	
		fördert nicht	0	8,8 E-6	-
			1	1,3 E-5	-
	1		1,3 E-5	-	
	5		3,5 E-5	-	
	11		7,6 E-5	-	
	erreicht nicht die volle Leistung	2	9,3 E-6	-	
		1	1,9 E-5	-	
		2	-	8,3 E-4	



Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Pumpe	Leckage nach außen	2	2,6 E-5	-
		6	7,7 E-5	-
		4	5,1 E-5	-
		6	2,8 E-5	-
		2	1,9 E-5	-
		1	1,9 E-5	-
		3	2,1 E-5	-
		7	4,8 E-5	-
	startet ohne Anforderung	1	4,7 E-6	-
Motorarmatur	öffnet nicht	4	1,5 E-5	-
		9	3,1 E-5	-
		10	1,5 E-5	-
		14	1,5 E-5	-
		14	8,2 E-6	-
		2	4,7 E-6	-
		5	7,5 E-6	-
		9	-	2,1 E-3
		0	-	1,5 E-3
		3	-	5,7 E-3

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Motorarmatur	öffnet nicht	2	-	3,2 E-3
		14	-	1,5 E-3
		2	-	3,4 E-4
	schließt nicht	8	2,9 E-5	-
		6	9,0 E-6	-
		19	6,5 E-5	-
		14	1,5 E-5	-
		16	9,2 E-6	-
		4	9,4 E-6	-
		5	7,5 E-6	-
		8	-	1,7 E-3
		1	-	2,2 E-3
		16	-	1,7 E-3
		4	-	6,8 E-4
		2	-	3,8 E-3
		0	-	1,1 E-3
		öffnet nicht und schließt nicht <sup>1)</sup>	4	1,5 E-5
	3		1,0 E-5	-
	4		6,0 E-6	-

A2-5

<sup>1)</sup> Diese Ausfälle sind sowohl bei der Ausfallart "öffnet nicht" als auch "schließt nicht" berücksichtigt.

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$	
Motorarmatur	öffnet nicht und schließt nicht <sup>1)</sup>	8	8,5 E-6	-	
		7	4,1 E-6	-	
		2	4,7 E-6	-	
		5	7,5 E-6	-	
		7	-	7,3 E-4	
		2	-	3,4 E-4	
	Leckage nach innen	1	3,7 E-6	-	
		11	1,7 E-5	-	
		12	1,3 E-5	-	
		1	5,8 E-7	-	
		4	9,3 E-6	-	
	Leckage nach außen	5	2,9 E-6	-	
	Rückschlagarmatur	öffnet nicht	0	7,7 E-7	-
			0	5,9 E-7	-
			0	1,9 E-6	-
0			-	4,2 E-4	
schließt nicht		0	7,7 E-7	-	

<sup>1)</sup> Diese Ausfälle sind sowohl bei der Ausfallart "öffnet nicht" als auch "schließt nicht" berücksichtigt.

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Rückschlagarmatur	schließt nicht	0	5,9 E-7	-
		0	1,9 E-6	-
		1	6,9 E-6	-
		1	-	6,1 E-4
	Leckage nach außen	2	2,2 E-6	-
		1	1,3 E-5	-
Leckage nach innen	22	2,6 E-5	-	
	5	4,2 E-6	-	
Rückschlagarmatur, elektrisch absperrbar	elektrischer Antrieb fährt weder auf noch zu	1	4,3 E-6	-
		1	-	6,8 E-4
Rückschlagarmatur, elektrisch aufziehbar	elektrischer Antrieb zieht nicht auf	2	2,6 E-5	-
Handarmatur	öffnet nicht	2	7,2 E-7	-
		2	1,3 E-5	-
		1	4,8 E-7	-
		3	1,3 E-6	-

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Handarmatur	öffnet nicht	5	2,0 E-6	-
		2	2,4 E-6	-
	schließt nicht	2	7,2 E-7	-
		2	1,3 E-5	-
		2	9,0 E-7	-
		5	2,0 E-6	-
		1	1,2 E-6	-
	öffnet und schließt nicht	2	7,2 E-7	-
		2	1,3 E-5	-
		2	9,0 E-7	-
		5	2,0 E-6	-
		1	1,2 E-6	-
	Leckage nach außen	2	7,2 E-7	-
		5	3,2 E-5	-
		3	1,5 E-7	-
		8	3,6 E-6	-
	Leckage nach innen	1	3,6 E-7	-

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Handarmatur	Leckage nach innen	1	4,1 E-7	-
		3	1,5 E-7	-
		3	1,3 E-6	-
Handarmatur NW $\leq 25$	öffnet und schließt nicht	2	1,8 E-7	-
	Leckage nach innen	3	2,7 E-7	-
Regelarmatur	fährt nicht auf	12	7,7 E-5	-
		0	1,5 E-5	-
		1	3,1 E-6	-
	fährt nicht zu	13	8,3 E-5	-
		0	1,5 E-5	-
		1	3,1 E-6	-
	fährt weder auf noch zu	9	5,8 E-5	-
		0	1,5 E-5	-
		1	3,1 E-6	-
	Leckage nach innen	4	2,6 E-5	-

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Sicherheitsventile (zur Druckabsicherung wassergefüllter Rohrleitungen)	öffnet nicht	2	2,1 E-6	-
		0	3,6 E-6	-
		0	3,7 E-7	-
	schließt nicht	1	1,1 E-6	-
		0	3,6 E-6	-
	Kenndatendrift	2	2,1 E-6	-
	Leckage nach außen	3	3,2 E-6	-
		1	5,3 E-7	-
	Leckage nach innen	15	1,6 E-5	-
		2	1,1 E-6	-
Hydraulisch betätigte Armatur	schließt nicht	3	1,4 E-5	-
	öffnet oder schließt ohne Anforderung	1	4,7 E-6	-
Umschaltarmatur, eigenmediumbetätigt	schaltet nicht um	12	-	9,5 E-2

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Lüfter	läuft nicht an	24	-	6,0 E-2
		7	-	9,4 E-3
Lüftungsklappen	öffnet nicht	7	-	3,8 E-2
		1	-	1,5 E-3
		1	-	1,5 E-2
	schließt nicht	7	-	3,8 E-2
		9	-	1,3 E-2
		1	-	1,5 E-2
380-V-Einspeiseschalter	öffnet nicht	0	-	1,2 E-3
	schließt nicht	1	-	1,7 E-3
Druckmeßstelle (Geber und Meßumformer)	Ausgangsspannung oder Anzeige Null	3	1,3 E-6	-
		1	2,1 E-5	-
	volle Ausgangsspannung oder Vollausschlag	1	4,3 E-7	-



Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Druckmeßstelle (Geber und Meßumformer)	Kenndatendrift	1	4,3 E-7	-
	Schwingen, Instabilität, Aussetzer	4	1,7 E-6	-
	alle Ausfallarten	0	1,5 E-5	-
		0	1,5 E-5	-
0		2,4 E-6	-	
Durchflußmeßstelle (Geber und Meßumformer)	Ausgangsspannung oder Anzeige Null	3	8,0 E-6	-
		2	1,4 E-5	-
	beliebige Ausgangsspannung oder Anzeige	1	6,9 E-6	-
	Verstopfung	1	6,9 E-6	-
Durchflußmeßstelle (Differenzdruckprinzip mit Grenzkontakten)	Ausgangsspannung oder Anzeige Null	3	2,1 E-6	-
	Schwingen, Instabilität, Aussetzer	2	1,4 E-6	-
	Kenndatendrift	5	3,5 E-6	-

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Niveaumeßstelle (Geber und Meßumformer)	volle Ausgangsspannung oder Vollauschlag	1	1,6 E-6	-
	Ausgangsspannung oder Anzeige Null	2	3,1 E-6	-
	Kenndatendrift	1	1,6 E-6	-
Niveaumeßstelle mit Grenzkontakten	volle Ausgangsspannung oder Vollauschlag	1	6,9 E-6	-
Temperaturmeßstelle (Geber und Meßumformer)	volle Ausgangsspannung oder Vollauschlag	2	5,3 E-7	-
	Ausgangsspannung oder Anzeige Null	1	2,6 E-7	-
	Schwingen, Instabilität, Aussetzer	1	2,6 E-7	-
Temperaturmeßstelle (Einschweiß-Doppelwiderstandsthermometer mit Grenzkontakten)	Ausfall mit Ausgangsspannung oder Anzeige Null	1	1,5 E-6	-
Aktivitätsmeßstelle	Ausgangsspannung oder Anzeige Null	2	4,2 E-5	-

Komponente	Ausfallart	Anzahl der Ausfälle	Ausfallrate $\lambda(1/h)$	Ausfallwahrscheinlichkeit $P(1/A)$
Aktivitätsmeßstelle	Schwingen, Instabilität, Aussetzer	2	4,2 E-5	-

Basis-Ausfallraten für leittechnische Komponenten

Funktionselement-Ausfall	Ausfallrate		Anmerkungen
	Medianwert [ $10^{-6}/h$ ]	Streufaktor der logarithmischen Normalverteilung	
<u>Meßwerterfassung</u>			
Differenzdruckmeßumformer mit Bartonzelle			LIT
- Ausgabe eines unveränderlichen Wertes (mechanisches oder elektrisches Versagen)	0,3	3	
- mißt zu hohen Druck	1,0	3	
Druckmeßumformer mit Rohrfedermeßwerk			LIT
- mißt zu hohen oder zu niedrigen Druck	3,5	3	
Druckschalter			LW
- schließt ohne Anregung	2,5	10	
- spricht nicht an	1,0	10	
Thermoelement und Umformer			AFEA
- mißt zu niedrige Temperatur	5,0	10	
- Meßbereich nach oben eingengt	0,02	10	
Drehzahlfühler und Umformer			AFEA
- mißt zu hohe Drehzahl	2,2	3	
Niveauschalter			LW
- spricht nicht an	7,0	10	
Strom-Spannungs-Wandler M 4335-A 1			AFEA
- Ausgangsspannung zu groß	0,6	3	
- Ausgangsspannung zu klein	2,0	3	
- untere Meßbereichsgrenze angehoben	0,01	3	
- obere Meßbereichsgrenze abgesenkt	0,01	10	

Funktionselement-Ausfall	Ausfallrate		Anmerkungen
	Medianwert [10 <sup>-6</sup> /h]	Streufaktor der logarithmischen Normalverteilung	
Spannungs-Spannungs-Wandler M 4335-A 1			AFEA
- Ausgangsspannung zu groß	0,5	3	
- Ausgangsspannung zu klein	2,0	3	
- untere Meßbereichsgrenze angehoben	0,01	3	
- obere Meßbereichsgrenze abgesenkt	0,01	10	
Trennverstärker TTK			AFEA
- Ausgangsstrom zu groß	0,4	3	
- Ausgangsstrom zu klein	3,3	3	
- untere Meßbereichsgrenze angehoben	0,02	10	
- obere Meßbereichsgrenze abgesenkt	0,02	10	
Summierverstärker M 4010-E 1			AFEA
- Ausgangsspannung zu groß	1,0	3	
- Ausgangsspannung zu klein	1,0	3	
- untere Meßbereichsgrenze angehoben	0,02	10	
- obere Meßbereichsgrenze abgesenkt	0,02	10	
Grenzwertmelder RG 11 (dynamisch arbeitend)			AFEA
- Maximalgrenzwert selbstmeldend höher	0,6	3	
- Maximalgrenzwert selbstmeldend tiefer	0,6	3	
- Maximalgrenzwert unentdeckt höher	0,02	3	
- Minimalgrenzwert unentdeckt tiefer	0,02	3	
Druckmeßgerät (analoges Anzeigegerät)			LW
- ausgefallen	10,0	3	

Funktionselement-Ausfall	Ausfallrate		Anmerkungen
	Medianwert [10 <sup>-6</sup> /h]	Streufaktor der logarithmischen Normalverteilung	
Vergleicher und Meldeeinrichtungen			LW
- Meldung ausgefallen	5,0	10	
<u>Logische Verknüpfung</u>			
2v3-Auswahleinheit			AFEA
- spricht fälschlich an	0,9	3	
- Kurzschluß Eingang-Ausgang	0,0003	10	
Impulsumformer für Taktgeber			AFEA
- ausgefallen	2,0	10	
NOR-Gatter im Taktgeber			AFEA
- ausgefallen	0,4	3	
Abschlußglied			AFEA
- spricht fälschlich an	2,6	3	
Binärsignaleingabe			AFEA
- gibt fälschlich Impulse aus			
• nur Eingang E beschaltet	1,2	3	
• Eingänge E und $\bar{E}$ beschaltet	0,3	3	
Taktgeber			AFEA
- spricht fälschlich an	3,9	3	
Abschlußrelais			LIT
- schließt nicht	0,3	3	
- öffnet nicht	0,1	3	
<u>Steuerung</u>			
Leitungsanschluß/Lötstelle			BE
- Unterbrechung	0,001	10	
- Masseschluß	0,001	10	
Kabel			LW
- Unterbrechung	0,3/km	3	

Funktionselement-Ausfall	Ausfallrate		Anmerkungen
	Medianwert [ $10^{-6}/h$ ]	Streufaktor der logarithmischen Normalverteilung	
Endschalter - spricht nicht an	1,0	3	LW
UND-Gatter			AFEA
- gibt kein Signal aus	$0,4+x_1 \cdot 0,02$	3	
- gibt fälschlich Signal aus • wenn kein Eingang P führt • wenn nur ein Eingang 0 führt	0,02 0,1	3 3	
ODER-Gatter			AFEA
- gibt kein Signal aus • wenn mehrere Eingänge P führen • wenn nur ein Eingang P führt	$0,2+x_1 \cdot 0,02$ $0,3+x_1 \cdot 0,02$	3 3	
- gibt fälschlich Signal aus	0,01	3	
Betätigungsbaustein B22			AFEA
- AUF-Befehl wird nicht ausgegeben	0,6	3	
- ZU-Befehl wird nicht ausgegeben	0,6	3	
- verursacht Kurzschluß (AUF- oder ZU-Befehl)	0,06	3	
Betätigungsbausteine B21 und B23			AFEA
- EIN-Befehl wird nicht ausgegeben	0,4	3	
- AUS-Befehl wird nicht ausgegeben	0,3	3	
- Schalterfallmeldung wird fälschlich ausgegeben	0,2	3	
- verursacht Kurzschluß bei EIN-Befehl	0,07	3	
- verursacht Kurzschluß bei AUS-Befehl	0,05	3	

$x_1$  = Anzahl der Gatter derselben Karte, die gleichzeitig mit dem betrachteten Gatter angesteuert werden



Funktionselement-Ausfall	A u s f a l l r a t e		Anmer- kungen
	Medianwert [ $10^{-6}/h$ ]	Streufaktor der logarithmischen Normalverteilung	
Verzögerungsstufe (analog arbeitend)			AFEA
- gibt kein Signal aus	1,0	3	
- gibt fälschlich Signal aus	0,35	3	
Verzögerungsstufe (digital arbeitend)			AFEA
- spricht nicht an	0,5	3	
- verursacht Kurzschluß	0,3	3	
- Signal bleibt stehen	0,2	3	
- gibt fälschlich Signal aus	0,09	3	
- zählt dual	0,04	3	
- Veränderung des Zeitbereichs	0,014	3	
- Veränderung der Zeitvorwahl	0,1	3	
Stromversorgung im Betätigungs- schrank			AFEA
- ganzer Schrank ausgefallen	0,1	3	
- eine Schrankhälfte ausge- fallen	+0,1	3	
Speicherbaustein (Flip-Flop)			LW
- unterdrückt P	0,25	3	
Steuerkette für Motorarmaturen			AFEA
- öffnet nicht bei nicht ver- schalteter "Sperrre ZU"	$1,9+x_2 \cdot 0,16$	3	
- schließt nicht	$1,8+x_3 \cdot 0,13$	10	
- öffnet bei ZU-Befehl	0,004	3	
Steuerkette für Leistungs- schalter und Schütze			AFEA
- schaltet nicht ein bei nicht verschalteter "Sperrre AUS"	$0,7+x_4 \cdot 0,16$		
- schaltet nicht aus	$0,6+x_5 \cdot 0,13$		

$x_2$  = Anzahl der an den AUF-Befehl angeschlossenen Bausteine

$x_3$  = Anzahl der an den ZU-Befehl angeschlossenen Bausteine

$x_4$  = Anzahl der an den EIN-Befehl angeschlossenen Bausteine

$x_5$  = Anzahl der an den AUS-Befehl angeschlossenen Bausteine

Funktionselement-Ausfall	Ausfallrate		Anmerkungen
	Medianwert [ $10^{-6}/h$ ]	Streufaktor der logarithmischen Normalverteilung	
NOR-Gatter mit Leistungs- verstärker (Simatic N) - ausgefallen	0,6	3	LW
2v3-Schaltung (Simatic N) - ausgefallen	0,1	3	LW
Speicherbaustein (Simatic N) - ausgefallen	0,4	3	LW
ODER-Baustein (Simatic N) - ausgefallen	0,1	3	LW

## Anmerkungen:

- AFEA = Ausfallraten wurden mittels einer Ausfalleffektanalyse ermittelt (Abschnitt 8.3).
- LIT = Ausfallraten wurden mittels einer Literaturrecherche ermittelt (Abschnitt 8.1).
- BE = Ausfallraten wurden durch Auswerten von Betriebserfahrung ermittelt (Abschnitt 8.2).
- LW = Hier lag nur eine Literaturstelle vor. Diese Werte wurden aber nachträglich durch Auswerten zusätzlicher Betriebserfahrung /F3, 8-12/ abgesichert (Abschnitt 8.2).

