Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik

GRS - 494

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik

Christian Müller
Jörg Peschke
Ewgenij Piljugin

März 2018

Anmerkung:

Das diesem Bericht zugrunde liegende F&E-Vorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, und nukleare Sicherheit (BMU) unter dem Kennzeichen 3615R01343 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

GRS - 494
ISBN 978-3-946607-79-3

Deskriptoren

Architektur, Ausfallrate, digitale Leitechnik, Fehlerbaumanalyse, Gemeinsam Verursachte Ausfälle (GVA), Markov-Prozess, Modellierung, Nichtverfügbarkeit, Sensitivitätsanalyse, Signalverarbeitung, Systemausfall, Wahrscheinlichkeit, Zustandsraum

Kurzfassung

Eine Aufgabe der GRS ist die Weiterentwicklung von Methoden der sicherheitstechnischen Bewertung technischer Anlagen, um damit dazu beizutragen, Mensch und Umwelt vor Gefahren und Risiken kerntechnischer Anlagen zu schützen.

Die moderne Leittechnik basiert zunehmend auf softwarebasierten Einrichtungen, die teilweise durch komplexe Netzwerke vernetzt sind. Die Struktur, die Funktionsweise und die Kommunikation sicherheitsrelevanter Leittechnik zeichnen sich durch automatische Fehlererkennung und Fehlerbehandlung aus, wodurch das System im zeitlichen Ablauf verschiedene Zustände annehmen kann. Für die Sicherheits- und Zuverlässigkeitsanalyse der Leittechnik, deren Komponenten in zeitlicher Wechselwirkung zueinanderstehen, sind die klassischen Analysemethoden allein weniger gut geeignet, da diese Methoden die zeitlichen Zustandsänderungen solcher Systeme nicht angemessen berücksichtigen können.

Im Rahmen des BMUB-Vorhabens 3615R01343 „Entwicklung und Erprobung der Werkzeuge zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik“ wurden umfangreiche Arbeiten zur Modellierung von unterschiedlichen Architekturen digitaler Leittechniksysteme mittels Fehlerbaum-Methoden und Markov-Prozessen durchgeführt. Die GRS verfolgt mit diesem Eigenforschungsvorhaben speziell das Ziel, Werkzeuge zur Analyse des Ausfallverhaltens digitaler Leittechnik beim Auftreten potentieller Fehler zu entwickeln, um die Kompetenz und Aussagefähigkeit im Bereich der sicherheitstechnischen Bewertung kerntechnischer Anlagen zu stärken.

Der vorliegende Bericht enthält die Beschreibung der Vorgehensweise bei der Modellierung verschiedener Leittechnikarchitekturen und die Annahmen hinsichtlich Fehlererkennung und Reparaturen. In weiterer Folge werden die Sensitivitätsanalyse sowie die Ergebnisse der Fehlerbaumanalyse und der Markov-Methode miteinander verglichen und erläutert.

Inhaltsverzeichnis

1 Einleitung

Eine zentrale Aufgabe der GRS ist die Entwicklung wissenschaftlicher Erkenntnisse und Methoden auf dem Gebiet der Reaktorsicherheit, um den hohen Sicherheitsstand deutscher Kernkraftwerke weiter zu verbessern. Sie liefert durch wissenschaftlich abgesicherte Analysen und Bewertungen einen Beitrag, um den Stand von Wissenschaft und Technik weiterzuentwickeln sowie Mensch und Umwelt vor Gefahren und Risiken kerntechnischer Anlagen zu schützen.

Die sicherheitsrelevanten Funktionen der Informations-, Steuerungs- und Prozessleittechnik (z. B. Leitechnik der Reaktoranlagen, Leittechnik der Überwachungs- und Handhabungseinrichtungen zur Lagerung und zum Transport radioaktiver Stoffe) sind wichtig, um frühzeitig Störungen bei der Steuerung verfahrenstechnischer Komponenten und in Prozessabläufen zu erkennen und ggf. automatische oder manuelle Gegenmaßnahmen einzuleiten.

Die moderne Leittechnik basiert zunehmend auf softwarebasierten Einrichtungen, die teilweise durch komplexe Netzwerke (z. B. redundante vermaschte Topologien) verbunden sind. Die Struktur, die Funktionsweise und die Kommunikation sicherheitsrelevanter Leittechnik zeichnen sich durch automatische Fehlererkennung und Fehlerbehandlung (u. a. Signalvalidierung, Watch-Dog-Schaltung, Master/Slave-Architektur) aus, wodurch das System im zeitlichen Ablauf verschiedene Zustände (u. a. vollständiger Ausfall einer Funktion, Teilausfall einer Funktion, kurzzeitige Nichtverfügbarkeit einer Teilfunktion, automatische Fehlerbehandlung einer gestörten Teilfunktion) annehmen kann.

Für die Sicherheits- und Zuverlässigkeitsanalyse der Leittechnik, deren Komponenten in zeitlicher Wechselwirkung zueinanderstehen, sind die klassischen Fehler- und Ereignisbaumanalysemethoden allein weniger gut geeignet, da diese Methoden statisch sind und die zeitlichen Zustandsänderungen solcher Systeme nicht angemessen berücksichtigen können.

Die GRS verfolgt mit diesem Eigenforschungsvorhaben das Ziel, Werkzeuge zur Analyse des Ausfallverhaltens digitaler Leittechnik beim Auftreten potentieller Fehler zu entwickeln, um ihre Kompetenz und Aussagefähigkeit im Bereich der sicherheitstechnischen Bewertung kerntechnischer Anlagen zu stärken. Hierzu wurden unterschiedliche Analysemethoden (Fehlerbaumanalyse und Markov-Prozesse) eingesetzt, um das

dynamische Verhalten der Leittechnik beim Eintreten von systeminternen Fehlern zu modellieren. Hiermit sollen möglichst frühzeitig sicherheitstechnische Defizite in der Auslegung und im Betrieb realer Leittechniksysteme aufgedeckt werden. Mit dem entwickelten Werkzeug zur Sensitivitätsanalyse wurden außerdem weitere bisher nicht ausreichend geklärte Fragestellungen zum Einsatz digitaler Leittechnik für sicherheitsrelevante Funktionen methodisch untersucht:

- Bewertung des Einflusses von Diversität in der Leittechnik zur Beherrschung von potentiellen GVA der Hard- und Software,
- Untersuchung bei welchen Fehlerarten und Fehlerraten in einer generischen Leittechnikarchitektur signifikante Verschlechterungen der Zuverlässigkeit zu erwarten sind.

Die Entwicklung des Analysewerkzeugs, das eine systematische und konsistente Unsicherheits- und Sensitivitätsanalyse digitaler Leittechnik erlauben soll, wurde auf den Erkenntnissen des BMUB-Vorhabens 3612R01351 "Entwicklung eines Ansatzes zur Analyse der Netzwerktechnologien in sicherheitsrelevanten Leittechniksystemen hinsichtlich Verbreitung und Auswirkung postulierter Fehler" /HEJ 15/ und auf der in der GRS entwickelten Methode der Unsicherheits- und Sensitivitätsanalyse von Markov- und Semi-Markov-Prozessen /PES 91/ aufgebaut. Die Entwicklung und Erprobung wurde an den generischen Modellen digitaler Leittechnik durchgeführt.

Der Bericht enthält die Beschreibung der Vorgehensweise bei der Modellierung verschiedener Leittechnikarchitekturen und die Annahmen hinsichtlich Fehlererkennung und Reparaturen.

Des Weiteren sind im Bericht die Fehlerbaumanalyse und die Modellierung von Markov-Prozessen mit dem Programm RAMESU (**R**eliability **A**nalysis with **M**arkov-Models **E**xtended by **S**ensitivity- and **U**ncertainty-Analysis) beschrieben, wobei die Verwendung von Markov-Prozessen für die Analyse digitaler Leittechnik ausführlicher als die klassische Fehlerbaummodellierung dargestellt ist.

Ebenfalls werden im Bericht die Sensitivitätsanalyse sowie die Ergebnisse der Fehlerbaumanalyse sowie der Markov-Analyse miteinander verglichen und erläutert. Die Detailergebnisse der Variantenuntersuchungen für alle modellierten Leittechnikarchitekturen (u. a. Ausfalleffektanalyse, Bestimmung von Ausfallraten, Fehlerbäume) sind auf einer CD zusammengefasst und werden bei Bedarf zur Verfügung gestellt.

2 Kurzdarstellung des relevanten Standes von Wissenschaft und Technik

Für die sicherheitstechnische Bewertung sicherheitsrelevanter Leittechnik sind zahlreiche qualitative und quantitative Analysemethoden bekannt, die die GRS bereits im Rahmen verschiedener Forschungsvorhaben (/PIL 10/, /PIL 14/, /HEJ 15/, /JOP 17/) ausgewertet und ggf. eingesetzt hat. Im kerntechnischen Bereich werden häufig folgende Methoden zur Analyse sicherheitsrelevanter Leittechnik eingesetzt

- Verfahren für die Fehlzustandsart und -auswirkungsanalyse (FMEA-Failure Mode and Effects Analysis) /DIN 06/,
- Fehlzustandsbaumanalyse (FTA – Fault Tree Analysis) /DIN 07/,
- Markov-Verfahren /DIN 07a/.

Der Einsatz dieser Methoden ist von der Zielsetzung, der Komplexität des zu analysierenden Objekts und der Verfügbarkeit von Daten und Informationen abhängig. Die Ergebnisse dieser Analysen werden im Rahmen der Nachweisführung (z. B. FMEA in KTA-3503 für Typprüfungen /KTA 15/ und KTA-3903 für Prüfung und Betrieb von Hebezeugen /KTA 12/) gefordert.

Eine bewährte systematische Methode zur Analyse der Fehlerfortpflanzung bzw. der Auswirkungen von Fehlern in komplexen technischen Systemen ist die Fehlerbaumanalyse. Diese wird in der Kerntechnik bereits seit langem insbesondere im Rahmen der probabilistischen Sicherheitsanalyse (PSA) angewendet /FRE 06/, /PIL 10/. Die Fehlerbaumanalyse-Methode ist eine statische Methode und ist deshalb weniger geeignet um dynamische Abläufe, wie z. B. zeitabhängige Zustände eines Systems, zu modellieren. Ergebnisse anderer Analysemethoden (u. a. FMEA, Monte-Carlo-Verfahren) werden üblicherweise als Basisereignisse im Fehlerbaum der Leittechnikausfälle in der PSA verwendet.

Die Eignung verschiedener weiterer Methoden (u. a. Dynamic Flowgraph Methodology, Petri-Netze) für die Zuverlässigkeitsanalyse digitaler Leittechnik wurde bereits vielfach in der Literatur (z. B. /ALD 06/) sowie in den Vorhaben RS1180 /PIL 10/, /HEJ 15/ diskutiert und wird an dieser Stelle nicht weiter erläutert.

In der Vergangenheit wurde in der GRS das Programmsystem RAMESU für probabilistische Sicherheitsanalysen von Reaktoranlagen entwickelt /PES 91/. Mit dem Programm RAMESU können generell zeitliche Abhängigkeitsstrukturen technischer Systeme als Markov- und Semi-Markov Prozesse modelliert und die Wahrscheinlichkeiten von Systemzuständen im zeitlichen Ablauf berechnet werden. Das Programm enthält eine Option zur Durchführung von Unsicherheits- und Sensitivitätsanalysen. Zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in Verbindung mit dem Programm RAMESU wird das Programmsystem SUSA (**S**oftware for **U**ncertainty and **S**ensitivity **A**nalyses) /KLS 14/ verwendet.

Die Programme RAMESU und SUSA wurden bereits erfolgreich bzgl. der Frage nach der möglichen Entstehung einer Kritikalität in der Nachverschlussphase eines Endlagers angewendet /GMA 09/, /KIL 13/.

Die Anwendung des RAMESU-Programms zur Analyse digitaler Leittechnik soll erstmalig im aktuellen Vorhaben erfolgen, um einen möglicherweise erforderlichen Weiterentwicklungsbedarf der Methode zu ermitteln.

3 Methodische Vorgehensweise

Die Methodenentwicklung im Vorhaben erfolgte modellbasiert, wobei die generischen Architekturen digitaler Leittechnik zunächst sehr vereinfacht modelliert wurden. Hierzu wurden Erfahrungen aus den früheren Forschungsvorhaben der GRS zur Zuverlässigkeitsbewertung digitaler Leittechnik (u. a. /FRE 06/, /PIL 10/ und /HEJ 15/) und aus der Mitarbeit der GRS bei der Entwicklung eines FMEA-Leitfadens (/NEA 15/) im Rahmen eines OECD-Projekts angewandt.

3.1 Modellierungsansatz

Zunächst wurde ein Grundmodell bestehend aus den Funktionseinheiten eines rechnerbasierten Leittechniksystems festgelegt, das sowohl Architekturaspekte (z. B. Kommunikationswege) als auch die Funktionsweise der vernetzten Hardware digitaler Leittechnik (u. a. Analogsignalverarbeitung, logische Verknüpfungen, Antriebssteuerung) konsistent berücksichtigt und darüber hinaus erweiterungsfähig ist.

Alle potentiellen Ausfälle (Ausfallarten) von Funktionseinheiten wurden entsprechend der Annahmen aus den Analysen /FRE 06/, /HEJ 15/ und Vorgaben aus /NEA 15/ in zwei Gruppen unterteilt:

- erkannte Ausfälle (SF, engl. Self-signaling Failure) oder
- nichterkannte Ausfälle (NSF, engl. Non Self-signaling Failure).

Die Signalverarbeitung der modellierten digitalen Leittechnikarchitekturen findet auf drei Ebenen statt (Abb. 3.1), wobei jede Ebene aus mehreren redundanten Rechnern bestehen kann, z. B.

- Erfassungsebene AU (engl. Acquisition Unit): Rechner AU1, AU2, AU3 …,
- Verarbeitungsebene PU (engl. Processing Unit): Rechner PU1, PU2, PU3 …,
- Steuerungsebene VU (engl. Voting Unit): Rechner VU1, VU2, VU3 ….

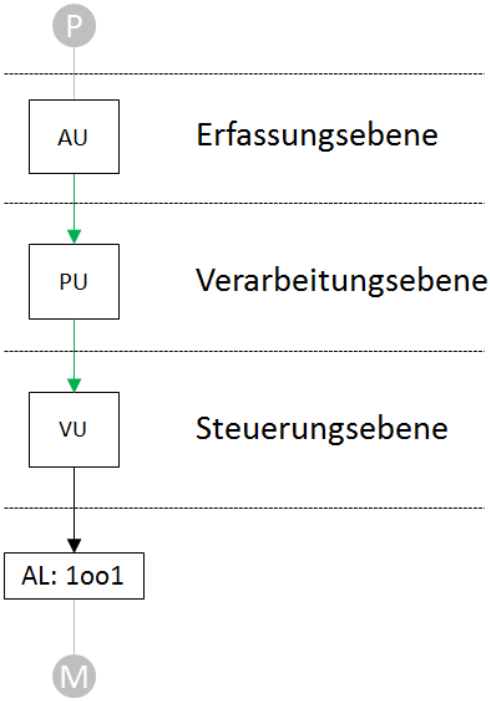

Abb. 3.1 Grundlegender Aufbau der modellierten digitalen Leittechniksysteme

Die Architektur der Leittechnik in Abb. 3.1 besteht aus

- Erfassungsebene (Messwerterfassung), z. B. bestehend aus drei AU-Rechnern:
  - In der Erfassungsebene werden die Messwerte (Prozessparameter der Anlage, wie z. B. Druck, Temperatur, Füllstand, Durchsatz) in redundanten Erfassungsrechnern (AU) erfasst, digitalisiert und als Datentelegramme über das Kommunikationsnetzwerk an die nächste Ebene weitergeleitet.
  - Erkannte Ausfälle werden mit einem entsprechenden Wert (engl. Flag) (Ausfall: „1“, valides Signal: „0“) markiert. Wurde der Fehler erkannt und das Flag auf „1“ gesetzt, so handelt es sich um einen selbstmeldenden Fehler (SF). Ist das Flag hingegen auf „0“ gesetzt, kann es sich sowohl um ein wahres Signal (OK) als auch um ein unerkannt fehlerhaftes Signal (NSF) handeln.
- Verarbeitungsebene (logische Signalverarbeitung), z. B. bestehend aus drei PU-Rechnern:
  - In den redundanten Verarbeitungsrechnern (PU) werden die auf der Erfassungsebene aufbereiteten Messwerte der Prozessparameter durch die Anwendersoftware (LEFU, „Leittechnik-Funktion“) verarbeitet.

- Die validen Werte aus den AUs (Flag „0“) werden in aufsteigender Reihenfolge sortiert und daraus das zweite Maximum (2. Max) bestimmt. Ist eines der Eingangssignale des Verarbeitungsrechners selbstmeldend ausgefallen (Flag „1“), wird das zweite Maximum nur aus den restlichen Signalen des zu überwachenden Parameters gebildet. Sind alle Eingangssignale des Verarbeitungsrechners bis auf eines selbstmeldend ausgefallen, wird das verbliebene Eingangssignal direkt für die mögliche Bildung eines Anregesignals (bei Überschreitung des entsprechenden Grenzwerts) verwendet (Max).

- Das zweite Maximum (oder Maximum, s. o.) wird mit einem Grenzwert verglichen und gegebenenfalls ein binäres Steuersignal („1“ – „EIN“ bzw. „0“ – AUS) zur Weiterleitung an die nächste Ebene generiert. Auch hier werden die erkannten Ausfälle der Rechner (PU) bzw. der Kommunikation zwischen den PUs und VUs mit einem Flag „1“ markiert und daher durch die Signalverarbeitung in den VU als ungültige Signale erkannt.

- Steuerungsebene (2-von-3-Auswahllogik), z. B. bestehend aus drei VU-Rechnern:

  - In den redundanten Votern (VU) werden die binären Signale der vorherigen Ebene durch eine 2-von-3-Auswahl ausgewertet und gegebenenfalls binäre Signale („1“ – EIN bzw. „0“ – „AUS“) zur Steuerung einer verfahrenstechnischen Komponente erzeugt. Liegen also an mindestens zwei der drei Eingänge des Voters valide Anregesignale (Signal „1“, Flag „0“) vor, so wird die entsprechende Leittechnikfunktion aktiviert.

  - Die Ausgangssignale der VUs enthalten keine Fehlererkennungsinformationen, selbstmeldende Fehler werden jedoch gemeldet und können dann gegebenenfalls repariert werden.

  - Fallen ein oder zwei der Eingangssignale selbstmeldend aus, wechselt der Voter intern zu einer 1-von-2-Auswahl, so dass bei einem oder zwei selbstmeldenden Ausfällen ein einzelnes valides Anregesignal für eine Auslösung ausreicht.

Die Antriebssteuerung einer verfahrenstechnischen Komponente des Systems in Abb. 3.1 (M) wurde vereinfacht durch die analoge Logik (AL, z. B. Schaltanlage) modelliert.

Bei der Modellierung der Signalverarbeitung der generischen digitalen Leittechniksysteme werden darüber hinaus folgende konservative Annahmen getroffen:

- Die Kommunikation zwischen den Rechnern erfolgt über ein Netzwerk, welches für die Sicherheitsleittechnik typisch ist /HEJ 15/. Das heißt, es wird angenommen, dass alle Hardwareausfälle im Kommunikationsnetzwerk der Sicherheitsleittechnik immer erkannt werden und daher selbstmeldend sind. Vereinfachend werden daher die Ausfallraten der Kommunikationswege (beispielsweise zwischen AUs und PUs) direkt in den Ausfallraten der entsprechenden signalsendenden Komponenten berücksichtigt (z. B. selbstmeldende Ausfälle von AUs).
- Die Kommunikation zwischen den Ebenen erfolgt in vereinfachter Form, wobei die Signale der Erfassungsebene einen (digitalen) Zahlenwert und die Signale der Verarbeitungsebene binäre Werte darstellen. Hierbei wird zwischen dem Vorliegen eines Anregesignals („1“) und keines Anregesignals („0“) unterschieden. Außerdem wird die Übertragung jedes Signals mit einem Flag gekennzeichnet. Wird ein Signal als fehlerhaft erkannt, wird das Flag auf „1“ gesetzt. Es handelt sich dann um einen selbstmeldenden Fehler (SF). Ist das Flag auf „0“ gesetzt, kann es sich sowohl um ein wahres Signal (OK) als auch um ein unerkannt fehlerhaftes Signal (NSF) handeln.
- Nichtselbstmeldend ausgefallene AUs geben den minimalen Messwert aus.
- Nichtselbstmeldend ausgefallene PUs geben eine logische „0“ aus.
- Ausgefallene VUs geben eine logische „0“ aus.
- Die Software der AUs, PUs und VUs kann sowohl selbstmeldende als auch nichtselbstmeldende Ausfälle verursachen und wird zunächst nicht explizit modelliert. Die berücksichtigten Ausfallraten wurden nur über die möglichen Hardware-Ausfälle bestimmt. Die Auswirkungen der potenziellen Softwarefehler sollen ggf. zu einem späteren Zeitpunkt in einem speziell zu entwickelnden Modell analysiert werden.

Die Messeinrichtungen (u. a. Sensoren, Messumformer), Stromversorgung und Schnittstellen der Leittechnik werden in den vereinfachten Modellen nicht explizit berücksichtigt.

3.1.1 Modellierung verschiedener Leittechnikarchitekturen

Für die Analysen wurden verschiedene Leittechnikarchitekturen modelliert. Diese werden nachfolgend erläutert.

Die Modellbezeichnung ist als alphanumerische Darstellung der Leittechnikarchitektur aufgebaut:

- ein Buchstabe (z. B. A, B) für die unterschiedlichen Varianten der Leittechnikarchitektur (z. B. für jedes Teilsystem, das auf der Basis der Hardware und Software einer spezifischen Leittechniktechnologie aufgebaut ist),
- die Anzahl von redundanten Komponenten jeder Signalverarbeitungsebene einer Leittechnikarchitektur (z. B. Modelle: A222, A133, A333, A133B133).

Das Modellsystem A222 (Abb. 3.2) besteht aus zwei VUs, zwei PUs und zwei AUs. Es dient zusätzlich als Referenzsystem, um die Ergebnisse der Fehlerbaumanalysen mit denen durch Markov-Prozesse gewonnenen Erkenntnissen zu vergleichen. Die zusätzliche Kennzeichnung der Modellsysteme mit Buchstaben (hier „A“) soll später die Unterscheidung zwischen diversitären Teilsystemen ermöglichen. Die einzelnen Komponenten werden zusätzlich gemäß ihrer Redundanzzuordnung durchnummeriert. So bezeichnet beispielsweise AU1.A die AU der ersten Redundanz der Diversität A.

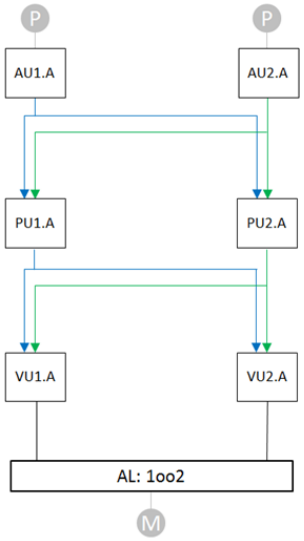

Abb. 3.2 Modellsystem A222

Da bis auf das System A133, bestehend aus einer VU, drei PUs und drei AUs (siehe Abb. 3.3), alle betrachteten Modellsysteme über mehr als eine VU verfügen, sind in allen Systemen den VUs jeweils zusätzlich analoge Baugruppen (AL) nachgeschaltet. Diese führen in Abhängigkeit der Anzahl der Eingangssignale (aus den vorgelagerten

VUs) eine Wertung durch, z. B. für das Modellsystem A222 eine 1-von-2-Auswahl („1oo2“ - „1-out-of-2“) und für das Modellsystem A133 eine 1-von-1-Auswahl („1oo1“).

Die analogen Baugruppen können selbst Ursache von Ausfällen sein. In den Modellen werden im Hinblick auf spätere Modellerweiterungen die ALs mit der nichtselbstmeldenden Ausfallart „Schaltet nicht“ (NSF) berücksichtigt. Bei der Fehlerbaummodellierung der Ausfälle mittels der Software RiskSpectrum wird diese Ausfallart allerdings mit der willkürlich bestimmten sehr kleinen Ausfallrate von $1 \cdot 10^{-10}$ h^{-1} festgelegt, da zunächst nur Effekte innerhalb der digitalen Leittechnik betrachtet werden sollen.

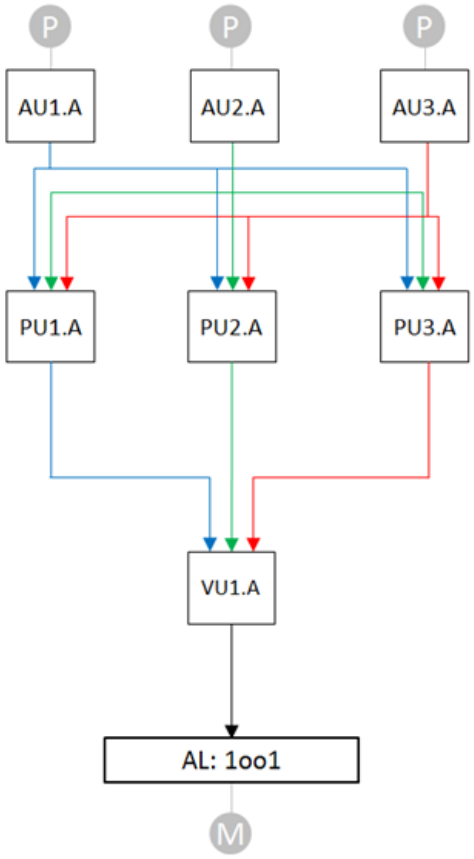

Abb. 3.3 Modellsystem A133.

Als nächst komplexeres System wird das Modellsystem A333 aus drei VUs, drei PUs und drei AUs betrachtet (siehe Abb. 3.4). Da dieses System über drei VUs verfügt, werden deren drei Ausgangssignale durch eine analoge Logik in 2-von-3-Auswahl in der Schaltanlage (AL) bewertet.

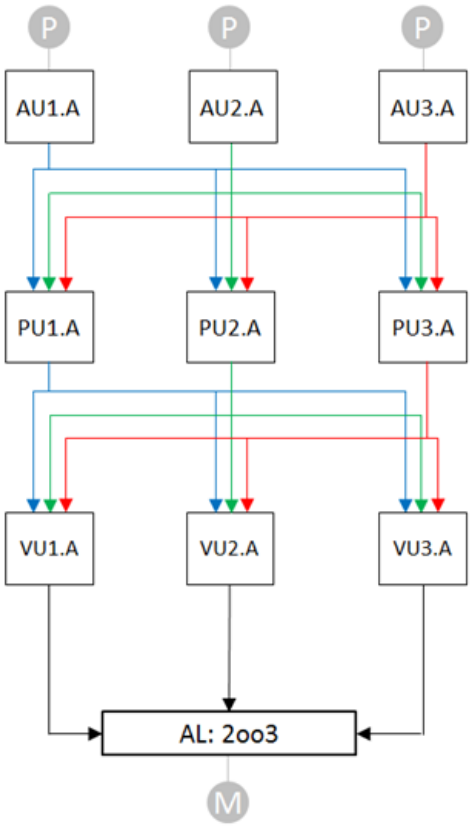

Abb. 3.4 Modellsystem A333

Das Modellsystem A133A133 besteht aus zwei Teilsystemen des Typs A133. Jedes Teilsystem ist aus einer VU, drei PUs und drei AUs aufgebaut (siehe Abb. 3.5). Die Ausgänge der beiden Voter werden von einer analogen Logik (AL) der Schaltanlage in einer 1-von-2-Auswahl verarbeitet.

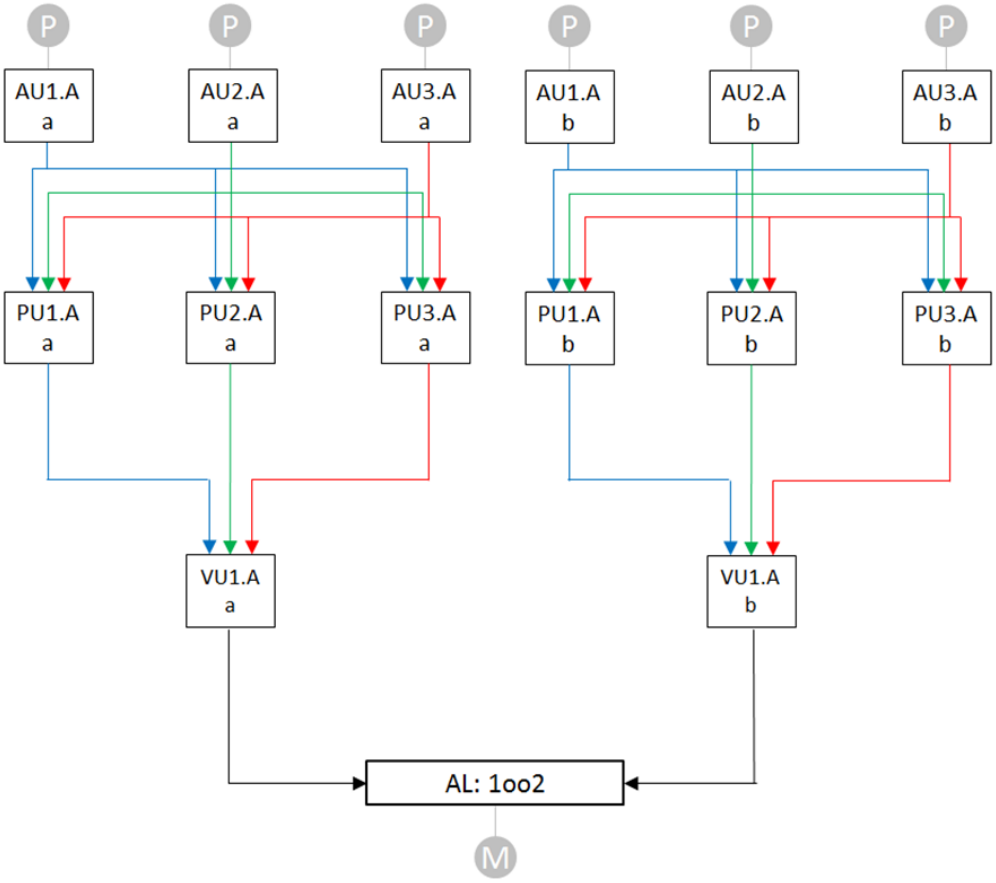

Abb. 3.5 Modellsystem A133A133

Im Modell A133A133 wurde zur Unterscheidung der beiden (identischen) Teilsysteme an die AUs, PUs und VUs zusätzlich ein Index „a“ bzw. „b“ als Indikator für das entsprechende Teilsystem angehängt, wobei keine Diversität in der Hard- und Software angenommen wurde.

Nimmt man für das Modellsystem A133A133 an, dass die beiden Teilsysteme diversitär aufgebaut sind (z. B. Hardware und Software der Leittechnik von unterschiedlichen Herstellern), ergibt sich das Modellsystem A133B133 (siehe Abb. 3.6).

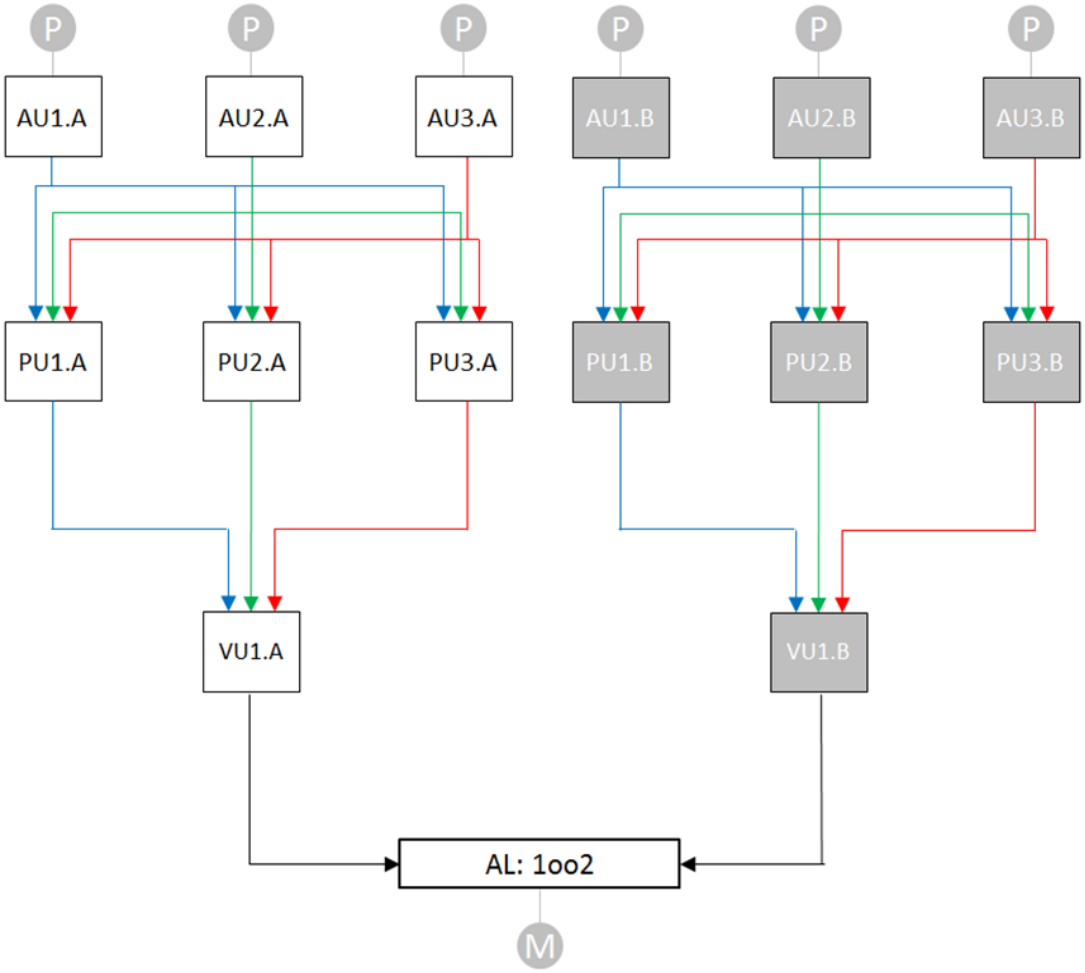

Abb. 3.6 Modellsystem A133B133

Das Modellsystem A2MC(1)33 ist in Abb. 3.7 dargestellt. Es besteht aus zwei Votern, die jeweils über eine Master-Checker-Konfiguration von zwei redundanten Prozessor-Baugruppen (vgl. hierzu Anhang A.2) verfügen, sowie drei PUs und drei AUs. Die Master-Checker-Konfiguration ist ein bewährtes Verfahren zur Erhöhung der Fehlertoleranz eines Rechnersystems, wobei die Master- und Checker-Prozessorpaare die gleichen redundanten Eingangssignale verarbeiten und die Funktion des redundanten Rechners überwachen. Wird ein Fehler in der Signalverarbeitung des Voters identifiziert, dann soll eine Fehlerbehandlungsfunktion (u. a. Abschaltung der VU, Maskierung des fehlerhaften Signals) gestartet werden. Bei Modellierung der Master-Checker-Konfiguration sind entsprechende Annahmen zu treffen.

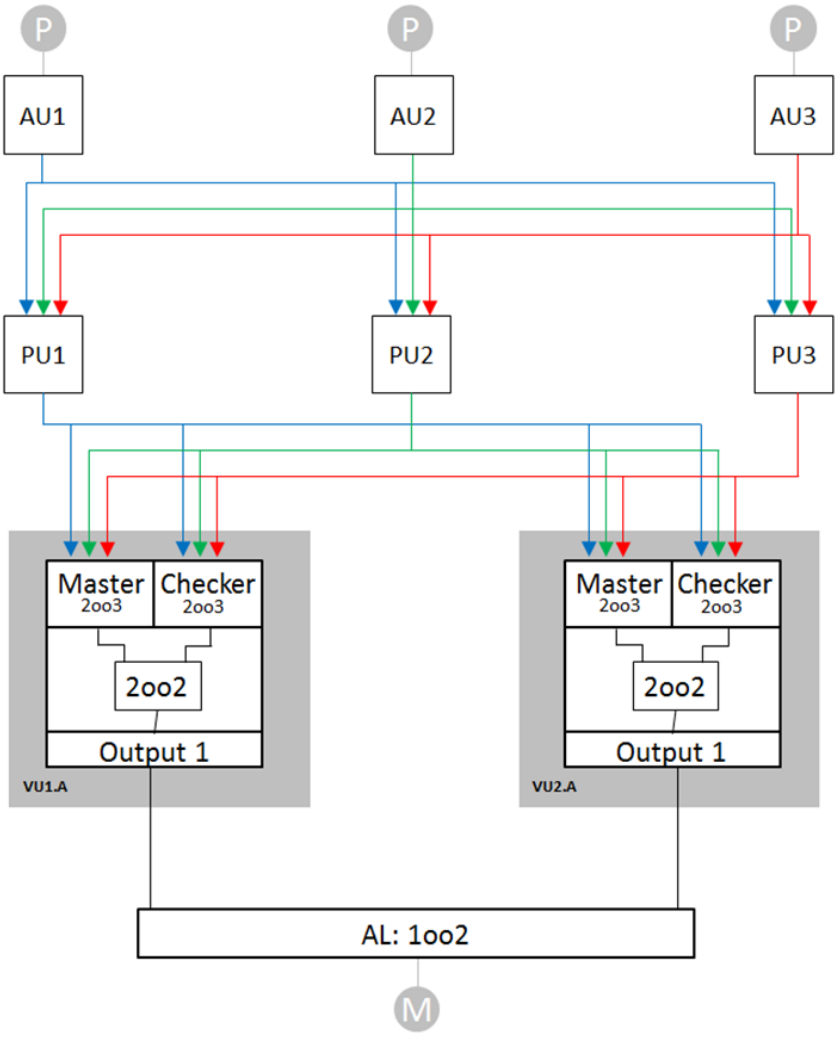

Abb. 3.7 Modellsystem A2MC(1)33

Der Aufbau des Modellsystems A2MC(1)33 entspricht prinzipiell einem Modellsystem mit der Bezeichnung A233, allerdings verändert die Master-Checker-Konfiguration der

VU-Rechner das Ausfallverhalten (siehe Anhang A.1 und A.2) derartig, dass die Einzelausfälle der VU1.A und VU2.A nur noch als selbstmeldende Ausfälle (Annahme zur Ausfallrate: $\lambda \leq 1{,}0 \cdot 10^{-5}\ h^{-1}$) in der Analyse berücksichtigt werden müssen.

Das komplexeste Modellsystem in den durchgeführten Analysen ist das Modell A2MC(2)4. Dieses wurde in Anlehnung an reale Leittechniksysteme (z. B. einige Architekturvarianten der Sicherheitsleittechnik TELEPERM XS der Firma Areva) aus einer AL , zwei VUs (mit jeweils einem Master-Checker-Paar-Voter), vier PUs und vier AUs gestaltet.

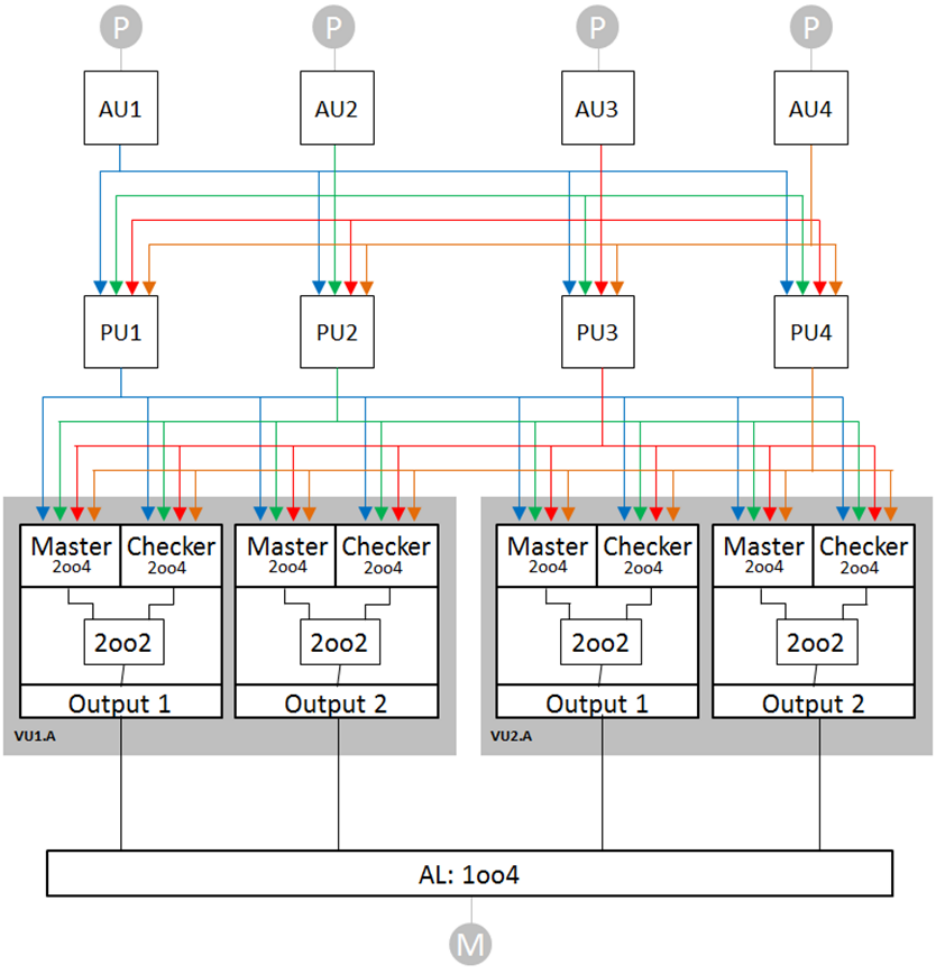

Abb. 3.8 Modellsystem A2MC(2)44

Weitere denkbare Modellvarianten mit Master-Checker-Konfigurationen wurden im Vorhaben nicht analysiert, weil hierzu keine neuen Erkenntnisse hinsichtlich Beherrschung potentieller GVA in der Hardware und Software in den redundanten Architekturen digitaler Leittechnik zu erwarten waren.

3.1.2 Festlegungen von Testzyklen und Reparaturzeiten

Für die Analysen in diesem Bericht werden die in Tab. 3.1 festgelegten Testzyklen verwendet. So wird beispielsweise die Redundanz 1 bei einem dreifachredundanten Aufbau (z. B. AU1.A, PU1.A, VU1.A im Modellsystem A133) in der Woche „0“ und anschließend alle drei Monate einer Prüfung („T“ – Test) unterzogen. Die durchgeführten Tests erlauben es, nichtselbstmeldende Fehler zu finden und anschließend zu beheben.

Die analogen Baugruppen (AL) sind keiner Redundanz zugeordnet und werden zum Zeitpunkt Null („Woche 0“) zum ersten Mal, danach aller 4 Wochen (672 h) getestet, d. h. gemeinsam mit jedem durchgeführten Test in allen Redundanzen.

Für alle Reparaturzeiten aller Baugruppen/Rechner werden dieselben Annahmen getroffen. Diese können in der Realität deutlich schwanken. So kann z. B. in sehr kurzer Zeit eine Karte getauscht werden oder umgekehrt die genaue Fehlerlokalisierung sehr lange dauern. Im Folgenden wird daher für die benötigten Reparaturzeiten eine Wahrscheinlichkeitsverteilung angenommen.

Als plausible Verteilung für die Reparaturzeiten kann eine logarithmische Normalverteilung verwendet werden /NAS 17/. Die Wahrscheinlichkeitsdichteverteilung der logarithmischen Normalverteilung wird durch die Dichtefunktion

$$f(x) = \frac{1}{\sigma \cdot x \cdot \sqrt{2\pi}} \cdot e^{\left\{-\frac{(\ln(x)-\mu)^2}{2\sigma^2}\right\}} \tag{3.1}$$

beschrieben. Im Unterschied zur Normalverteilung stehen hier die beiden Parameter σ^2 und μ aber nicht für die Varianz und den Erwartungswert (Mittelwert) der Verteilung. Für eine gegebene Varianz *Var* und einen Erwartungswert *E* der logarithmischen Normalverteilung lassen sich diese Parameter aber einfach berechnen aus:

$$\sigma^2 = ln\left(\frac{Var}{E^2} + 1\right) \tag{3.2}$$

$$\mu = ln(E) - \frac{\sigma^2}{2} \tag{3.3}$$

Da der GRS keine Daten über Reparaturzeiten vorliegen, wird der Erwartungswert für die Reparaturzeit für die Basisberechnungen zunächst jeweils auf acht Stunden gesetzt (d. h. $E = 8$ h) und später im Sinne der Sensitivitätsanalyse variiert. Die Standardabweichung der Reparaturzeiten ($\sqrt{Var}$) soll im selben Sinne zunächst eine Stunde betragen, d. h. $Var = 1\ h^2$. Es ergeben sich dann für die Parameter σ^2 und μ:

$$\sigma^2 = ln\left(\frac{1\ h^2}{8^2\ h^2} + 1\right) \approx 0{,}0155 \tag{3.4}$$

$$\mu = ln(8) - \frac{0{,}0155}{2} \approx 2{,}0793 \tag{3.5}$$

Die entsprechende Verteilung wird in der folgenden (Abb. 3.9) gezeigt

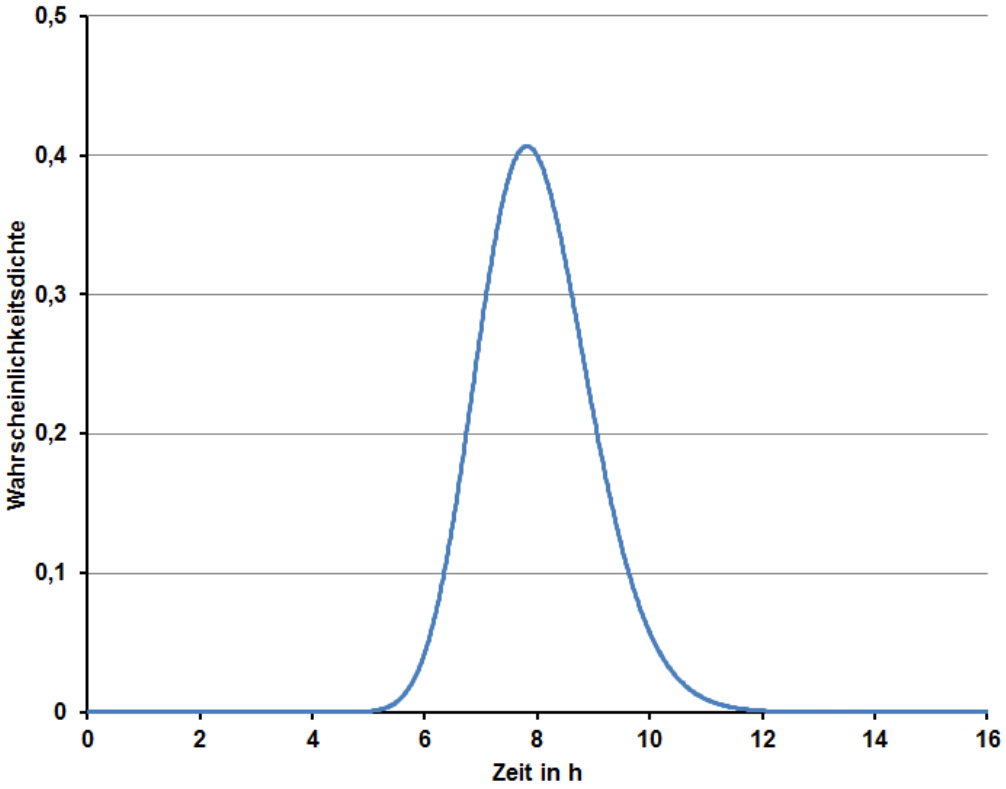

Abb. 3.9 Angenommene Wahrscheinlichkeitsdichtefunktion für die Reparaturzeiten

In der Analysesoftware RiskSpectrum /SCA 12/ werden solche Verteilungen mit Hilfe des oben definierten Erwartungswerts E und dem Fehlerfaktor (engl. Errorfactor, EF) beschrieben.

Der Fehlerfaktor *EF* wird in RiskSpectrum wie folgt definiert:

$$\sigma = \frac{ln(EF)}{1{,}6449} \tag{3.6}$$

(Anm.: 1,6449 ist das $z_{0.95}$-Quantil der Standardnormalverteilung).

Für die Wahrscheinlichkeitsdichtefunktion in Abb. 3.9 ergibt sich somit durch Einsetzen des Wertes für σ aus Gleichung (3.4):

$$EF \approx e^{0{,}1245 \cdot 1{,}6449} \approx 1{,}227 \tag{3.7}$$

Tab. 3.1 Testzyklen für die einzelnen Redundanzen

Die analogen Bausteine der Auswahllogik (AL) werden keiner Redundanz zugeordnet und bei jeder Prüfung mitgetestet (also alle vier Wochen).

2 Redundanzen

Woche:	**0**	**4**	**8**	**12**	**16**	**20**	**24**	**28**	**32**	**36**	**40**	**44**	**48**	**52**
Red. 1	T		T		T		T		T		T		T	
Red. 2		T		T		T		T		T		T		T

3 Redundanzen

Woche:	**0**	**4**	**8**	**12**	**16**	**20**	**24**	**28**	**32**	**36**	**40**	**44**	**48**	**52**
Red. 1	T			T			T			T			T	
Red. 2		T			T			T			T			T
Red. 3			T			T			T			T		

4 Redundanzen

Woche:	**0**	**4**	**8**	**12**	**16**	**20**	**24**	**28**	**32**	**36**	**40**	**44**	**48**	**52**
Red. 1	T				T				T				T	
Red. 2		T				T				T				T
Red. 3			T				T				T			
Red. 4				T				T				T		

3.1.3 Ausfallraten der Funktionseinheiten

Die für die Erstellung der Fehlerbaum-Modelle verwendeten Ausfallraten der einzelnen Komponenten (AUs, PUs, VUs) wurden aus dem im GRS-Bericht 377 /HEJ 15/ beschriebenen Modell bestimmt. Die Vorgehensweise wird in den Abschnitten A.1 und A.2 im Anhang) beschrieben. An dieser Stelle werden nur die für Fehlerbaummodellierung relevanten Ausfallraten aufgelistet.

Um darüber hinaus Ausfälle gemeinsamer Ursache (GVA, engl. Common Cause Failures, CCF) zu berücksichtigen, wurde zusätzlich angenommen, dass jeweils 2,5 % der nichtselbstmeldenden Ausfälle einer Komponente durch GVA der entsprechenden Komponentenart (z. B. AUs) und weitere 2,5 % durch einen GVA aller Komponenten des Teilsystems (einer Diversität, z. B. A) verursacht werden. Es ergeben sich die Ausfallraten in Tab. 3.2.

Tab. 3.2 Ausfallraten bei Berücksichtigung von GVA

Parameter	**λ (Ausfallraten aus RiskSpectrum)**	**Anmerkungen**
FR AL NSF	1E-10 h^{-1}	Analog Logic
FR AU SF	2,09832E-05 h^{-1}	incl. COM_AU1.A_PU1.A
FR AU NSF	8,26472E-08 h^{-1}	
FR PU SF	1,57295E-05 h^{-1}	incl. COM_PU1.A_VU1.A
FR PU NSF	8,26472E-08 h^{-1}	
FR VU SF	6,97175E-06 h^{-1}	
FR VU NSF	8,26472E-08 h^{-1}	
FR AU CCF	2,17493E-09 h^{-1}	CCF of all AUx.A
FR PU CCF	2,17493E-09 h^{-1}	CCF of all PUx.A
FR VU CCF	2,17493E-09 h^{-1}	CCF of all VUx.A
FR ALL CCF	2,17493E-09 h^{-1}	CCF of all components of A

Außerdem wird angenommen, dass alle GVA bei jeder Prüfung in einer beliebigen Redundanz bemerkt und anschließend innerhalb derselben Zeit wie die entsprechenden nichtselbstmeldenden Ausfälle behoben werden.

Wie bereits erwähnt, werden in den Modellsystemen zusätzlich analoge Logikbausteine verwendet (AL), die eine Schaltanlage darstellen. Diese werden im Hinblick auf spätere Erweiterungen mit der nichtselbstmeldenden Ausfallart „schaltet nicht“ (NSF) be-

rücksichtigt, allerdings zunächst mit der festgelegten Ausfallrate von $\lambda = 1 \cdot 10^{-10}$ h^{-1}. Diese Ausfallrate wurde extra so klein angenommen, um die Ausfalleffekte nur innerhalb der digitalen Leittechnik im Rahmen der Fehlerbaumanalyse (u. a. Analyse der Minimalschnitte) besser erfassen zu können.

Werden VUs mit sogenannter Master-Checker-Konfiguration verwendet, so ändern sich die Kenndaten der VUs (siehe Anhang A.2) und diese können dann auch nur noch selbstmeldend mit der Ausfallrate $\lambda = 1{,}0 \cdot 10^{-5}$ h^{-1} ausfallen.

Tab. 3.3 Ausfallraten für VUs mit Master-Checker-Konfiguration

Parameter	**λ (Ausfallraten aus RiskSpectrum)**	**Anmerkungen**
FR AL NSF	1E-10 h^{-1}	Analog Logic
FR AU SF	2,09832E-05 h^{-1}	incl. COM_AU1.A_PU1.A
FR AU NSF	8,26472E-08 h^{-1}	
FR PU SF	1,57295E-05 h^{-1}	incl. COM_PU1.A_VU1.A
FR PU NSF	8,26472E-08 h^{-1}	
FR VU SF	1,0288E-05 h^{-1}	no NSF due to Master-Checker
FR AU CCF	2,17493E-09 h^{-1}	CCF of all AUx.A
FR PU CCF	2,17493E-09 h^{-1}	CCF of all PUx.A
FR VU CCF	2,17493E-09 h^{-1}	CCF of all VUx.A
FR ALL CCF	2,17493E-09 h^{-1}	CCF of all components of A

3.2 Analysemethodik

Für die übersichtliche und allgemeinverständliche Darstellung der verwendeten Methoden (Ausfalleffektanalyse, Fehlerbaumanalysen, Markov-Prozesse) wird im Folgenden das sehr vereinfachte Modellsystem A120 verwendet (Abb. 3.10), welches nachfolgend kurz erläutert wird:

- Zwei Messungen (hier „P“ für Druckmessungen), bei denen angenommen wird, dass sie stets fehlerfrei funktionieren und ihre Signale fehlerfrei an die oberste Ebene der Leittechnik weitergeben, sind jeweils an eine Zusammenfassung von AU- und PU-Rechnern (engl. Acquisition and Processing Unit, APU) angeschlossen. Diese erfassen die Messwerte und überwachen die Eingangssignale auf

Überschreitung eines MAX-Grenzwerts. Wird der Grenzwert überschritten, so gibt die jeweilige APU eine logische „1“ aus.

- Die Voting Unit VU1 bewertet die Eingangssignale mit einer 1-von-2-Auswahl. Stehen also ein oder zwei Signale mit einer logischen „1“ am Eingang der VU1 an, so gibt sie einen Startbefehl an den angeschlossenen Motor (M) aus. Der angeschlossene Motor soll stets fehlerfrei auf Signale von der VU1 reagieren.

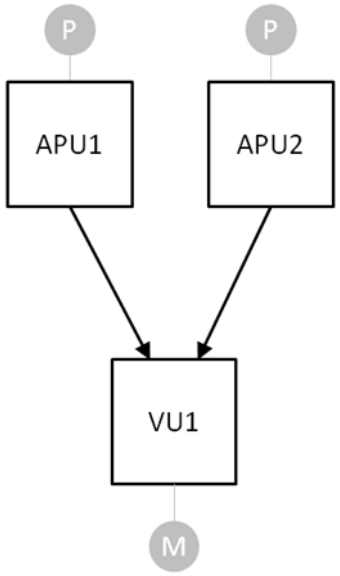

Abb. 3.10 Modellsystem A120

Es wird angenommen, dass alle Kommunikationswege stets fehlerfrei funktionieren. Die leittechnischen Komponenten können entweder fehlerfrei funktionieren (OK) oder nichtselbstmeldend ausfallen (NSF). Für dieses Beispielmodell gibt es daher drei Basisereignisse (siehe Tab. 3.4).

Tab. 3.4 Basisereignisse des Beispielmodells A120 mit Ausfallraten

Basisereignis	**Beschreibung**	**Ausfallrate λ**
APU1.NSF	Nichtselbstmeldender Ausfall von APU1	$4 \cdot 10^{-2}\ h^{-1}$
APU2.NSF	Nichtselbstmeldender Ausfall von APU2	$4 \cdot 10^{-2}\ h^{-1}$
VU1.NSF	Nichtselbstmeldender Ausfall von VU1	$2 \cdot 10^{-2}\ h^{-1}$

3.2.1 Ausfalleffektanalyse

Die folgende Tab. 3.5 gibt eine Übersicht über alle denkbaren Zustände der Komponenten des Systems A120. Sie berücksichtigt alle Kombinationen von funktionsfähigen (OK) und ausgefallenen Komponenten (NSF). Der Gesamtzustand des Systems muss zu einem beliebigen Zeitpunkt einer Zeile dieser Tabelle entsprechen. Die letzte Spalte gibt an, ob das Modellsystem A120 aufgrund der jeweiligen Kombination als ausgefallen gelten muss (und damit unverfügbar ist) oder nicht.

Tab. 3.5 Übersicht über die möglichen Komponentenzustände des Modells A120

lfd. Nummer	APU1	APU2	VU1	Gesamtausfall
1	OK	OK	OK	nein
2	NSF	OK	OK	nein
3	OK	NSF	OK	nein
4	OK	OK	NSF	ja
5	NSF	NSF	OK	ja
6	NSF	OK	NSF	ja
7	OK	NSF	NSF	ja
8	NSF	NSF	NSF	ja

3.2.2 Fehlerbaumanalyse

Die Fehlerbaumanalyse für das Modellsystem A120 wurde mit der Software RiskSpectrum durchgeführt. Da in den späteren Analysen Test- und Reparaturzeiten berücksichtigt werden, wurden bereits für dieses einfache Beispiel die entsprechenden Berechnungsmodelle der Fehlerbaumanalyse verwendet. Dabei wurden allerdings die Zeitintervalle für Test- und Reparaturzeiten so groß gewählt, dass innerhalb der hier betrachteten Zeiträume keine Prüfungen der Komponenten durchgeführt und daher Ausfälle nicht entdeckt oder behoben wurden.

Der Fehlerbaum für das Modellsystem A120 lässt sich in der Software RiskSpectrum wie in Abb. 3.11 gezeigt darstellen.

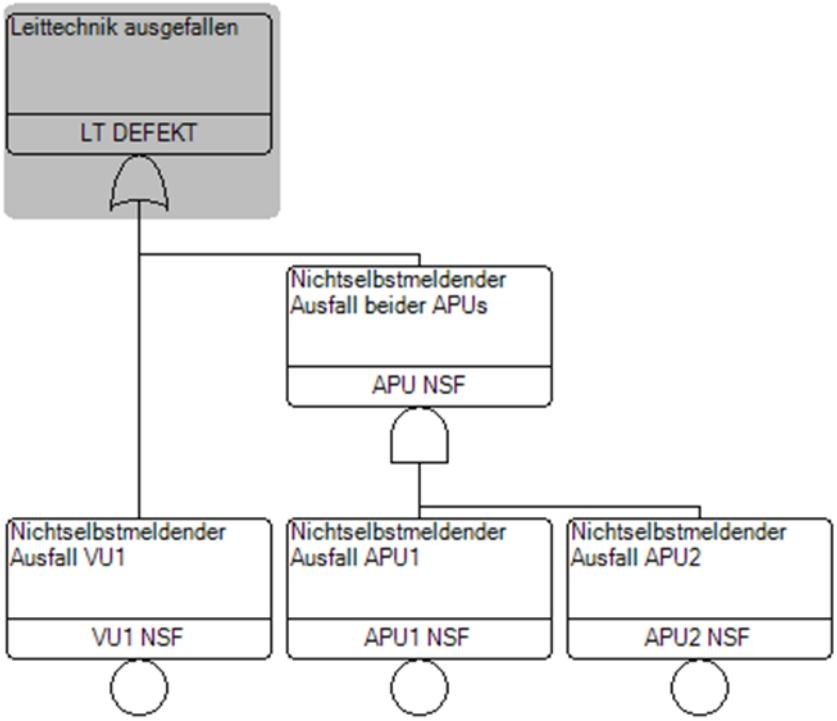

Abb. 3.11 Fehlerbaum für das Modellsystem A120

Wie im vorangegangenen Abschnitt wurde auch hier von den folgenden Ausfallraten ausgegangen:

- Ausfallrate einer APU $4 \cdot 10^{-2}\ h^{-1}$ für APU1 und APU2,
- Ausfallrate einer VU1 $2 \cdot 10^{-2}\ h^{-1}$ für VU1.

Die Rechnung mit der Analysesoftware RiskSpectrum liefert hierzu zeitabhängige Ergebnisse. In Abb. 3.12 ist die Wahrscheinlichkeit für die Verfügbarkeit bzw. Unverfügbarkeit des Modellsystems A120 in Abhängigkeit von der Zeit für die ersten 100 Stunden dargestellt.

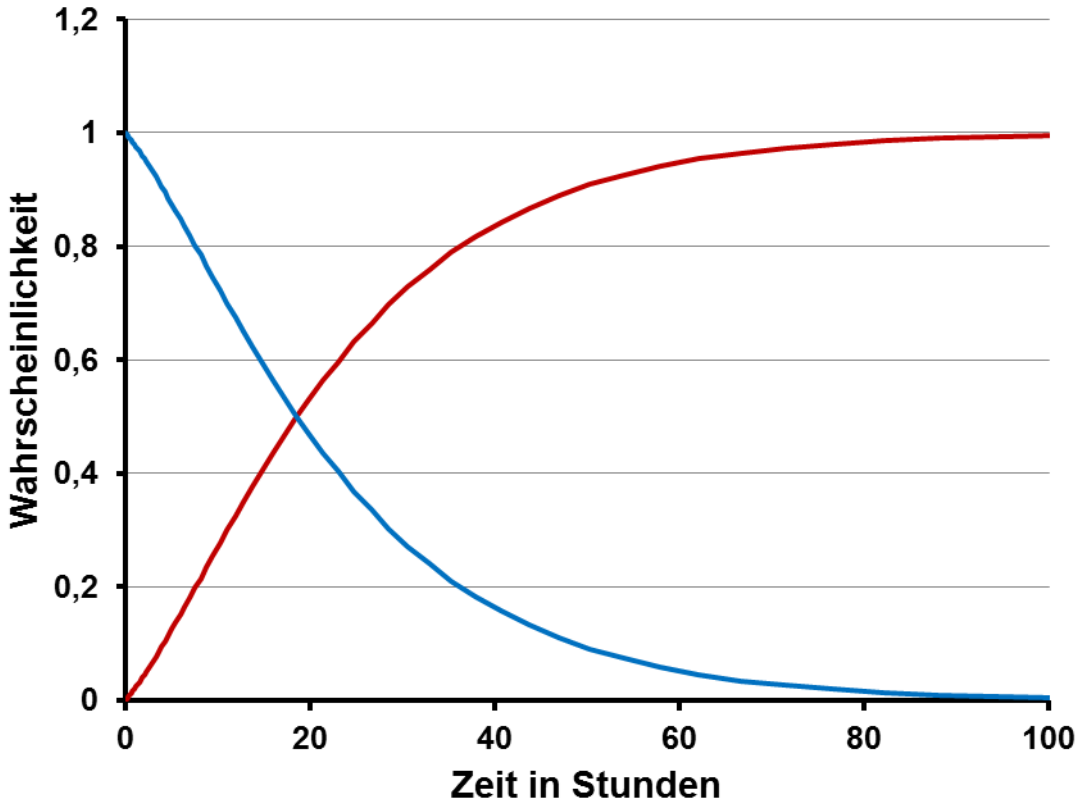

Abb. 3.12 Die berechnete Verfügbarkeit (blau) und Unverfügbarkeit (rot) für das Modellsystem A120 als Funktion der Zeit (in Stunden)

3.2.3 Markov-Prozess-Analysemethode

Für die Sensitivitätsuntersuchungen in diesem Vorhaben soll als Vergleich zur Fehlerbaumanalyse die Methode der Markov-Prozesse angewendet werden, um die Zuverlässigkeit dynamischer Systeme zu ermitteln.

Im Kapitel 4 wird eine allgemeine mathematische Beschreibung der Markov-Prozesse gegeben sowie das in der GRS entwickelte und eingesetzte Programm RAMESU /BRO 88/, /PES 91/ kurz erläutert.

Im Unterkapitel 4.1 wird detailliert dargestellt, wie die Berechnung der Zustandswahrscheinlichkeiten in einem Markov-Prozess für ein einfaches System prinzipiell ausgeführt werden können. An diesem einfach gehaltenen Demonstrationsbeispiel können die Wahrscheinlichkeitsberechnungen nachvollzogen werden, ohne dass das zugrundeliegende Differentialgleichungssystem (s. Gleichung (4.2)) gelöst werden muss.

Wie die Berechnungen eines Markov-Prozesses durch eine Matrix-Schreibweise vereinfacht werden können, wird kurz in Abschnitt 4.2 beschrieben und an einem Beispiel demonstriert.

In Abschnitt 4.3 wird sowohl die Fehlerbaumanalyse unter Verwendung der Software RiskSpectrum als auch die Methode der Markov-Prozesse unter Verwendung des Programmsystems RAMESU an dem einfachen Beispiel des Modells A120 angewendet. Anhand dieses Beispiels wird außerdem diskutiert, welche Unterschiede in den Modellierungsmöglichkeiten zwischen Markov-Prozessen und der Fehlerbaumanalyse bestehen.

4 Mathematische Beschreibung eines Markov-Prozesses und Eigenschaften des GRS-Programms RAMESU

Ein Markov-Prozess ist ein mathematisches Modell zur Untersuchung komplexer Systeme, wobei der dynamische Aspekt im Verhalten der Systeme berücksichtigt werden kann.

In vielen Anwendungen treten Abhängigkeiten zwischen den Ereignissen nachfolgender Zeitpunkte oder auch nachfolgender Handlungsschritte auf. In dieser Situation müssen die zeitlichen Abhängigkeiten im Verhalten der Systemkomponenten berücksichtigt werden. Dies kann durch die klassische Methode zur Zuverlässigkeitsbestimmung komplexer Systeme (z. B. Fehlerbaumanalyse) nicht in ausreichendem Maß durchgeführt werden, da zeitliche Abhängigkeiten nur sehr eingeschränkt berücksichtigt werden. Um zeitliche Abhängigkeiten umfassender berücksichtigen zu können, müssen Methoden der stochastischen Prozesse eingesetzt werden.

Ein stochastischer Prozess ist definiert als eine Menge $\{X_t, t \in T\}$ von Zufallsvariablen, wobei T einen diskreten oder stetigen Parameterraum beschreibt, z. B. diskrete Zeitschritte oder ein stetiges Zeitintervall. Die einfachste Abhängigkeitsstruktur zwischen zeitabhängigen Zufallsvariablen erhält man, wenn die Markov-Eigenschaft gilt. Die Markov-Eigenschaft besagt, dass die Zukunft des Prozesses nur vom Zustand der Gegenwart abhängt und nicht von den Zuständen, die das System in der Vergangenheit angenommen hat. Formal kann das durch die Gleichung (4.1) ausgedrückt werden:

$$\begin{aligned} P(X(t_n) = i_n \mid X(t_{n-1}) = i_{n-1},\, X(t_{n-2}) = i_{n-2}, \dots, X(t_0) = i_0) \\ = P(X(t_n) = i_n \mid X(t_{n-1}) = i_{n-1}) \end{aligned} \tag{4.1}$$

wobei $t_n > t_{n-1} > \cdots > t_1 > t_0$ und $n \geq 1$.

D. h., die Wahrscheinlichkeit des Zustands $X(t_n) = i_n$ zum Zeitpunkt t_n ist nur vom zuletzt angenommenen Zustand $X(t_{n-1}) = i_{n-1}$ zum Zeitpunkt t_{n-1} abhängig und nicht von den zu vorhergehenden Zeiten $t_{n-2}, \dots, t_0$ angenommenen Zuständen $i_{n-2}, \dots, i_0$.

Um ein System durch einen Markov-Prozess zu modellieren, müssen die möglichen Zustände, die das System zu beliebigen Zeiten annehmen kann, explizit definiert wer-

den. Wenn das zu untersuchende System die unterschiedlichen Zustände $1, \dots, N$ annehmen kann, dann erhält man durch die Anwendung eines Markov-Modells die Zustandswahrscheinlichkeiten $P_j(t)\big|_{j=1,\dots,N}$ des Systems zu beliebigen Zeitpunkten t. Hierbei ist $P_j(t)$ die Wahrscheinlichkeit, dass sich das System zu einem beliebigen Zeitpunkt t im Zustand $j = 1, \dots, N$ befindet. Mit der Berechnung der Zustandswahrscheinlichkeiten $P_j(t)$ kann z. B. das Ausfallverhalten des Systems im zeitlichen Verlauf beschrieben werden.

Zur Berechnung der Zustandswahrscheinlichkeiten $P_j(t)\big|_{j=1,\dots,N}$ muss neben dem Zustandsraum des Systems noch zusätzlich die Matrix der Übergangswahrscheinlichkeiten (für diskrete Zeitschritte) bzw. die Matrix der Übergangsraten (im stetigen Fall) spezifiziert werden. Die Matrix der Übergangsraten $R = (r_{ij})$ vom Zustand i in den Zustand j wird auch als Intensitätsmatrix bezeichnet. Die Elemente der Intensitätsmatrix R sind definiert als $r_{ij} = \lim_{\Delta t \to 0} \frac{P(X(t+\Delta t)=j \mid X(t)=i)}{\Delta t}$ und geben die Rate an, dass der Prozess vom Zustand *i* in den Zustand *j* übergeht. Somit ist $r_{ij} \cdot \Delta t$ die Wahrscheinlichkeit, dass der Prozess vom Zustand *i* in den Zustand *j* in einem Zeitintervall Δt übergeht. Ein Markov-Prozess hat die Eigenschaft, dass ein Übergang in einen anderen Zustand nur nach exponentialverteilten Verweildauern möglich ist. Die Übergangsraten können somit als Parameter von Exponentialverteilungen betrachtet werden /FAH 81/.

Zur Berechnung der Zustandswahrscheinlichkeiten $P_j(t)\big|_{j=1,\dots,N}$ eines Systems durch einen Markov-Prozess muss zusätzlich der Anfangszustand $P_j(t = 0)$ des Systems definiert werden. Normalerweise wird der Anfangszustand eines Systems so gewählt, dass das System zum Zeitpunkt *t = 0* mit Wahrscheinlichkeit 1 in einem intakten Zustand ist, d. h. alle Komponenten des Systems sind intakt. Es besteht aber auch die Möglichkeit den Anfangszustand so zu wählen, dass sich das System zu Beginn der Untersuchung mit bestimmten Wahrscheinlichkeiten in verschiedenen Zuständen befinden kann. Beispielsweise könnte der Anfangszustand eines Systems mit zwei Komponenten so definiert werden, dass sich das System zu Beginn der Berechnung mit einer Wahrscheinlichkeit von 0,7 in einem intakten Zustand befindet (d. h. Komponenten 1 und 2 im intakten Zustand) und mit einer Wahrscheinlichkeit von 0,3, dass sich Komponente 1 in einem ausgefallenen Zustand und Komponente 2 im intakten Zustand befindet. Damit kann der Einfluss von Unsicherheiten unterschiedlicher Anfangsbedingungen auf die Berechnung der zeitabhängigen Zustandswahrscheinlichkeiten sehr einfach berücksichtigt werden.

Mit den Definitionen

- des Zustandsraumes $j = 1, \ldots, N$ des zu berechnenden Systems,
- der Matrix der Übergangsraten $R = (r_{ij})$ vom Zustand i in den Zustand j und
- dem Anfangszustand $P_0(j)$ des Systems

lassen sich die Zustandswahrscheinlichkeiten $P_j(t), j = 1, \ldots, N$ für beliebige Zeitpunkte t durch das in Gleichung (4.2) dargestellte Differentialgleichungssystem lösen:

$$\begin{pmatrix} \frac{dP_1(t)}{dt} \\ \frac{dP_2(t)}{dt} \\ \vdots \\ \frac{dP_N(t)}{dt} \end{pmatrix} = \begin{pmatrix} -\sum_{k=2}^{N} r_{1,k} & r_{2,1} & \cdots & r_{N,1} \\ r_{1,2} & -\sum_{\substack{k=1 \\ k\neq 2}}^{N} r_{2,k} & \cdots & r_{N,1} \\ \vdots & \vdots & & \vdots \\ r_{N,1} & r_{N,2} & \cdots & -\sum_{K=1}^{N-1} r_{N,k} \end{pmatrix} \begin{pmatrix} P_1(t) \\ P_2(t) \\ \vdots \\ P_N(t) \end{pmatrix} \qquad (4.2)$$

Bei der Modellierung von Systemen durch Markov-Modelle kann der Zustandsraum des Modells schnell sehr groß werden. In diesem Fall bietet es sich an, geeignete Computer-Programme zur Systemmodellierung durch Markov-Prozesse zu verwenden.

In der GRS wurde das Programm RAMESU (**R**eliability **A**nalysis with **M**arkov-Models **E**xtended by **S**ensitivity- and **U**ncertainty-Analysis) entwickelt, das die Zuverlässigkeit eines technischen Systems durch einen Markov-Prozess modelliert und verschiedene zusätzliche Modellierungsmöglichkeiten erlaubt /PES 91/. In diesem Programm lassen sich Einflüsse von redundanten Systemauslegungen genauso leicht einbeziehen wie der Einfluss von verschiedenen Test-, Wartungs- und Reparaturstrategien. In beschränktem Ausmaß können auch Abhängigkeiten des Prozesses von physikalischen Größen (wie z. B. Druck, Temperatur etc.) berücksichtigt werden. Eine genauere Beschreibung des Programms RAMESU ist in /BRO 88/, /PES 91/ zu finden.

Das Programm RAMESU hat die besondere Eigenschaft, dass es in der Lage ist, Situationen, in denen zu bestimmten Zeitpunkten Veränderungen auftreten (z. B. Erhöhung der Ausfallrate einer Komponente, die bereits eine bestimmte Zeit in Betrieb ist), zu modellieren. Ein reiner Markov-Prozess wäre dazu nicht geeignet, da ein Markov-Prozess – wie oben bereits erwähnt – Zustandsänderungen lediglich nach exponential-

verteilten Verweildauern erlaubt. Durch die speziellen Eigenschaften des Programms, können folgende Situationen für die Modellierung dynamischer Systeme berücksichtigt werden:

a) Übergangsraten, die in der Intensitätsmatrix R angegeben werden, können vom aktuellen Zustand des Systems und seiner Umgebung abhängen. Unter bestimmten Bedingungen können sich somit die Werte einiger Übergangsraten zu bestimmten Zeitpunkten verändern. Beispielsweise könnten sich die Ausfallraten verschiedener Komponenten um einen gewissen Betrag erhöhen, wenn die jeweiligen Komponenten eine bestimmte Zeit in Betrieb sind oder sich bestimmte Umgebungsbedingungen (z. B. Temperatur überschreitet einen kritischen Schwellenwert) zu bestimmten Zeitpunkten einstellen. Sowohl die Übergangsraten selbst als auch die Beträge, um die sich die Übergangsraten erhöhen, sowie die Zeitpunkte zu denen Änderungen von Übergangsraten eintreten, können im Programm RAMESU als unsichere Größen in Form von Kenntnisstandunsicherheiten spezifiziert werden.
   Mit diesen Modellierungsmöglichkeiten könnten beispielsweise die Auswirkungen verschiedener Alterungseffekte von Komponenten relativ einfach in der Analyse berücksichtigt und quantifiziert werden.

b) Die Verweilzeit des Prozesses in einer spezifizierbaren Menge von Zuständen, kann durch eine Zeitkomponente über einen bzw. mehrere Zeitzähler erfasst werden. Damit kann z. B. eine Situation modelliert werden, dass sich das System über eine gewisse Zeit in einem defekten Zustand befinden kann (AOT – Allowable Outage Time), in der es ggf. repariert werden kann. Erst wenn das System innerhalb der AOT nicht repariert werden kann, gilt das System als ausgefallen.
   Des Weiteren können zeitliche Zustandsänderungen erfasst werden, die z. B. bei Umschaltungen, Systemtests und Änderungen physikalischer Größen auftreten.

c) Reparaturen können nicht nur über eine exponentialverteilte Wahrscheinlichkeit modelliert werden. Es besteht die Möglichkeit, bestimmte Zeiten für Reparaturen sowie auch Wahrscheinlichkeiten dafür anzugeben, dass die Reparaturen in dem angegebenen Zeitraum erfolgreich durchgeführt werden.
   In der Fehlerbaumanalyse wird von der Annahme ausgegangen, dass eine Komponente nach einem Test oder einer Reparatur so gut wie neu (‚As Good As New') ist. Diese ‚As Good As New'-Annahme der Fehlerbaumanalyse ist aber nicht in jedem Falle gerechtfertigt. Beispiele aus der Realität belegen, dass nach der Durchführung von Reparatur-, Instandhaltungs- und Wartungsarbeiten die betroffenen Komponen-

ten durch menschliche Fehler weiterhin in einem geschädigten Zustand vorliegen können, wodurch sich die Ausfallwahrscheinlichkeit der Komponente erhöht. Die ‚As Good As New'- Annahme der Fehlerbaumanalyse würde in solchen Fällen somit zu einer Unterschätzung der Ausfallwahrscheinlichkeit des Systems führen. Analog gilt dies auch für die regelmäßig durchgeführten Tests von Systemkomponenten.

Mit dem Programm RAMESU können Situationen modelliert werden, in denen eine Reparatur oder ein Komponententest nicht erfolgreich durchgeführt wurde, sondern sich die Komponente nach der Reparatur oder nach dem Test mit einer gewissen Wahrscheinlichkeit in einem mehr oder weniger geschädigten Zustand befindet. Der geschädigte Zustand, den die Komponente nach dem Reparaturversuch oder nach dem Test annimmt, kann sich dann in einer mehr oder weniger starken Erhöhung der Ausfallrate der jeweiligen Komponente auswirken.

Mit diesen Modellierungsmöglichkeiten kann mit dem Programm RAMESU z. B. untersucht werden, in welchem Ausmaß die Ausfallwahrscheinlichkeit eines Systems durch die optimistische ‚As Good As New' Annahme (die in der Fehlerbaumanalyse zugrunde liegt) unterschätzt wird, wenn davon ausgegangen wird, dass eine Komponente nach durchgeführtem Test nicht mit einer neuen Komponente gleichzusetzen ist.

d) Da man in der Regel von Unsicherheiten für die Parameter des Markov-Prozesses (z. B. Übergangsraten von Zuständen, Wahrscheinlichkeiten mit denen bestimmte Zustände zu den definierten Anwendungszeiten angenommen werden) ausgehen muss, wurde das Programm um eine Option zur Durchführung einer Unsicherheits- und Sensitivitätsanalyse erweitert. Zur Durchführung einer Unsicherheits- und Sensitivitätsanalyse wird das Programm RAMESU über eine Schnittstelle mit dem in der GRS entwickelten Softwaresystem SUSA gekoppelt.

Die Modellierung eines Systems erfolgt in dem Programm RAMESU über spezielle Anweisungen, die zur Vereinfachung der Systembeschreibung dienen. Unter Verwendung dieser speziellen Systembeschreibung werden der gesamte Zustandsraum des Systems, die Matrix der Übergangsraten R und die jeweiligen Matrizen zur Erfassung bestimmter zeitlicher Inhomogenität automatisch generiert. Auch die Zustandswahrscheinlichkeiten zu beliebigen Zeitpunkten werden berechnet. Auf die Struktur der Anweisungen zur Beschreibung eines Systems wird in den nachfolgenden Abschnitten näher eingegangen.

4.1 Beschreibung eines Markov-Prozesses anhand eines einfachen Modellsystems

In diesem Abschnitt wird die Ausführung eines Markov-Prozesses anhand eines einfachen Systems beschrieben. Dazu werden zunächst Berechnungen für ein noch einfacheres Beispiel als das Modellsystem A120 durchgeführt, da die notwendigen Rechenschritte dann noch einzeln erläutert werden können. Bereits für relativ einfache Systeme (wie beispielsweise das Modellsystem A120) können die notwendigen Berechnungen jedoch recht unübersichtlich und umfangreich werden.

Als erstes Beispiel wird daher das in Abb. 4.1 dargestellte Modellsystem betrachtet, das nach der in diesem Dokument verwendeten Nomenklatur als A110 bezeichnet wird. Dieses Modellsystem besteht aus zwei Komponenten, einer APU (eine kombinierte AU-PU; AU – Acquisition Unit; PU – Processing Unit) und einer VU (Voting Unit). Die APU1 erhält Messwerte aus einem analogen Messumformer („P“ – Druckmessung), der im Folgenden als fehlerfrei angenommen wird, und vergleicht den Messwert mit einem intern hinterlegten MAX-Grenzwert. Die APU1 gibt eine logische „1“ an die VU1 weiter, wenn der MAX-Grenzwert überschritten wurde, andernfalls gibt die APU1 eine logische „0“ aus. Bei der VU1 handelt es sich in diesem Fall um eine 1-von-1-Auswahl, d. h. sobald eine logische „1“ am Eingang der VU1 ansteht, soll diese im fehlerfreien Betrieb selbst eine logische „1“ ausgeben und damit die entsprechenden Maßnahmen auslösen (hier beispielsweise einen Motor „M“ starten). Die ausgelösten Maßnahmen sollen in diesem einfachen Beispiel bei Anforderung ebenfalls stets fehlerfrei funktionieren, dasselbe gilt für die gesamte Kommunikation zwischen den Komponenten.

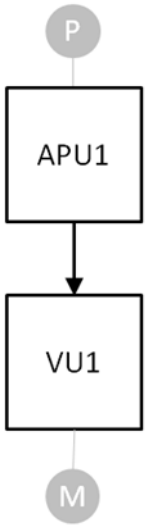

Abb. 4.1 Das Modellsystem A110

Als mögliche Ausfallarten sollen vorerst nur nichtselbstmeldende Fehler (NSF) betrachtet werden. Das bedeutet, dass beide Komponenten jeweils nur im bestimmungsgemäßen Zustand („OK“) oder nichtselbstmeldend ausgefallen („NSF“) sein können. In diesem Sinne beschreibt die folgende Tabelle alle denkbaren Zustände des Modellsystems A110. Die letzte Spalte gibt an, ob das Modellsystem aufgrund der jeweiligen Ausfallkombination als ausgefallen gilt (und damit unverfügbar ist) oder nicht.

Tab. 4.1 Übersicht der möglichen Gesamtzustände des Modellsystems A110

lfd. Nummer	APU1	VU1	Gesamtausfall
1	OK	OK	nein
2	NSF	OK	ja
3	OK	NSF	ja
4	NSF	NSF	ja

Tests und Reparaturen der Komponenten sollen für das Modellsystem A110 ebenfalls ausgeschlossen sein, d. h. ein einmal aufgetretener Fehler in einer Komponente bleibt dauerhaft bestehen und stellt somit einen absorbierenden Zustand dar.

Für die Beschreibung von Systemen mit Markov-Prozessen muss zunächst der sogenannte Zustandsraum bestimmt werden. Jedes Element des Zustandsraums steht dabei für einen Zustand des Gesamtsystems. So ist beispielsweise der Zustand „APU 1 nichtselbstmeldend ausgefallen und VU1 OK“ ein Element des Zustandsraums des Modellsystems A110. Dieses Element entspricht der Zeile mit der lfd. Nummer 2 in Tab. 4.1. In diesem Sinne entsprechen die vier Zeilen in Tab. 4.1 also den vier Zuständen des Zustandsraums des Modellsystems A110. Im nachfolgenden Text werden die einzelnen Zustände wie folgt dargestellt:

- (APU1 NSF; VU1 OK)
- „APU1 ist nichtselbstmeldend ausgefallen und VU1 ist OK“

In den nachfolgenden Abbildungen werden diese Zustände immer als Kasten dargestellt (siehe z. B. Abb. 4.2).

Als nächster Schritt werden die möglichen Übergänge zwischen den Zuständen des Zustandsraumes bestimmt. Dabei ist zu berücksichtigen, dass man nicht von jedem beliebigen Zustand in jeden anderen Zustand gelangen kann, insbesondere da die Fehlerzustände der einzelnen Komponenten APU1 und VU1 in dieser Betrachtung absorbierend sind. Dies folgt aus der Annahme, dass Reparaturen oder „Selbstheilungen“ von Komponenten ausgeschlossen sein sollen. Daher ist beispielsweise ein Übergang aus dem Zustand (APU1 NSF; VU1 OK) in den Zustand (APU1 OK; VU1 NSF) nicht möglich, da bei diesem Übergang die defekte APU1 wieder funktionieren müsste, was ohne Reparatur nicht möglich ist.

Unter einem defekten Zustand soll hier ein Zustand des Zustandsraums verstanden werden, in dem das Modellsystem nicht mehr verfügbar ist. Der Begriff „defekter Zustand“ ist daher streng vom Begriff „defekte Komponente“ zu trennen. So besteht der defekte Zustand (APU1 OK; VU1 NSF) beispielsweise aus einer defekten und einer fehlerfreien Komponente. Insgesamt ist das Modellsystem A110 in diesem Zustand allerdings nicht verfügbar, so dass die durch das System zu veranlassenden Maßnahmen nicht ausgelöst werden.

Insgesamt ergibt sich für den Zustandsraum des Modellsystems A110 inklusive aller erlaubten Übergänge der in Abb. 4.2 dargestellte Übergangsgraph.

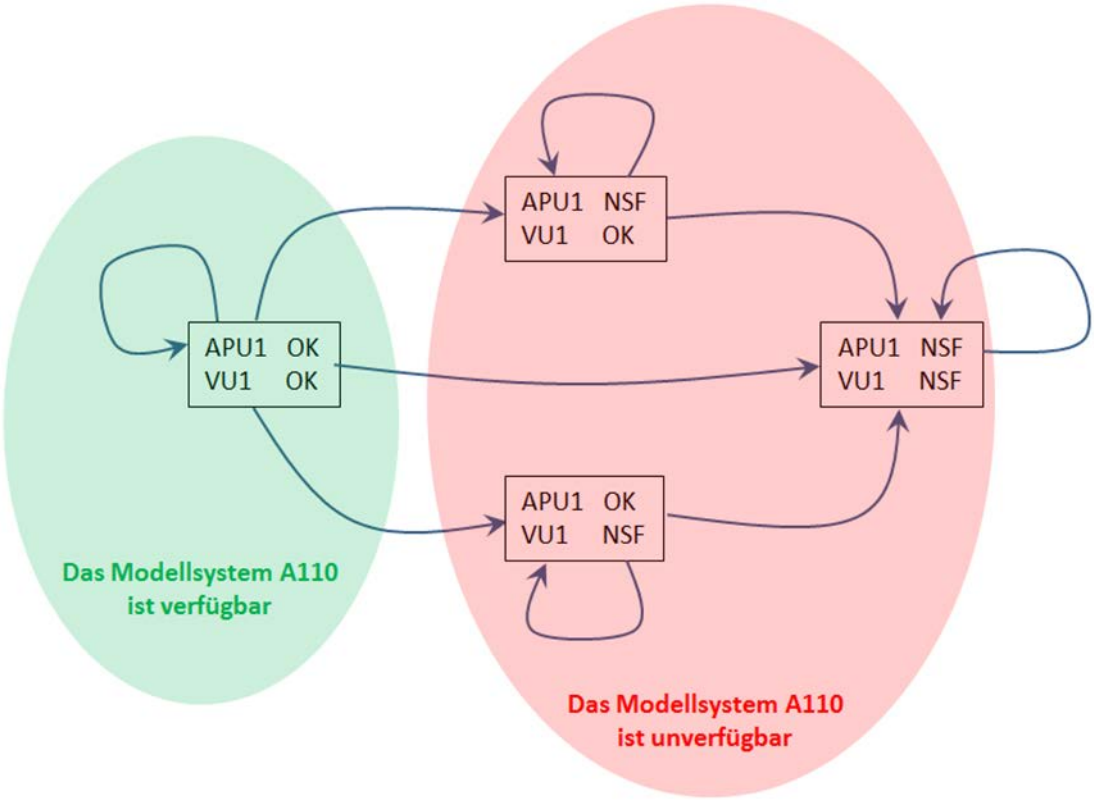

Abb. 4.2 Zustandsraum inklusive aller erlaubten Übergänge (Übergangsgraph) für das Modellsystem A110

Im linken, grün hinterlegten Zustand ist das Modellsystem A110 verfügbar, in den rechten drei Zuständen (rotes Feld) ist es hingegen unverfügbar.

Als nächstes müssen die Übergangswahrscheinlichkeiten für die in Abb. 4.2 dargestellten Übergänge berechnet werden. Ausgangspunkte für deren Berechnung sind in Anlehnung an die späteren Analysen die Ausfallraten der Komponenten. Im günstigsten Fall können die Ausfallraten von Komponenten aus der Betriebserfahrung geschätzt werden. Die dazu verwendeten Daten sind die Anzahl der Ausfälle, die in der Betriebszeit der jeweiligen Komponente beobachtet wurden. Für das Modell werden zu Demonstrationszwecken die Ausfallraten der Einfachheit halber wie folgt willkürlich festgelegt:

- Ausfallrate APU1 = 2 Ausfälle pro 50 h = $4 \cdot 10^{-2}$ h^{-1}
- Ausfallrate VU1 = 1 Ausfall pro 50 h = $2 \cdot 10^{-2}$ h^{-1}

Für die Berechnung der Ausfallwahrscheinlichkeit einer einzelnen Komponente muss bei gegebener Ausfallrate auch die Betrachtungszeit (Zeitdauer) angegeben werden,

innerhalb der die Zustandswahrscheinlichkeit der Komponente bestimmt werden soll. Da die Ausfallraten als Parameter der Exponentialverteilung zur Berechnung der Ausfallwahrscheinlichkeiten verwendet werden, gilt für die Berechnung der Ausfallwahrscheinlichkeit einer Komponente /NRC 81/:

$$P = 1 - e^{-\lambda t} \tag{4.3}$$

Dabei sind: *t* - Zeitdauer (in h)

P - Ausfallwahrscheinlichkeit (nach der Zeitdauer *t*)

λ - Ausfallrate (in h^{-1})

Für $\lambda \cdot t < 0{,}1$ kann für die Berechnung der Ausfallwahrscheinlichkeit folgende Näherung verwendet werden:

$$P = 1 - e^{-\lambda t} \approx \lambda t \tag{4.4}$$

Beispielsweise beträgt für die APU1 demnach die Ausfallrate $\lambda = 4 \cdot 10^{-2}\ h^{-1}$. Berechnet man die Ausfallwahrscheinlichkeiten für Zeitintervalle von einer, zwei und drei Stunden, so ergibt sich gemäß der Näherungsformel:

$$P_{APU1.NSF}(t = 1\ h) \approx 4 \cdot 10^{-2} \frac{1}{h} \cdot 1\ h = \ 4 \cdot 10^{-2} \tag{4.5}$$

$$P_{APU1.NSF}(t = 2\ h) \approx 4 \cdot 10^{-2} \frac{1}{\mathrm{h}} \cdot 2\ \mathrm{h} = \ 8 \cdot 10^{-2} \tag{4.6}$$

$$P_{APU1.NSF}(t = 3\ h) \approx 4 \cdot 10^{-2} \frac{1}{\mathrm{h}} \cdot 3\ \mathrm{h} = \ 1{,}2 \cdot 10^{-1} \tag{4.7}$$

Die exakt berechneten Werte (ohne Näherung) ergeben sich zu 0.039, 0.077 und 0.113. Während die Näherungen nach einer und zwei Stunden den gerundeten Werten

der exakten Berechnungen entsprechen, weist die Näherung nach drei Stunden eine etwas größere Abweichung vom exakten Wert auf. In diesem Fall wäre die Näherung auch nicht mehr angemessen, da die Bedingung $\lambda \cdot t < 0{,}1$ für $\lambda = 0{,}04$ und $t = 3$ nicht mehr erfüllt ist.

An dieser Stelle wird festgelegt, dass die nachfolgend berechneten Wahrscheinlichkeiten für den Zustandsraum jeweils stundenweise berechnet werden sollen. D. h. zwischen zwei aufeinanderfolgenden Berechnungen soll jeweils genau eine Stunde vergangen sein. Diese Festlegung hat keinen Einfluss auf die berechneten Ergebnisse und legt lediglich den Detaillierungsgrad der berechneten zeitlichen Entwicklung der Ergebnisse fest.

Für die beiden Basis-Ereignisse (APU1.NSF) bzw. (VU1.NSF) berechnen sich die Ausfallwahrscheinlichkeiten mit der exakten Formel von oben zu:

$$P_{APU1.NSF}(t = 1\,h) = 1 - e^{-4 \cdot 10^{-2} \frac{1}{h} \cdot 1\,h} \approx 0{,}039211 \tag{4.8}$$

$$P_{VU1.NSF}(t = 1\,h) = 1 - e^{-2 \cdot 10^{-2} \frac{1}{h} \cdot 1\,h} \approx 0{,}019801 \tag{4.9}$$

Möchte man hingegen die Wahrscheinlichkeit berechnen, dass ein bestimmtes Basis-Ereignis gerade nicht eintritt, so lässt sich dies ebenfalls sehr einfach berechnen (die Striche über den Ereignisnamen bedeuten eine Verneinung, d. h. das Komplement des Ereignisses):

$$P_{\overline{APU1.NSF}} = 1 - P_{APU1.NSF} = e^{-4 \cdot 10^{-2} \frac{1}{h} \cdot 1\,h} \approx 0{,}960790 \tag{4.10}$$

$$P_{\overline{VU1.NSF}} = 1 - P_{VU1.NSF} = e^{-2 \cdot 10^{-2} \frac{1}{h} \cdot 1\,h} \approx 0{,}980199 \tag{4.11}$$

Im Folgenden wird wie hier zugunsten der Lesbarkeit häufig auf die explizite Angabe von $t = 1$ h verzichtet, diese Festlegung bleibt aber durchgängig gültig.

Da im vereinfachten Modell A110 die einzelnen Komponenten nur zwei Zustände annehmen können („OK“ bzw. „NSF“), kann statt wie oben besser geschrieben werden:

$$P_{APU1.OK} = P_{\overline{APU1.NSF}} \tag{4.12}$$

$$P_{VU1.OK} = P_{\overline{VU1.NSF}} \tag{4.13}$$

Mit den in Gleichungen (4.10) und (4.11) berechneten Wahrscheinlichkeiten können die Übergangswahrscheinlichkeiten im Übergangsgraphen des Modells A110 berechnet werden:

- (APU1 OK; VU1 OK) → (APU1 NSF; VU1 OK)

Die Wahrscheinlichkeit für diesen Übergang im Zustandsraum ergibt sich aus der Wahrscheinlichkeit $P_{APU1.NSF}$ des Ereignisses, dass die APU1 nichtselbstmeldend ausfällt, und der Wahrscheinlichkeit $P_{VU1.OK}$ des Ereignisses, dass die VU1 keinen Ausfall erleidet:

$$P_1 = P_{APU1.NSF}\, P_{VU1.OK} \sim 0{,}039211 \cdot 0{,}980199 \sim 0{,}038435 \tag{4.14}$$

- (APU1 OK; VU1 OK) → (APU1 OK; VU1 NSF)

Die Wahrscheinlichkeit für diesen Übergang im Zustandsraum folgt aus der Wahrscheinlichkeit $P_{APU1.OK}$ des Ereignisses, dass die APU1 keinen Ausfall erleidet, und der Wahrscheinlichkeit $P_{VU1.NSF}$ des Ereignisses, dass die VU1 nichtselbstmeldend ausfällt:

$$P_1 = P_{APU1.OK} \cdot P_{VU1.NSF} \sim 0{,}960790 \cdot 0{,}019801 \sim 0{,}019025 \tag{4.15}$$

- (APU1 NSF; VU1 OK) → (APU1 NSF; VU1 NSF)

Die Wahrscheinlichkeit für diesen Übergang im Zustandsraum folgt unmittelbar aus der Wahrscheinlichkeit $P_{VU1.NSF}$ des Basis-Ereignisses, da die APU1 im Ausgangszustand bereits nichtselbstmeldend ausgefallen ist und sich im absorbierenden Zustand befindet, da keine Reparaturen vorgesehen sind:

$$P_3 = P_{VU1.NSF} \sim 0{,}019801 \tag{4.16}$$

- (APU1 OK; VU1 NSF) → (APU1 NSF; VU1 NSF)

Die Wahrscheinlichkeit für diesen Übergang im Zustandsraum folgt unmittelbar aus der Wahrscheinlichkeit $P_{APU1.NSF}$ des Basis-Ereignisses, da die VU1 im Ausgangszustand bereits nichtselbstmeldend ausgefallen ist und sich im absorbierenden Zustand befindet:

$$P_4 = P_{VU1.NSF} \sim 0{,}039211 \qquad (4.17)$$

- (APU1 OK; VU1 OK) → (APU1 NSF; VU1 NSF)

Dieser Übergang setzt sich aus den zwei Ereignissen zusammen, dass sowohl APU1 als auch VU1 im betrachteten Zeitintervall (eine Stunde) einen Ausfall erleiden. Die Wahrscheinlichkeit hierfür lässt sich aus den Basis-Ereignissen durch Multiplikation berechnen:

$$P_5 = P_{APU1.NSF}\ P_{VU1.NSF} = 0{,}039211 \cdot 0{,}019801 = 0{,}000776 \qquad (4.18)$$

Zeichnet man die so ermittelten Werte in Abb. 4.2 ein, so erhält man Abb. 4.3.

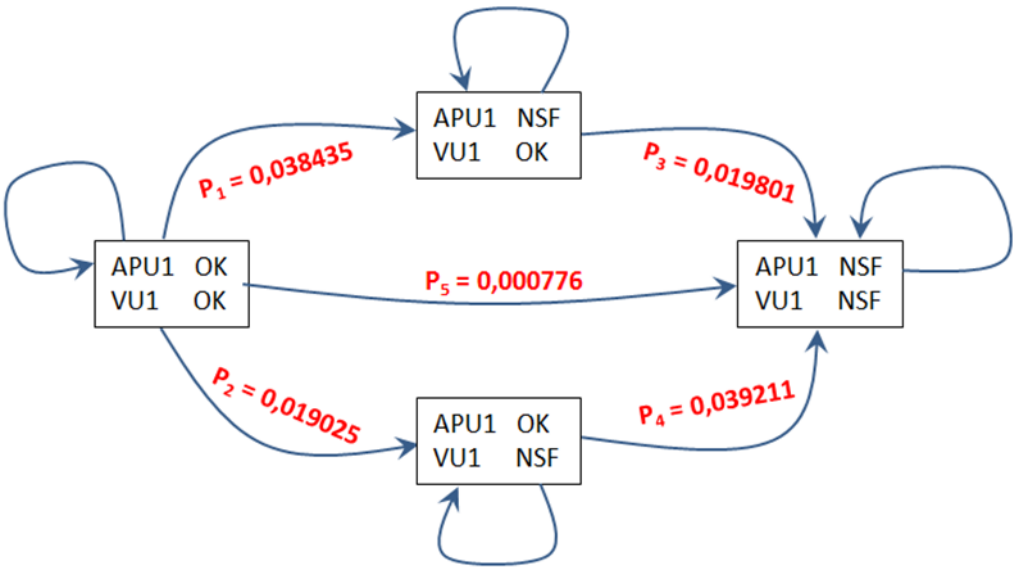

Abb. 4.3 Zustandsraum des Modells A110 mit den berechneten Übergangswahrscheinlichkeiten für Übergänge zwischen verschiedenen Zuständen (Übergangsgraph)

Die in Abb. 4.3 noch fehlenden Übergangswahrscheinlichkeiten lassen sich jetzt sehr einfach berechnen, wenn man Folgendes berücksichtigt:

Die Summe der Übergangswahrscheinlichkeiten aller von einem Zustand *ausgehenden* Pfeile muss 1 ergeben. Dies sagt nichts anderes aus, als das die Summe der Wahrscheinlichkeiten in andere Zustände zu wechseln ODER im selben Zustand zu verharren genau 1 ergeben muss. Das kann man gut repräsentativ am Zustand (APU1 OK; VU1 OK) verdeutlichen:

(APU1 OK; VU1 OK) geht mit der Wahrscheinlichkeit $P_1 = 0{,}038435$ in den Zustand (APU1 NSF; VU1 OK), mit $P_5 = 0{,}000776$ in den Zustand (APU1 NSF; VU1 NSF) und mit $P_2 = 0{,}019025$ in den Zustand (APU1 OK; VU1 NSF) über. Insgesamt geht der fehlerfreie Zustand also mit der Wahrscheinlichkeit

$$P_1 + P_5 + P_2 = 0{,}058236 \tag{4.19}$$

in einen der drei anderen Zustände über. Der zum Wert 1 fehlende Rest stellt die Wahrscheinlichkeit dar, dass der Zustand sich nicht ändert und berechnet sich daher gemäß

$$1 - (P_1 + P_5 + P_2) = 0{,}941764 \tag{4.20}$$

Führt man analog auch die Berechnungen für die verbleibenden drei Übergänge durch, so ergibt sich insgesamt der vollständige Übergangsgraph inklusive aller Übergangswahrscheinlichkeiten für das Modellsystem A110 in Abb. 4.4.

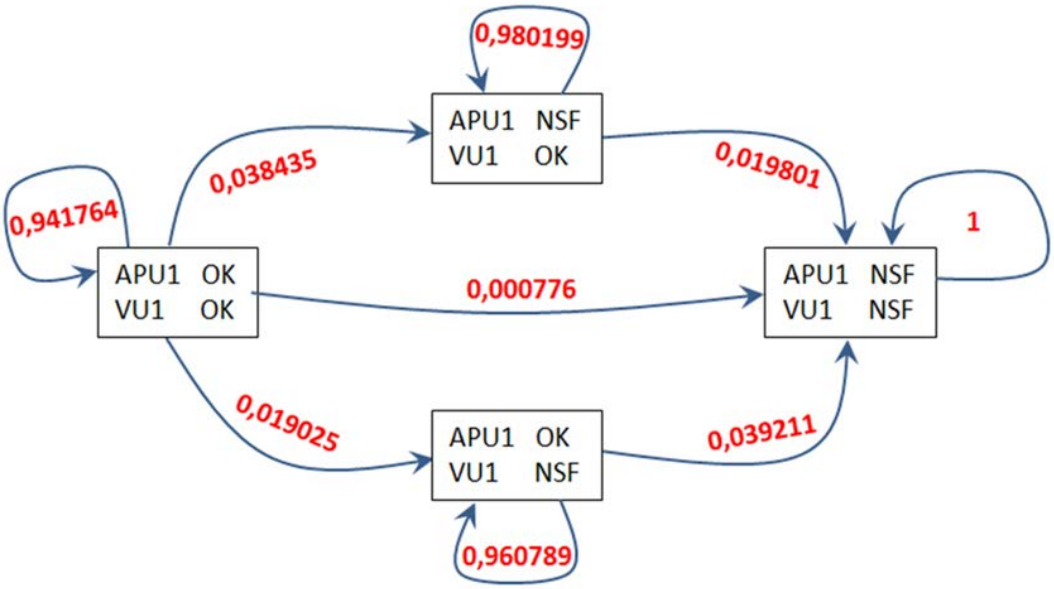

Abb. 4.4 Übergangsgraph des Modells A110 inklusive aller Übergangswahrscheinlichkeiten (für jeweils eine Stunde)

Die nächsten Überlegungen sollen die Entwicklung der Zustandswahrscheinlichkeiten über die Zeit ermitteln. Als Startpunkt wird festgelegt, dass zum Zeitpunkt t = 0 h das System fehlerfrei sei. Das bedeutet, dass die Wahrscheinlichkeit dafür, dass sich das System zu diesem Zeitpunkt im Zustand (APU1 OK; VU1 OK) befindet, den Wert 1 hat. Alle anderen Zustände haben die Wahrscheinlichkeit 0 (vgl. Abb. 4.5). Die grün gekennzeichneten Werte bezeichnen im Folgenden die Zustandswahrscheinlichkeiten des Systems und die rot gekennzeichneten Werte die Übergangswahrscheinlichkeiten zwischen den Zuständen.

Oder anders ausgedrückt: Der Vektor der Zustandswahrscheinlichkeiten zum Zeitpunkt t = 0 h ist gegeben durch

$$P(t=0) = \begin{pmatrix} P(APU1\ OK, VU1\ OK) \\ P(APU1\ NSF, VU1\ OK) \\ P(APU\ 1\ OK, VU1\ NSF) \\ P(APU1\ NSF, VU1\ NSF) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{4.21}$$

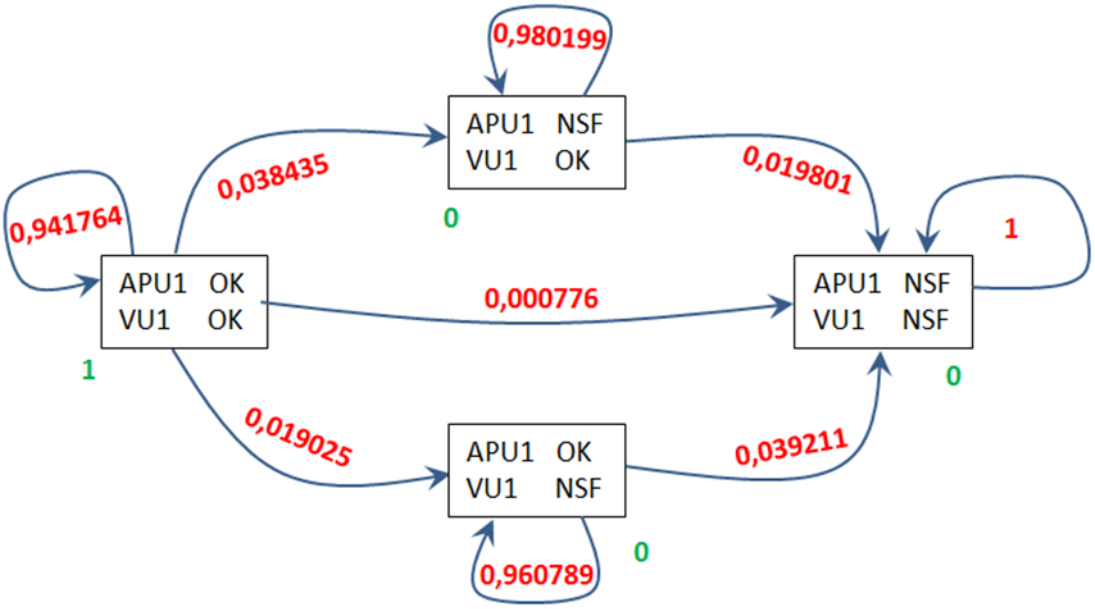

Abb. 4.5 Der Zustandsraum des Modells A110 zum Zeitpunkt $t = 0$ h als Übergangsgraph

Die grünen Zahlen sind die Wahrscheinlichkeiten, dass sich das System zum Zeitpunkt t in diesem Zustand befindet

Ausgehend vom Übergangsgraphen in Abb. 4.5 und dem Vektor $P(t = 0)$ der Zustandswahrscheinlichkeiten zum Zeitpunkt $t = 0$ h wird jetzt die zeitliche Entwicklung für eine Stunde berechnet, um den Zustandsraum zum Zeitpunkt $t = 1$ h zu bestimmen. Hierfür betrachtet man nacheinander jeden Zustand des Zustandsraumes einzeln.

Die Wahrscheinlichkeit, dass sich das System nach einer Stunde in einem bestimmten Zustand befindet, ist durch die Summe aller Übergangswahrscheinlichkeiten *eingehender* Pfeile multipliziert mit der jeweiligen Zustandswahrscheinlichkeit (im Folgenden grün dargestellt) gegeben.

Dieser Zusammenhang wird am besten durch die Berechnungen für alle einzelnen Zustände des Zustandsraums des Systems A110 für $t = 1$ h verdeutlicht:

- (APU1 OK; VU1 OK)

Es gibt nur einen einzigen eingehenden Pfeil (der in diesem Zustand endet). Die Übergangswahrscheinlichkeit für diesen Übergang beträgt 0,941764 (siehe Abb. 4.5). Ausgangspunkt des Pfeils ist der Zustand (APU 1 OK; VU1 OK) selbst. Die Wahrschein-

lichkeit, dass sich das System zuvor (t = 0 h) in diesem Zustand befand, beträgt 1 (siehe Abb. 4.5). Demnach berechnet sich die Wahrscheinlichkeit, dass sich das System nach 1 h im Zustand (APU1 OK; VU1 OK) befindet zu:

$$P_{(APU1\ OK;\ VU1\ OK)}(t = 1\ \text{h}) = 1 \cdot 0{,}941764 = \underline{0{,}941764} \qquad (4.22)$$

- (APU1 NSF; VU1 OK)

Für diesen Zustand gibt es zwei eingehende Pfeile:

Der erste Pfeil kommt vom fehlerfreien Zustand (APU1 OK; VU1 OK), die entsprechende Übergangswahrscheinlichkeit beträgt 0,038435. Die Wahrscheinlichkeit, dass sich das System zum Zeitpunkt t = 0 h im Ausgangszustand des Pfeils befand, beträgt 1.

Der zweite eingehende Pfeil startet am Zustand (APU1 NSF; VU1 OK) selbst und die zugehörige Übergangswahrscheinlichkeit beträgt 0,980199 (Abb. 4.5). Die Wahrscheinlichkeit, dass sich das System zum Zeitpunkt t = 0 h gerade in diesem Zustand befand, beträgt 0.

Insgesamt berechnet sich daher die Wahrscheinlichkeit, dass sich das System nach einer Stunde im Zustand (APU1 NSF; VU1 OK) befindet, zu

$$P_{(APU1\ NSF;\ VU1\ OK)}(t = 1\ \text{h}) = 1 \cdot 0{,}038435 + 0 \cdot 0{,}980199 = \underline{0{,}038435} \qquad (4.23)$$

- (APU1 OK; VU1 NSF)

Analog berechnet sich die Wahrscheinlichkeit, sich zum Zeitpunkt t = 1 h in diesem Zustand zu befinden, nach Gleichung (4.24):

$$P_{(APU1\ OK;VU1\ NSF)}(t = 1\ \text{h}) = 1 \cdot 0{,}019025 + 0 \cdot 0{,}960789 = \underline{0{,}019025} \qquad (4.24)$$

- (APU1 NSF; VU1 NSF)

Die Wahrscheinlichkeit, sich zum Zeitpunkt t = 1 h im Zustand (APU1 NSF; VU1 NSF) zu befinden, ergibt sich aus Gleichung (4.25):

$$P_{(APU1\ NSF;\ VU1\ NSF)}\ (t = 1\ \text{h}) = 0 \cdot 0{,}019801 + 1 \cdot 0{,}000776 + 0 \cdot 0{,}039211 + 0 \cdot 1 = \underline{0{,}000776} \tag{4.25}$$

Somit sind jetzt die Wahrscheinlichkeiten für alle Zustände zum Zeitpunkt $t = 1$ h bekannt. Entsprechen ergibt sich der Vektor der Zustandswahrscheinlichkeiten zum Zeitpunkt $t = 1$ h zu

$$P(t = 1) \approx \begin{pmatrix} 0{,}941764 \\ 0{,}038435 \\ 0{,}019025 \\ 0{,}000776 \end{pmatrix}. \tag{4.26}$$

Trägt man diese in den Zustandsraum in Abb. 4.5 anstatt der Werte für $t = 0$ h ein, so erhält man Abb. 4.6.

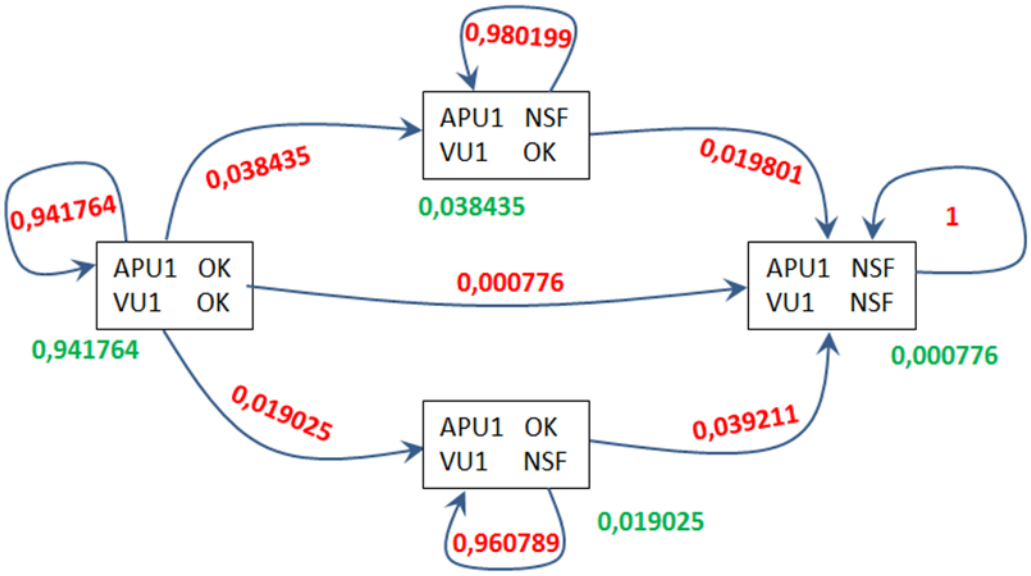

Abb. 4.6 Zustandsraum des Modellsystems A110 zum Zeitpunkt $t = 1$ h als Übergangsgraph

Dieselben Überlegungen wie für den Zeitpunkt $t = 1$ h gelten genauso auch für den nächsten Zeitpunkt ($t = 2$ h). Da erneut eine Stunde vergeht, verändern sich die Zu-

standswahrscheinlichkeiten des Systems (grüne Zahlen). Die Übergangswahrscheinlichkeiten (rote Zahlen in Abb. 4.5 und Abb. 4.6) bleiben konstant.

Für t = 2 h ergibt sich:

- (APU1 OK; VU1 OK)

$$P_{(APU1\ OK;\ VU1\ OK)}(t = 2\ \text{h}) = 0{,}941764 \cdot 0{,}941764 = \underline{0{,}886919} \tag{4.27}$$

- (APU1 NSF; VU1 OK)

$$P_{(APU1\ NSF;\ VU1\ OK)}(t = 1\ \text{h}) = 0{,}941764 \cdot 0{,}038435 + 0{,}038435 \cdot 0{,}980199 = \underline{0{,}073871} \tag{4.28}$$

- (APU1 OK; VU1 NSF)

$$P_{(APU1\ NSF;\ VU1\ OK)}(t = 1\ \text{h}) = 0{,}941764 \cdot 0{,}019025 + 0{,}019025 \cdot 0{,}960789 = \underline{0{,}036196} \tag{4.29}$$

- (APU1 NSF; VU1 NSF)

$$\begin{aligned} P_{(APU1\ NSF;\ VU1\ NSF)}(t = 1\text{h}) = {} & 0{,}038435 \cdot 0{,}019801 \\ & + 0{,}941764 \cdot 0{,}000776 \\ & + 0{,}019025 \cdot 0{,}039211 + 0 \cdot 1 \\ & = 0{,}003014 \end{aligned} \tag{4.30}$$

Der Vektor der Zustandswahrscheinlichkeiten zum Zeitpunkt t = 2 h sieht also wie folgt aus:

$$P(t = 2) \approx \begin{pmatrix} 0{,}886919 \\ 0{,}073871 \\ 0{,}036196 \\ 0{,}003014 \end{pmatrix}. \tag{4.31}$$

Das Rechenschema lässt sich jetzt für jede weitere volle Stunde wiederholen, wodurch die zeitliche Entwicklung des Modellsystems vollständig beschrieben werden kann. Tab. 4.2 zeigt die Ergebnisse für die Zustandswahrscheinlichkeiten des Modells A110 für die ersten 20 Stunden.

Die Spalte „System verfügbar“ entspricht der Spalte (APU1 OK; VU1 OK), allerdings wurden die Werte auf vier Dezimalen gerundet. In allen anderen Fällen ist das System unverfügbar. In der entsprechenden Spalte („System unverfügbar“) sind die Wahrscheinlichkeiten der defekten Zustände daher aufaddiert. Die letzte Spalte summiert die Wahrscheinlichkeiten für die einzelnen Zustände auf und muss 1 ergeben, da sich das System mit Wahrscheinlichkeit 1 in irgendeinem der Zustände befinden muss. Abb. 4.7 stellt den zeitlichen Verlauf der Systemverfügbarkeit und -unverfügbarkeit graphisch dar.

Tab. 4.2 Die Wahrscheinlichkeiten für Verfügbarkeit und Nichtverfügbarkeit des Modellsystems A110 in den ersten 20 Stunden

t in h	(APU 1 OK; VU1 OK)	(APU 1 NSF; VU1 OK)	(APU 1 OK; VU1 NSF)	(APU 1 NSF; VU1 NSF)	System verfügbar	System unverfügbar	Summe
0	1	0	0	0	1	0	1
1	0,941764	0,038435	0,019025	0,000776	0,9418	0,0582	1
2	0,886919432	0,073870648	0,036196071	0,00301385	0,8869	0,1131	1
3	0,835268792	0,106496684	0,051650429	0,006584096	0,8353	0,1647	1
4	0,786626078	0,136491499	0,065516153	0,01136627	0,7866	0,2134	1
5	0,740816122	0,164022804	0,07791276	0,017248314	0,7408	0,2592	1
6	0,697673954	0,189248256	0,088951749	0,02412604	0,6977	0,3023	1
7	0,657044214	0,21231605	0,098737109	0,031902627	0,657	0,343	1
8	0,618780587	0,233365474	0,107365795	0,040488144	0,6188	0,3812	1
9	0,582745281	0,252527436	0,114928175	0,049799108	0,5827	0,4173	1
10	0,548808527	0,269924955	0,121508456	0,059758063	0,5488	0,4512	1
11	0,516848113	0,285673627	0,12718507	0,07029319	0,5168	0,4832	1
12	0,486748947	0,299882061	0,132031051	0,081337942	0,4867	0,5133	1
13	0,458402635	0,312652292	0,13611438	0,092830693	0,4584	0,5416	1
14	0,431707099	0,324080169	0,13949831	0,104714422	0,4317	0,5683	1
15	0,406566204	0,33425572	0,142241669	0,116936407	0,4066	0,5934	1
16	0,382889415	0,343263494	0,144399153	0,129447938	0,3829	0,6171	1
17	0,360591467	0,351182889	0,146021589	0,142204056	0,3606	0,6394	1
18	0,339592062	0,358088449	0,147156189	0,155163299	0,3396	0,6604	1
19	0,319815579	0,364050161	0,147846787	0,168287474	0,3198	0,6802	1
20	0,301190799	0,369133715	0,148134058	0,181541428	0,3012	0,6988	1

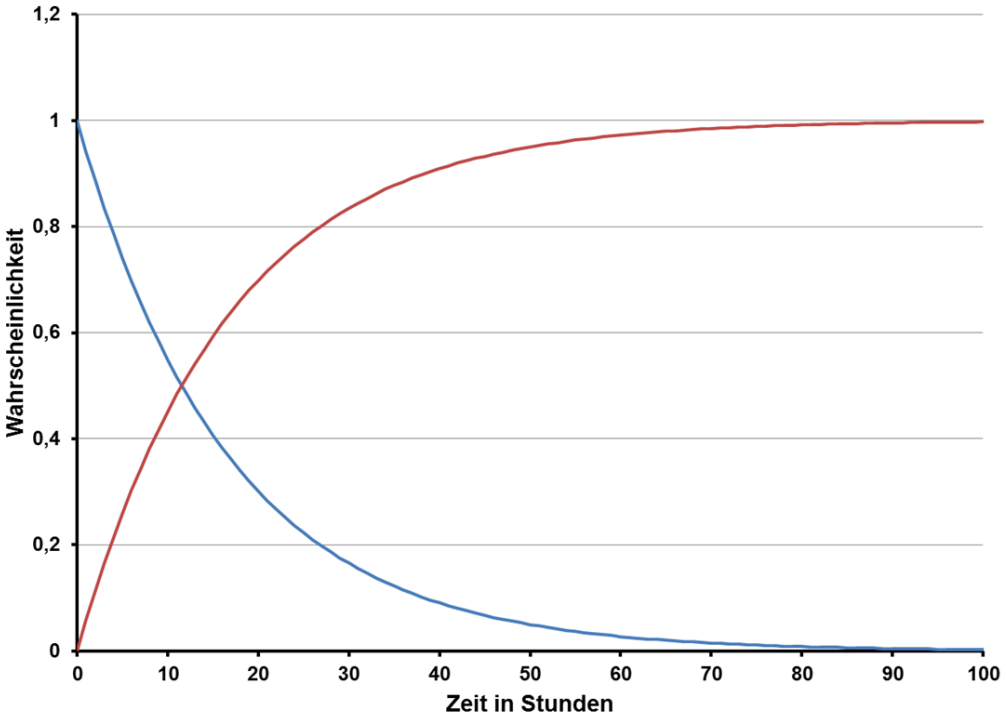

Abb. 4.7 Berechnete Verfügbarkeit (blau) und Unverfügbarkeit (rot) des Modellsystems A110 während der ersten 100 Stunden

4.2 Matrix-Schreibweise

Oben wurde bereits der Vektor $\overrightarrow{P(t)}$ der Zustandswahrscheinlichkeiten eingeführt, bisher aber noch nicht weiterverwendet. Der Vorteil dieser Schreibweise soll hier näher erläutert werden.

Die Zustandswahrscheinlichkeiten als Vektor zu schreiben, erlaubt es, den Übergangsgraphen durch die Übergangsmatrix *M* darzustellen und so die durchzuführenden Rechenoperationen sehr übersichtlich aufzuschreiben. Hierbei hat $\overrightarrow{P(t)}$ die Dimension *m* des Zustandsraums und die quadratische Übergangsmatrix *M* mit den Komponenten M_{ij} die Größe *m x m*. Die Komponenten M_{ij} selbst stellen die Übergangswahrscheinlichkeiten dar, um jeweils vom Zustand *j* in den Zustand *i* zu gelangen. Dann können die Rechenoperationen des Markov-Prozesses für einen Zeitschritt (t = 1 h) als Matrix-Vektor-Produkt dargestellt werden:

$$\vec{P}(t+1) = M \cdot \vec{P}(t) \tag{4.32}$$

bzw. für die Komponenten

$$P_i(t+1) = \sum_{j=1}^{m} M_{ij} \cdot P_j(t) \tag{4.33}$$

Dies soll durch folgendes Beispiel verdeutlicht werden. Für das Modellsystem A110 lautet die Übergangsmatrix

$$M = \begin{pmatrix} 0{,}941764 & 0 & 0 & 0 \\ 0{,}038435 & 0{,}980199 & 0 & 0 \\ 0{,}019025 & 0 & 0{,}960789 & 0 \\ 0{,}000776 & 0{,}019801 & 0{,}039211 & 1 \end{pmatrix} \tag{4.34}$$

und der Vektor P der Zustandswahrscheinlichkeiten lautet zum Zeitpunkt *t* = 0 h

$$P(t=0) = \begin{pmatrix} P_{(APU1.OK;VU1.OK)}(0) \\ P_{(APU1.NSF;VU1.OK)}(0) \\ P_{(APU1.OK;VU1.NSF)}(0) \\ P_{(APU1.NSF;VU1.NSF)}(0) \end{pmatrix} = \begin{pmatrix} P_1(0) \\ P_2(0) \\ P_3(0) \\ P_4(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{4.35}$$

Damit berechnet sich z. B. die Wahrscheinlichkeit $P_{(APU1.NSF;VU1.OK)}(t = 1)$ nach oben zu:

$$\begin{aligned} P_{(APU1.NSF;VU1.OK)}(1) &= P_2(1) \\ &= \sum_{j=1}^{4} M_{2j} \cdot P_j(0) \\ &= 0{,}038435 \cdot 1 + 0{,}980199 \cdot 0 + 0 \cdot 0 + 0 \cdot 0 = 0{,}038435 \end{aligned} \tag{4.36}$$

Dies entspricht genau der Rechnung, die bereits im Abschnitt 4.1 für diesen Zeitpunkt und diesen Zustand berechnet wurde (siehe Rechnungen zur Abb. 4.6).

Die bisherige Beschreibung in der Matrixform enthält die Besonderheit, dass in der Matrix *M* die Übergangswahrscheinlichkeiten für die Zustände des Systems aufgeführt sind. In Abschnitt 4.1 wurde anschaulich beschrieben, wie die Übergangswahrscheinlichkeiten aus den gegebenen Übergangsraten für das sehr einfach gehaltene System berechnet werden. Bereits für etwas größere Systeme ist eine solche Art der Berech-

nung der Übergangswahrscheinlichkeiten, wie sie in Abschnitt 4.1 durchgeführt worden ist, nicht praktikabel, da die möglichen Kombinationen der Übergänge zu den jeweiligen Zuständen schnell sehr unübersichtlich werden.

In Abschnitt 4 wurde einleitend beschrieben, dass bei gegebenen Übergangsraten die Zustandswahrscheinlichkeiten eines Systems durch die Lösung eines Differentialgleichungssystems gemäß Gleichung (4.2) berechnet werden können. Im Folgenden soll beispielhaft gezeigt werden, wie die Berechnung des Beispielsystems A110 des Abschnitts 4.1 über ein Differentialgleichungssystem durchgeführt werden kann.

Die Ausfallrate von APU1 ist $\lambda_A = 4 \cdot 10^{-2}$, die Ausfallrate von VU1 ist $\lambda_B = 2 \cdot 10^{-2}$. Das Differentialgleichungssystem für das Beispiel A110 hat dann die Form:

$$\begin{pmatrix} dP_1(t)/dt \\ dP_2(t)/dt \\ dP_3(t)/dt \\ dP_4(t)/dt \end{pmatrix} = \begin{pmatrix} -(\lambda_A + \lambda_B) & 0 & 0 & 0 \\ \lambda_A & -\lambda_B & 0 & 0 \\ \lambda_B & 0 & -\lambda_A & 0 \\ 0 & \lambda_B & \lambda_A & 0 \end{pmatrix} \cdot \begin{pmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{pmatrix} \tag{4.37}$$

bzw. ausführlich geschrieben

$$\begin{aligned} dP_1(t)/dt &= -(\lambda_A + \lambda_B) \cdot P_1(t) \\ dP_2(t)/dt &= \lambda_A \cdot P_1(t) - \lambda_B \cdot P_2(t) \\ dP_3(t)/dt &= \lambda_B \cdot P_1(t) - \lambda_A \cdot P_3(t) \\ dP_4(t)/dt &= \lambda_B \cdot P_2(t) + \lambda_A \cdot P_3(t) \end{aligned} \tag{4.38}$$

In der ersten Spalte der Ratenmatrix in Gleichung (4.37) erfolgt der Übergang vom Zustand 1 (Spalte 1) in den Zustand 2 (Zeile 2) mit der Rate λ_A und der Übergang vom Zustand 1 (Spalte 1) in den Zustand 3 (Zeile 3) mit der Rate λ_B. Mit der Rate $-(\lambda_A + \lambda_B)$ verbleibt das System im Zustand 1.

Vom Zustand 2 (Spalte 2) kann nur der Zustand 4 (Zeile 4) erreicht werden, indem die Komponente VU1 ausfällt. Dies erfolgt mit der Rate λ_B. Analog kann der Übergang vom Zustand 3 (Spalte 3) nur in den Zustand 4 (Zeile 4) erfolgen, indem die Komponente APU1 ausfällt. Dies erfolgt mit der Rate λ_A.

In die Diagonalen der Ratenmatrix werden diejenigen Werte eingetragen, mit denen die Summe der aufgeführten Werte in jeder einzelnen Spalte den Wert 0 ergeben.

Als Lösung des Differentialgleichungssystems (4.37) erhält man die Zustandsgleichungen

$$
\begin{aligned}
P_1(t) &= exp(- (\lambda_A + \lambda_B) \cdot t) \\
P_2(t) &= exp(- \lambda_B \cdot t) \; - \; exp(- (\lambda_A + \lambda_B) \cdot t) \\
P_3(t) &= exp(- \lambda_A \cdot t) \; - \; exp(- (\lambda_A + \lambda_B) \cdot t) \\
P_4(t) &= 1 - (exp(- \lambda_A \cdot t) + exp(- \lambda_B \cdot t) - exp(- (\lambda_A + \lambda_B) \cdot t)
\end{aligned}
\qquad (4.39)
$$

Setzt man in die Gleichungen für $\lambda_A = 0{,}04$, für $\lambda_B = 0{,}02$ und für $t = 10$ h ein, so ergeben sich für die Zustandswahrscheinlichkeiten zum Zeitpunkt $t = 10$ h die Werte:

- P1(t) = 0,5488
- P2(t) = 0,2699
- P3(t) = 0,1215
- P4(t) = 0,0598

Diese Wahrscheinlichkeiten entsprechen genau den Werten, die in Tab. 4.2 für die jeweiligen Zustände für den Zeitpunkt $t = 10$ aufgeführt sind.

4.3 Variationsrechnungen für das Modellsystem A120 unter Verwendung des Programms RAMESU

Die Bestimmung aller Übergangsmöglichkeiten (Pfeile) und der zugehörigen Übergangswahrscheinlichkeiten des Modellsystems A120 (siehe Abb. 3.10) kann prinzipiell völlig analog zu den Beschreibungen in den vorangegangenen Abschnitten 4.1 bzw. 4.2 erfolgen. Abb. 4.7 in Abschnitt 4.1 stellt die Wahrscheinlichkeiten der Systemverfügbarkeit (blau) und Systemunverfügbarkeit (rot) für die ersten 100 Stunden dar.

Wie in Abb. 4.8 allerdings ersichtlich wird, ist der zu betrachtende Übergangsgraph für das Modellsystem A120 bereits relativ unübersichtlich. Dementsprechend wäre die manuelle Berechnung der Zustandswahrscheinlichkeiten über die Lösung des zugehörigen Differentialgleichungssystems und insbesondere die manuelle Berechnung, wie sie in Abschnitt 4.1 durchgeführt wurde, sehr aufwändig und fehleranfällig.

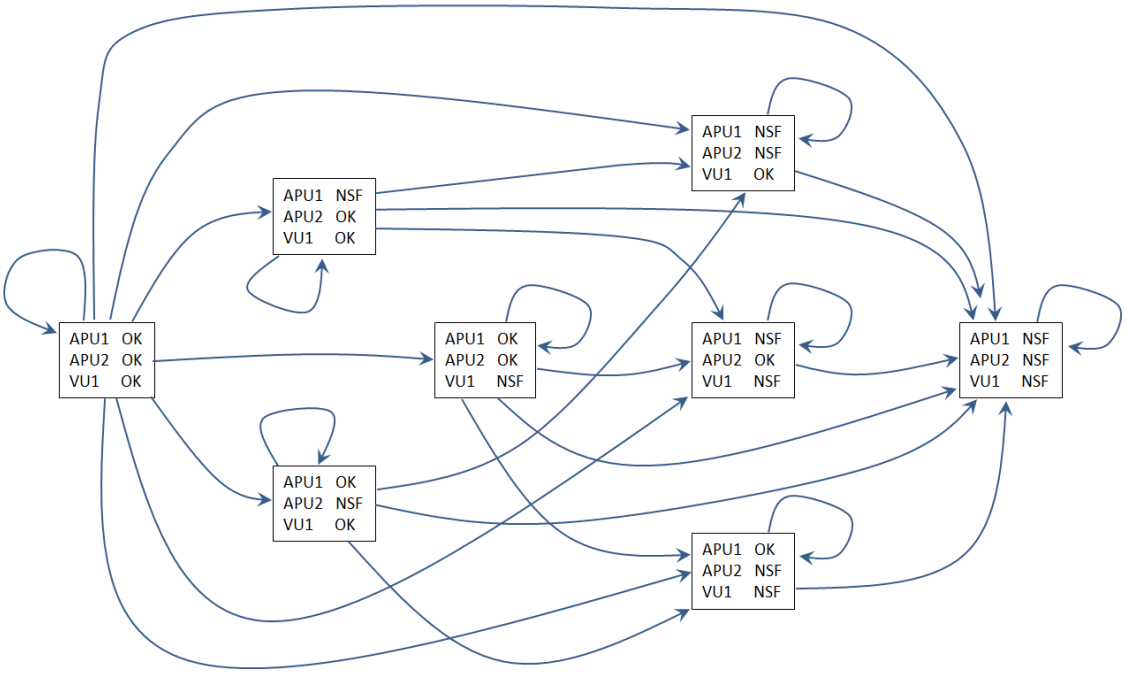

Abb. 4.8 Übergangsgraph des Modellsystems A120

Basierend auf dem Übergangsgraphen in Abb. 4.8 kann mittels einer Fehlerbaumanalyse (z. B. mittels des Programms „RiskSpectrum“) sukzessive die Wahrscheinlichkeit dafür berechnet werden, dass sich das System zu jeder vollen Stunde in einem der möglichen Zustände des Zustandsraums befindet (vergleiche Abschnitt 4.1).

Am Beispiel des Systems A120 soll im Folgenden gezeigt werden, in welcher Form unterschiedliche Systembeschreibungen mit dem Programm RAMESU modelliert und analysiert werden können. Unter den verschiedenen Systembeschreibungen, die im Folgenden diskutiert und berechnet werden, befinden sich auch Beschreibungen zum Systemverhalten, deren Modellierung sich über die Fehlerbaumanalyse schwierig gestaltet bzw. an ihre Grenzen gelangt und in der Form nicht möglich ist. Es soll an dieser Stelle darauf hingewiesen werden, dass die Diskussion nicht erschöpfend ist. Vielmehr sollen beispielhaft einige Situationen beschrieben werden, wann die Modellierung über einen Markov-Prozess Vorteile gegenüber der Fehlerbaumanalyse aufweist.

Da der Zustandsraum eines Systems mit wachsender Zahl an Komponenten exponentiell anwächst, können Markov-Prozesse von Systemen mit mehreren Komponenten nur noch äußerst mühsam – wenn überhaupt – manuell berechnet werden. Aufgrund der Unübersichtlichkeit erweist sich die manuelle Erstellung des Übergangsgraphen

sowie die Berechnung der entsprechenden Zustandswahrscheinlichkeiten außerdem als sehr fehleranfällig. Aus diesem Grund werden zur Berechnung von Markov-Modellen vorzugsweise entsprechende Computer-Programme eingesetzt.

In der GRS wird das Rechenprogramm RAMESU (**R**eliability **A**nalysis with **M**arkov-Models **E**xtended by **S**ensitivity- and **U**ncertainty-Analysis) eingesetzt, das in der GRS entwickelt wurde. Dieses Programm berechnet die Zuverlässigkeit eines technischen Systems durch einen Markov-Prozess. Es bietet zusätzliche Möglichkeiten an, zu gewissen diskreten Zeitpunkten Zustandsänderungen, die mit gewissen Wahrscheinlichkeiten auftreten, zu modellieren, wodurch das Spektrum der Modellierungsmöglichkeiten erheblich erweitert werden kann. Dies soll im Folgenden an einigen Beispielen demonstriert werden.

Beispiel 1

Im Beispiel 1 wird kurz beschrieben, mit welchen einfachen Anweisungen das Beispielsystem A120 über das Markov-Programm RAMESU modelliert werden kann und welche Ergebnisse das Programm liefert. Das zu modellierende System A120 wurde bereits zu Beginn des Abschnitts 3 ausführlich beschrieben (siehe Abb. 3.10). Die Ausfallraten der Komponenten sind in Tab. 3.4 angegeben.

Ein großer Vorteil ist, dass unter Verwendung des Programms RAMESU der Zustandsraum des Systems A120, der hier aus 8 Zuständen besteht (siehe Tab. 3.5 in Abschnitt 3.2.1), automatisch generiert wird. Die einzigen Anweisungen zur Beschreibung des Systems bestehen in der Definition

- aus welchen Komponenten das System besteht,
- welche Zustände die einzelnen Komponenten annehmen können,
- der Übergangsraten, mit denen die Komponenten in ihre definierten Zustände übergehen und
- welche Ausfälle der Komponenten einen Systemausfall verursachen.

Das System A120 kann durch folgende Anweisungen modelliert werden:

Definition der Komponenten:

1 : APU1
2 : APU2
3 : VU1

Definition der Komponentenzustände und der zugehörigen Übergangsraten

```
IF / APU1, 0  / THEN $ 4.0E-2    ! Wenn sich APU1 im Zustand 0 befindet, erfolgt der
   DO / APU1, 1 /                ! Übergang vom Zustand 0 in den Zustand 1 mit der Rate
ENDIF                            ! 4.E-02

IF / APU2, 0  / THEN $ 4.0E-2    ! Wenn sich APU2 im Zustand 0 befindet, erfolgt der
   DO / APU2, 1 /                ! Übergang vom Zustand 0 in den Zustand 1 mit der Rate
ENDIF                            ! 4.E-02

IF / VU1, 0  / THEN $ 2.0E-2     ! Wenn sich VU1 im Zustand 0 befindet, erfolgt der
   DO / VU1, 1  /                ! Übergang vom Zustand 0 in den Zustand 1 mit der Rate
ENDIF                            ! 2.E-02
```

Definition der Komponentenausfälle, die einen Systemausfall zur Folge haben

```
IF /  VU1,1  /  APU1,1  APU2,1  / THEN $ 2   ! Wenn VU1  oder gemeinsam APU1 und
ENDIF                                        ! APU2  ausgefallen sind, dann liegt ein
                                             ! Systemausfall vor
```

Mit diesen wenigen Anweisungen, die gemäß einer definierten einfachen Syntax erfolgen, generiert das Programm automatisch den dazugehörigen Zustandsraum und berechnet die dazugehörigen Zustandswahrscheinlichkeiten zu beliebigen Zeitpunkten. In diesem Beispiel wurde die Zeit so festgelegt, dass die Zustandswahrscheinlichkeiten in einem Zeitraum von 100 Stunden für jede Stunde berechnet und ausgegeben werden.

Der automatisch generierte Zustandsraum ist durch folgende 8 Zustände gegeben, die den Zuständen in Abb. 4.8 bzw. den Zuständen in Tab. 3.5 in Abschnitt 3.2.1 entsprechen:

Tab. 4.3 Die definierten Zustände der Komponenten

Zustand	APU1	APU2	VU1
L = 1:	**0**	**0**	**0**
L = 2:	**1**	**0**	**0**
L = 3:	**0**	**1**	**0**
L = 4:	**0**	**0**	**1**
L = 5:	**1**	**1**	**0**
L = 6:	**1**	**0**	**1**
L = 7:	**0**	**1**	**1**
L = 8:	**1**	**1**	**1**

Die definierten Zustände der Komponenten bedeuten hier:

0 – Komponente intakt und

1 – nicht selbstmeldender Fehler der Komponente.

Unter Verwendung des Programms RAMESU können nicht nur die zeitabhängigen Wahrscheinlichkeiten berechnet werden, mit denen sich das System im ausgefallenen oder im intakten Zustand befindet. Es können zusätzlich auch die Wahrscheinlichkeiten von Kombinationen verschiedener Zustände berechnet werden. Wie z. B. die Wahrscheinlichkeit, dass sich das System nur durch den Ausfall der VU im ausgefallenen Zustand befindet. Diese Wahrscheinlichkeit ergibt sich aus der Summe der Wahrscheinlichkeiten der Zustände 4, 6 und 7. D. h., bei dem Systemausfall, der nur durch die VU verursacht wird, werden diejenigen Zustände berücksichtigt, bei denen die VU1 ausgefallen und sich mindestens einer der beiden APUs im intakten Zustand befindet.

Analog kann die Wahrscheinlichkeit in Abhängigkeit der Zeit ermittelt werden, dass der Ausfall des Systems nur durch die AUs verursacht wird. Der Systemausfall, der durch die APUs versursacht wird, wird durch die Situation beschrieben, dass APU1 und APU2 ausgefallen sind, aber VU1 sich im intakten Zustand befindet. Diese Situation wird durch den Zustand L = 5 beschrieben.

Für den Zustand 8, bei dem alle drei Komponenten ausgefallen sind, ist die eindeutige Zuordnung, welche Komponente (AU oder VU) für den Systemausfall verantwortlich ist, nicht möglich.

In Abb. 4.9 werden die zeitabhängigen Wahrscheinlichkeiten für die folgenden vier Fälle dargestellt:

- Fall 1: Systemausfall gesamt
- Fall 2: Systemausfall, der ausschließlich durch die VU verursacht wird (Zustände 4, 6 und 7)
- Fall 3: Systemausfall, der ausschließlich durch den gemeinsamen Ausfall der APUs verursacht wird (Zustand 5)
- Fall 4: Zustand 8, dass alle drei Komponenten (APU1, APU2 und VU1) gemeinsam ausgefallen sind.

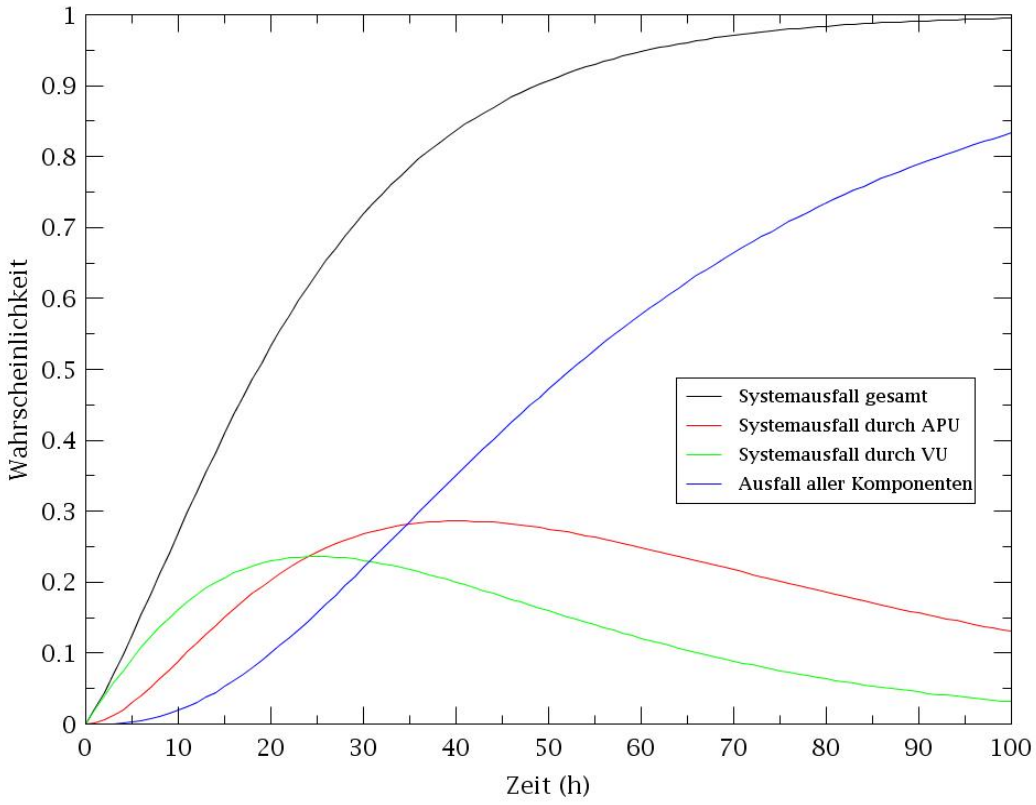

Abb. 4.9 Zeitabhängige Wahrscheinlichkeiten für einen Systemausfall insgesamt, durch VU oder durch APU sowie durch Ausfall aller Komponenten

Die Wahrscheinlichkeit für einen Systemausfall (schwarze Kurve in Abb. 4.9) entspricht der Kurve der Unverfügbarkeit des Systems in Abb. 3.12 (siehe Abschnitt 3.2.2), die unter Verwendung der Fehlerbaumanalyse mit RiskSpectrum berechnet wurde. In die-

sem Fall ergeben sich über die Fehlerbaumanalyse die gleichen Ergebnisse der Ausfallwahrscheinlichkeit des Systems, die auch unter Verwendung eines Markov-Prozesses erzielt werden.

Wichtige Erkenntnis ist, dass die Wahrscheinlichkeit des Ausfalls aller 3 Komponenten nach ca. 40 Stunden den Hauptbeitrag zur Wahrscheinlichkeit eines Systemausfalls liefert und mit zunehmender Zeit immer mehr an Bedeutung gewinnt. Dem gegenüber nimmt die Wahrscheinlichkeit, dass der Systemausfall nur durch die VU oder nur durch die APUs verursacht wird, nach einem anfänglichen Anstieg mit zunehmender Zeit wieder ab.

Dieses Verhalten widerspricht der ersten, oftmals üblichen Einschätzung, dass die Wahrscheinlichkeit für einen Ausfall aller 3 Komponenten doch geringer sein müsste als der alleinige Ausfall der VU-Komponente und auch geringer, als der Ausfall der zwei AUs. Bei dieser ‚naiven' Einschätzung vernachlässigt man jedoch den zeitlichen Effekt. Denn, je mehr Zeit vergeht, desto höher ist die Wahrscheinlichkeit, dass sich jede der drei einzelnen Komponenten im ausgefallenen Zustand befindet. Daraus erklärt sich auch das Absinken der Wahrscheinlichkeiten für den Ausfall der VU-Komponente und dem Ausfall der beiden APUs mit zunehmender Zeit. Nach ca. 40 Stunden wird z. B. der Systemausfall, der durch die beiden APUs verursacht wird und durch den Zustand 5 beschrieben wird, mit einer immer geringeren Wahrscheinlichkeit eintreten, je mehr Zeit vergeht. Der Grund liegt darin, dass die Wahrscheinlichkeit, dass sich die VU noch im intakten Zustand befindet, mit zunehmender Zeit geringer wird. Damit wird auch die Wahrscheinlichkeit des Zustands 5 immer geringer.

Aus den zeitlichen Verläufen der Wahrscheinlichkeiten in Abb. 4.9 erkennt man diejenigen Zeitbereiche, in denen die verschiedenen Zustände des Systems ihre maximalen Wahrscheinlichkeiten annehmen und es kann gezeigt werden, welche Ursachen zu verschiedenen Zeitpunkten den größten Beitrag zur Ausfallwahrscheinlichkeit des Systems liefern.

Beispiel 2

Im Modellsystem A120 (siehe Abb. 3.10) wurden die APUs als redundante Komponenten angeordnet. Die Anordnung der Komponenten APU1 und APU2 bestand in einer so

genannten ‚heißen' Redundanz, bei der beide Komponenten gleichzeitig in Betrieb sind. Nun könnten redundante Komponenten in einem System auch als sogenannte ‚kalte' Redundanz angeordnet werden. Bei der „kalten" Redundanz beginnt zunächst nur eine der beiden Komponenten (z. B. APU1) zu arbeiten, während sich die andere Komponente (APU2) in Ruhestellung („stand-by") befindet. Erst wenn die arbeitende Komponente (APU1) ausfällt, wird die Komponente in Ruhestellung (APU2) aktiviert. Während APU2 in Betrieb ist, könnte versucht werden die APU1 zu reparieren, so dass nach Ausfall von APU2 wieder auf APU1 umgeschaltet werden könnte, falls APU1 rechtzeitig repariert wurde und das System weiterhin in Betrieb ist.

Im Beispiel 2 soll zunächst die Frage untersucht werden, welche Auswirkung das System mit „kalter" Redundanz ohne Reparatur auf die Ausfallwahrscheinlichkeit des Systems hat. Das System mit „kalter" Redundanz wird in dem Programm RAMESU durch folgende Anweisungen beschrieben.

```
IF / APU1, 0 / THEN $ 4.0E-2
   DO / APU1, 1 /
ENDIF

IF / APU1, 1   APU2, 0   / THEN $ 4.0E-2      ! Erst wenn APU1 ausgefallen ist erfolgt für
   DO / APU2, 1 /                              ! APU2 der Übergang vom Zustand 0 in den
ENDIF                                          ! Zustand 1 mit der Rate 4.E-2

IF / VU1, 0 / THEN $ 2.0E-2
   DO / VU1, 1 /
ENDIF
```

Die Auswirkung der Änderung des Systems von einer „heißen" auf eine „kalte" Redundanz auf die Ausfallwahrscheinlichkeit des Systems wird durch Abb. 4.10 veranschaulicht. In Abb. 4.10 werden die zeitabhängigen Wahrscheinlichkeiten eines Systemausfalls für die Systeme mit „heißer" und „kalter" Redundanz gezeigt. Zusätzlich sind noch für beide Systeme die Wahrscheinlichkeiten für den Ausfall aller drei Komponenten sowie für den Ausfall des Systems, der nur durch die APUs verursacht wird, dargestellt.

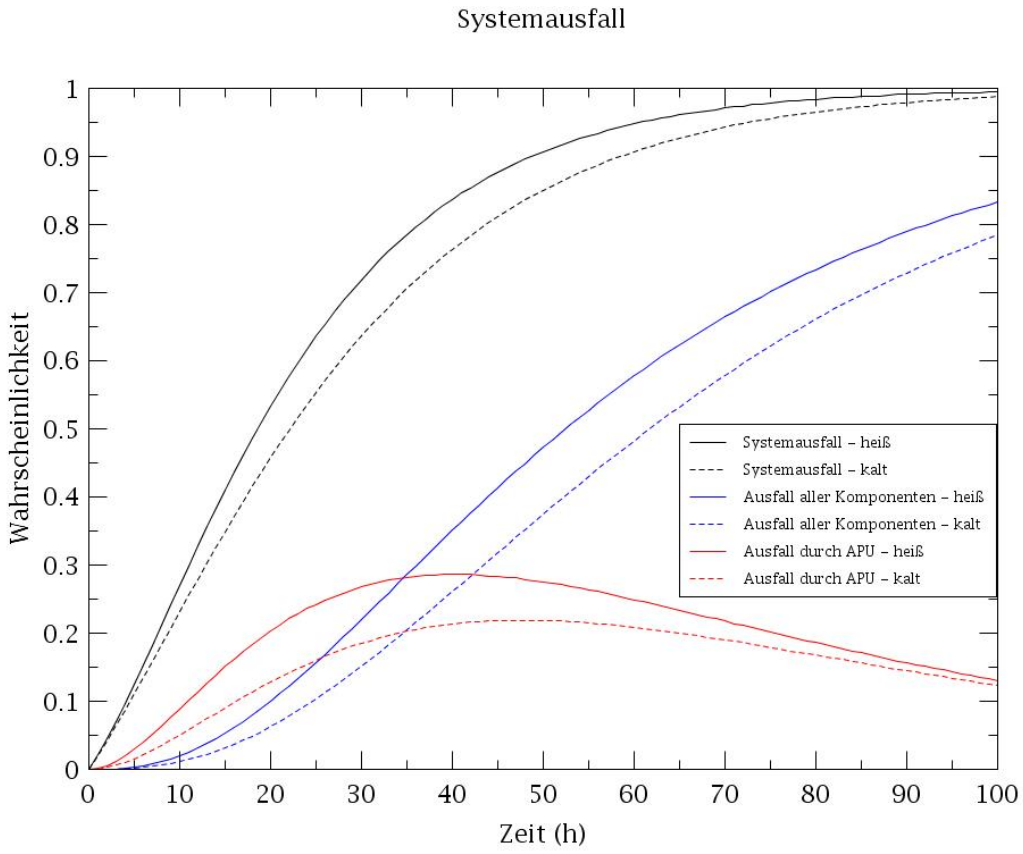

Abb. 4.10 Zeitabhängige Ausfallwahrscheinlichkeiten des Systems mit „heißer“ und „kalter“ Redundanz

Wie in Abb. 4.10 ersichtlich, erhält man durch Umstellung des Systems auf eine „kalte“ Redundanz eine leichte Verbesserung der Systemverfügbarkeit. Es zeigt sich, dass sich die größten Unterschiede in den Wahrscheinlichkeiten der Systeme mit „heißer“ und „kalter“ Redundanz nur auf bestimmte Zeitbereiche beschränken und sich die Ausfallwahrscheinlichkeiten der beiden Systeme mit zunehmender Zeit gegenseitig annähern.

Bei der bisherigen Modellierung des Systems mit „kalter“ Redundanz wurde stillschweigend vorausgesetzt, dass im Falle des Ausfalls von APU1 die Umschaltung auf APU2 absolut zuverlässig funktioniert. Diese sicherlich zu optimistische Annahme soll nun realistischer modelliert werden. Dazu wird angenommen, dass die Umschaltung von APU1 auf APU2 durch einen Schalter erfolgt, der mit einer bestimmten Zuverlässigkeit funktioniert.

Beispiel 3

In Beispiel 3 wird das Modell aus Beispiel 2 durch die Komponente „Schalter“ (im RAMESU-Programm als **Switch** bezeichnet) erweitert. Es wird angenommen, dass der Schalter mit einer Zuverlässigkeit von 90 % auf die Komponente APU2 umschaltet, wenn APU1 ausgefallen ist. Die notwendigen Anweisungen zur Einbindung des Schalters lauten:

Definition der Komponenten:

```
1 : APU1
2 : APU2
3 : VU1
4 : Switch

IF / APU1, 0  / THEN $ 4.0E-2
   DO / APU1, 1 /
ENDIF

IF / APU1, 1  Switch,0   / THEN        ! Wenn APU1 ausgefallen ist und der Schalter
  IF  / APU2, 0  / THEN $ 4.0E-2       ! funktioniert, erfolgt der Übergang von APU2 vom
     DO / APU2, 1 /                    ! Zustand 0 in den Zustand 1 mit der Rate 4.0 E-2
  ENDIF
ENDIF

IF / VU1, 0  / THEN $ 2.0E-2
   DO / VU1, 1  /
ENDIF
```

Die Modellierung für die Umschaltung durch den Schalter erfolgt durch folgende Anweisungen:

```
IF / APU1  Switch,0 / THEN $ 0.1, 1    ! Schalter fällt mit einer Wahrscheinlichkeit von 0.1 aus.
   DO / Switch,1 /                     ! Zeitpunkt der Aktivierung wird in der singulären Matrix 1
   RUNIF / Switch,1 APU2,0 / DO / APU2,1 /     ! definiert.
ENDIF
```

Aus der Anweisung wird deutlich, dass die Auswirkungen variierender Schalterzuverlässigkeiten auf das Systemverhalten untersucht werden können, indem die Ausfallwahrscheinlichkeit des Schalters von 0,1 pro Anforderung durch andere Ausfallwahrscheinlichkeiten ersetzt wird.

Die obige RUNIF-Anweisung besagt, dass die Komponente APU2 auf nicht verfügbar gesetzt wird, wenn der Schalter ausgefallen ist.

Die Zeitpunkte, wann die Umschaltungen über den Schalter erfolgen, wird über eine so genannte singuläre Matrix spezifiziert, in der diskrete Zeitpunkte definiert werden, zu denen bestimmte Übergänge mit bestimmten Wahrscheinlichkeiten auftreten können. Da die Umschaltung zu jedem beliebigen Zeitpunkt nach Ausfall der Komponente APU1 erfolgen kann, müsste der Zeitpunkt der Umschaltung als stetige Größe behandelt werden. Da die singuläre Matrix nur diskrete Zeitpunkte berücksichtigen kann, wird die stetige Zeit der Umschaltung dadurch approximiert, indem die Wahrscheinlichkeit des Schalterzustands in Zeitschritten von zwei Minuten ermittelt wird. Demzufolge wird in der singulären Matrix für den Berechnungszyklus des Schalterzustands die Periode 0.034 h angegeben. Der Zyklus startet bei Null und endet nach der Beobachtungszeit bei 100 Stunden.

```
C   No. OF SINGULAR MATRICES
        1
C   No. OF  CYCLES FOR 1. SING. MATRIX (ÜM1)
        1
C    START        PERIOD        END          ! Berechnungszyklus des Schalters
        1.           0.034         100.
```

Die Auswirkung einer Schalterzuverlässigkeit von 90 % auf die Ausfallwahrscheinlichkeit des Systems wird in Abb. 4.11 veranschaulicht. Zum Vergleich wird auch die Ausfallwahrscheinlichkeit des Systems mit „heißer“ und „kalter“ Redundanz mit 100%iger Zuverlässigkeit der Umschaltung dargestellt.

In Beispiel 2 wurde gezeigt, dass das System mit „kalter“ Redundanz und einer Zuverlässigkeit der Umschaltung von 100 % eine etwas geringere Ausfallwahrscheinlichkeit aufweist als das System mit „heißer“ Redundanz. In diesem Beispiel wurde angenommen, dass die Zuverlässigkeit der Umschaltung 90 % beträgt. Die Abb. 4.11 zeigt, dass bei einer Zuverlässigkeit des Schalters von 90 % die Wahrscheinlichkeit des Systemausfalls des Systems mit „kalter“ Redundanz über der des Systems mit „heißer“ Redundanz liegt.

Eine Zuverlässigkeit des Schalters von 90 % reicht somit nicht aus, das günstigere Verhalten der „kalten“ Redundanz mit absolut zuverlässiger Umschaltung gegenüber dem System mit „heißer“ Redundanz beizubehalten.

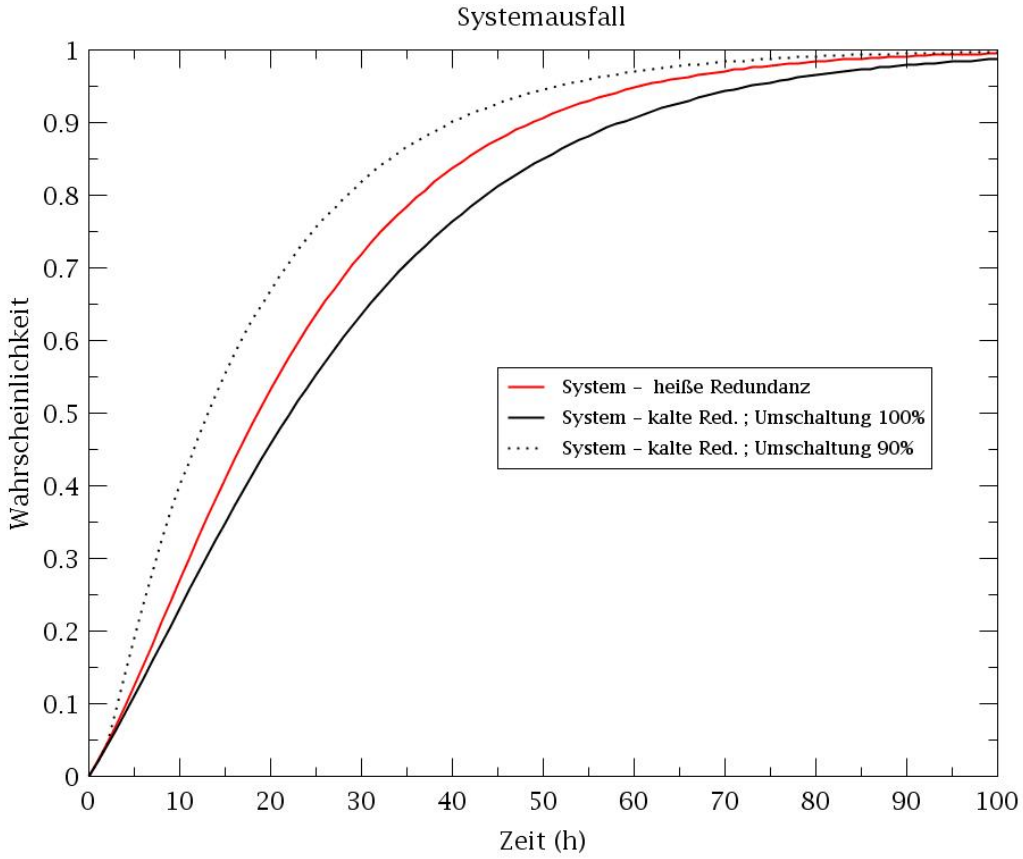

Abb. 4.11 Zeitabhängige Ausfallwahrscheinlichkeiten der Systeme mit „heißer“ bzw. „kalter“ Redundanz unter Berücksichtigung einer 90%igen Zuverlässigkeit der Umschaltung durch einen Schalter

Aufgrund der in Abb. 4.11 dargestellten Situation kann man die Frage stellen, wie groß die Zuverlässigkeit des Schalters sein muss, damit die Ausfallwahrscheinlichkeit des Systems mit „kalter“ Redundanz unter der des Systems mit „heißer“ Redundanz liegt. Bei einer Zuverlässigkeit von 100 % wurde das günstigere Verhalten schon gezeigt.

Im Folgenden sollen die Auswirkungen verschiedener Schalterzuverlässigkeiten untersucht werden. In Abb. 4.12 sind die Auswirkungen der Schalterzuverlässigkeiten von 90 %, 95 %, 99 % und 99,8 % dargestellt.

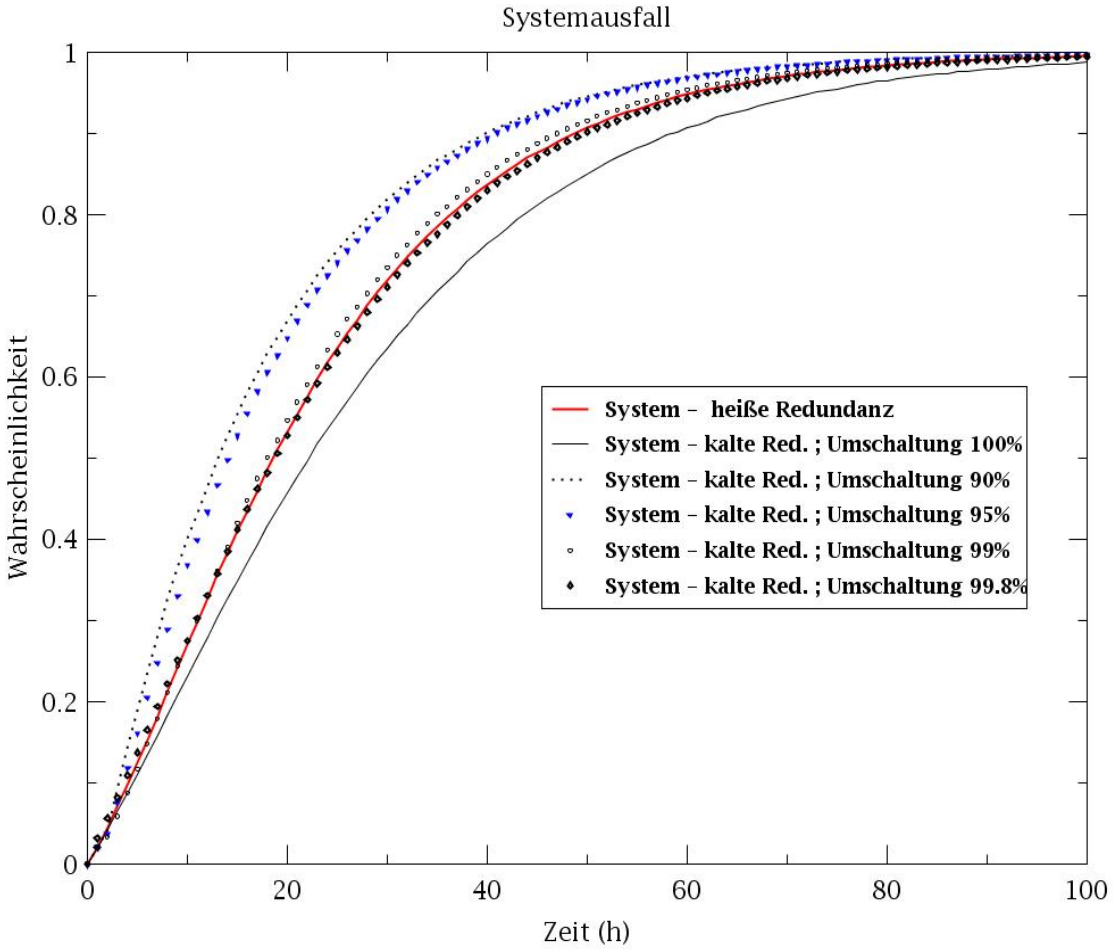

Abb. 4.12 Auswirkung verschiedener Systemzuverlässigkeiten auf die Ausfallwahrscheinlichkeit des Systems

Abb. 4.12 zeigt, dass eine Erhöhung der Schalterzuverlässigkeit von 90 % auf 95 % nur eine geringfügige Verringerung der Systemausfallwahrscheinlichkeit bewirkt. Eine Erhöhung auf 99 % zeigt dagegen eine deutlichere Verbesserung der Systemverfügbarkeit. Trotzdem liegt die Ausfallwahrscheinlichkeit des Systems noch etwas über der des Systems mit „heißer“ Redundanz. Wie aus Abb. 4.12 zu erkennen ist, erweist sich hier die Systemarchitektur mit „kalter“ Redundanz gegenüber dem System mit „heißer“ Redundanz erst dann als vorteilhaft, wenn eine Schalterzuverlässigkeit von mindestens 99,8 % gewährleistet werden kann.

Ein Vorteil der „kalten“ Redundanz liegt darin, dass nur eine der redundanten Komponenten in Betrieb ist. Solange diese eine Komponente in Betrieb ist, kann versucht werden, die andere ausgefallene Komponente zu reparieren. Diese Situation soll in dem folgenden Beispiel 4 untersucht werden.

Beispiel 4

Als weitere Verfeinerung des Modells soll im Beispiel 4 angenommen werden, dass nach dem Ausfall von AU1 und der erfolgreichen Umschaltung auf AU2 versucht wird, eine Reparatur von AU1 durchzuführen. Gelingt die Reparatur bevor AU2 ausfällt, kann nach Ausfall von AU2 wieder auf AU1 umgeschaltet werden. Während AU1 in Betrieb ist, wird versucht AU2 zu reparieren. Im Folgenden wird untersucht, wie sich eine Reparatur der Komponenten auf die Ausfallwahrscheinlichkeit des Systems auswirkt. Solange die Reparaturen der jeweiligen Komponenten abgeschlossen ist bevor die jeweils andere Komponente ausfällt, kann immer auf die jeweils andere Komponente umgeschaltet werden.

Für die Vergleichsrechnungen wird eine Zuverlässigkeit des Schalters von 95 % angenommen. Dies hat, wie in Beispiel 3 gezeigt wurde, eine höhere Systemausfallwahrscheinlichkeit als das System mit ‚heißer' Redundanz zur Folge.

Für die Reparaturen wird jeweils eine exponentialverteilte Reparaturzeit angenommen. Um die Effekte der Reparaturzeiten darzustellen, wird jeweils eine mittlere Reparaturzeit von 10 h bzw. 5 h angenommen. In Abb. 4.13 wird die Ausfallwahrscheinlichkeit des Systems für die durchgeführten Vergleichsrechnungen betrachtet.

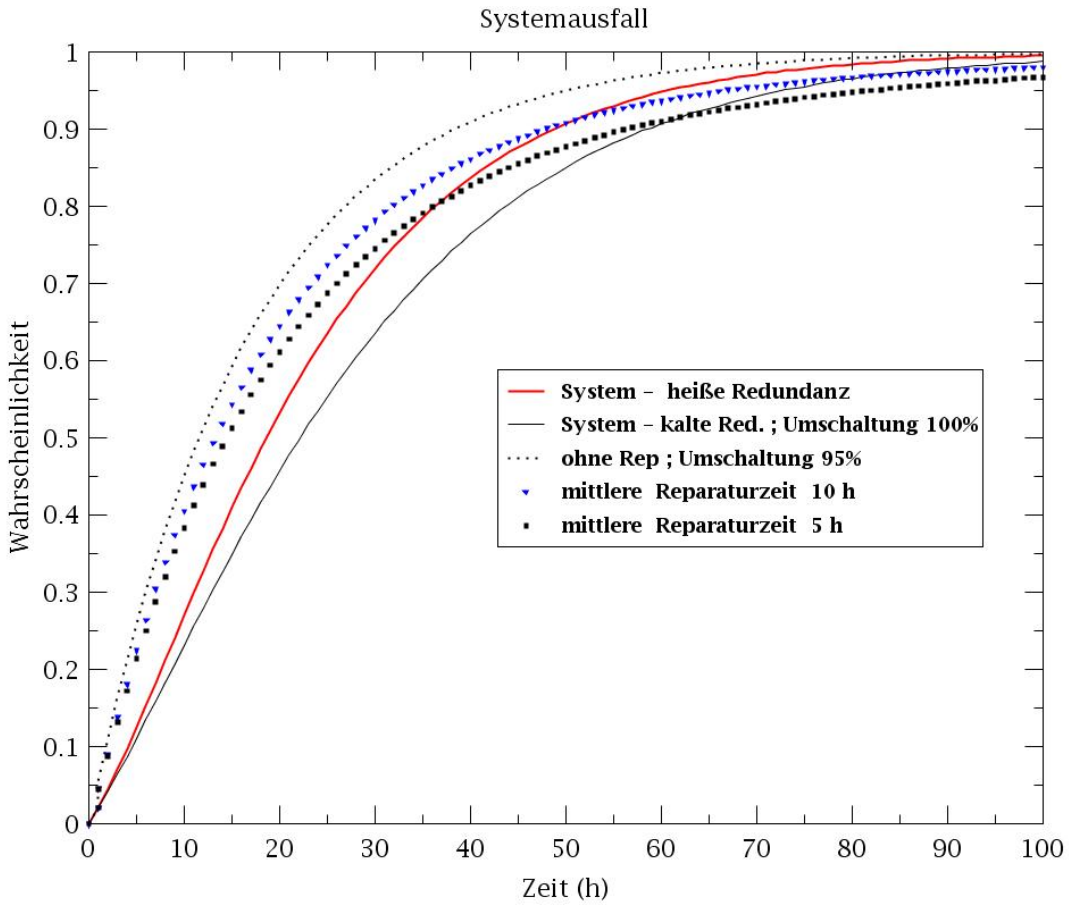

Abb. 4.13 Zeitabhängige Ausfallwahrscheinlichkeiten des Systems unter Berücksichtigung von Umschaltungen und Reparatur der Komponenten

Welche Auswirkungen es hat, wenn bei einem System mit „kalter“ Redundanz versucht wird, die ausgefallene Komponente zu reparieren, wird in Abb. 4.13 verdeutlicht. Hier ist zur erkennen, dass Reparaturen der ausgefallenen Komponenten bei den wechselseitigen Umschaltungen zu einer Verbesserung der Systemzuverlässigkeit führen, die sich insbesondere in der zweiten Hälfte der Beobachtungszeit auswirkt.

Bei einer mittleren Reparaturzeit von 10 h liegt die Ausfallwahrscheinlichkeit des Systems in den ersten 50 h über der des Systems mit „heißer“ Redundanz. Ab ca. 50 h bewirken die Reparaturen, dass die Ausfallwahrscheinlichkeiten des Systems mit „heißer“ Redundanz und nach ca. 80 h auch die Ausfallwahrscheinlichkeiten des Systems mit „kalter“ Redundanz und 100 % zuverlässiger Umschaltung unterschritten werden.

Bei einer mittleren Reparaturzeit von 5 h wirkt sich die Verbesserung der Systemzuverlässigkeit entsprechend deutlicher und früher aus. Hier werden die Ausfallwahrschein-

lichkeiten des Systems mit „heißer“ Redundanz bereits nach 35 h und die des Systems mit „kalter“ Redundanz und 100 % zuverlässiger Umschaltung nach ca. 60 h unterschritten.

An dieser Stelle wird darauf hingewiesen, dass die untersuchten Systeme in den genannten Beispielen sehr hohe Ausfallwahrscheinlichkeiten erreichen. Diese werden auch durch die Reparatur nicht wesentlich geringer. Dies ist dadurch begründet, dass die angenommenen Ausfallraten 0,04 bzw. 0,02 der APUs bzw. der VUs relativ groß sind. Welchen Einfluss die Reparaturen auf den Ausfall der APUs haben, kann man erkennen, wenn die Systemausfallwahrscheinlichkeiten betrachtet werden, die nur durch die APUs verursacht werden. Dies wird in Abb. 4.14 verdeutlicht.

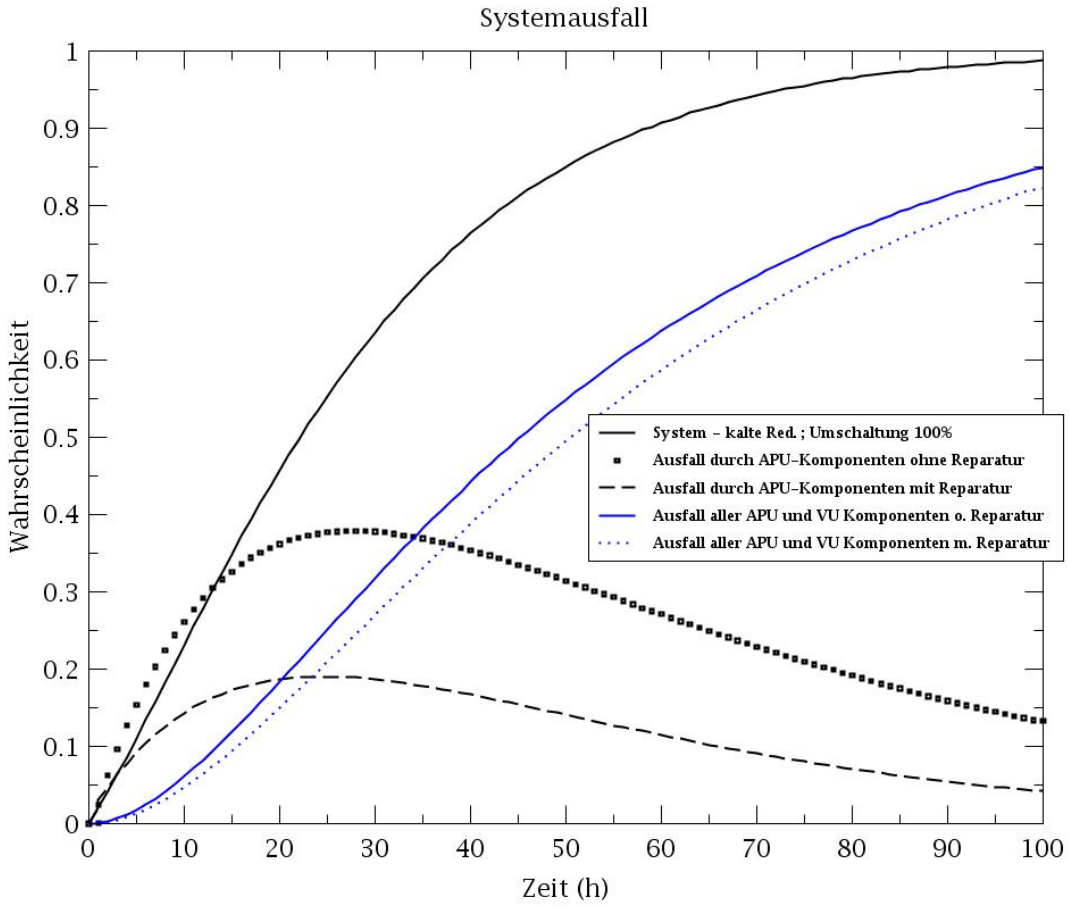

Abb. 4.14 Einfluss der Reparatur auf den Beitrag der APUs auf die Ausfallwahrscheinlichkeit des Systems

Abb. 4.14 zeigt, dass der Beitrag zur Systemausfallwahrscheinlichkeit, der durch den Ausfall der APUs verursacht wird, durch die Reparaturmaßnahme bei einer mittleren Reparaturzeit von 5 h ungefähr um die Hälfte verringert werden kann.

Der Einfluss der Reparaturen auf die Wahrscheinlichkeit, dass sich sowohl die APUs als auch die VU gemeinsam im ausgefallenen Zustand befinden, wirkt sich demgegenüber nicht so stark aus. D. h., die Reparaturen der APUs können die hohen angenommenen Ausfallraten der VU nicht hinreichend kompensieren.

Beispiel 5

Abschließend soll im Beispiel 5 gezeigt werden, dass mit dem Programm RAMESU auch der Einfluss einer Alterung von Komponenten (z. B. Hardware digitaler Leittechnik) modelliert werden kann. Dazu soll im Folgenden angenommen werden, dass sowohl die APUs als auch die VU-Komponenten einem Alterungsprozess unterworfen sind. Um den Einfluss der Alterung auf die Ausfallwahrscheinlichkeiten der Komponenten zu untersuchen, wird hier der Einfachheit halber von einem System mit „heißer“ Redundanz ausgegangen, in dem keine Umschaltung zwischen den Komponenten erfolgt.

Für den Alterungsprozess der Komponenten werden folgende Annahmen zugrunde gelegt. In diesem Beispiel soll zugleich demonstriert werden, dass auch Unsicherheiten bzgl. des Alterungsprozesses von Komponenten mit dem Markov-Programm berücksichtigt werden können. Bzgl. der Alterung werden folgende Unsicherheiten für die VU angenommen:

- Mit einer Wahrscheinlichkeit von 70 % erhöht sich die Ausfallrate der VU nach einer Betriebszeit von 60 h von 0,02 h^{-1} auf 0,03 h^{-1}.
- Mit einer Wahrscheinlichkeit von 30 % unterliegt die VU keiner Alterung.
- Die Ausfallrate der Komponente APU1 erhöht sich nach 50 h Betriebszeit von 0,04 h^{-1} auf 0,06 h^{-1}.
- Die Ausfallrate der Komponente APU2 erhöht sich nach 30 h Betriebszeit von 0,04 h^{-1} auf 0,05 h^{-1} und erhöht sich nach 70 h Betriebszeit weiter von 0,05 h^{-1} auf 0,07 h^{-1}.

Um den Einfluss der Alterung genauer zu untersuchen, werden in Abb. 4.15 die Auswirkungen der Alterung für die einzelnen Komponenten dargestellt.

Hier sind die Systemausfallwahrscheinlichkeiten dargestellt, die ausschließlich durch die APUs (d. h. beide APUs sind ausgefallen und die VU ist ok), ausschließlich durch die VU (d. h. die VU ist ausgefallen und mindestens eine der APUs ist ok) und durch den gemeinsamen Ausfall aller Komponenten verursacht werden.

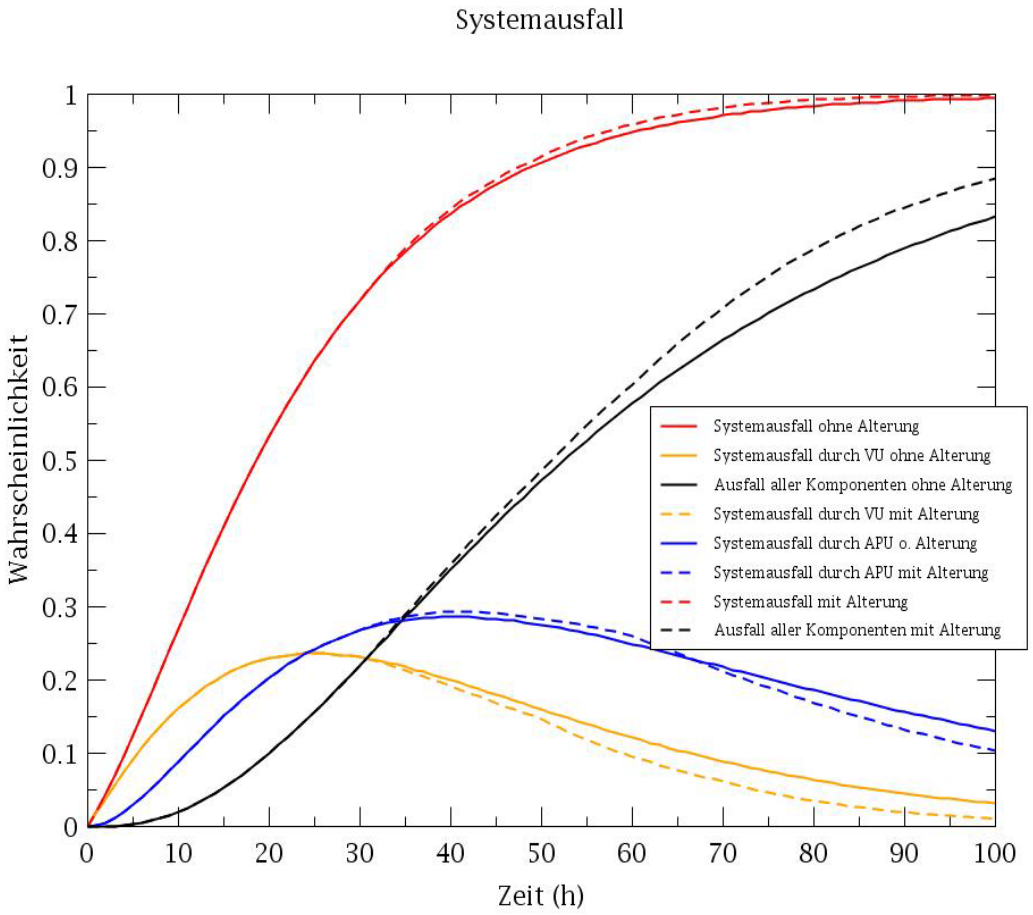

Abb. 4.15 Einfluss der Alterung auf die zeitabhängigen Wahrscheinlichkeiten verschiedener Systemzustände

Es zeigt sich eine Erhöhung der Wahrscheinlichkeit für den Zustand, dass sich alle drei Komponenten im ausgefallenen Zustand befinden. Die Erhöhung der Wahrscheinlichkeit beginnt nach 30 h und setzt sich bis 50 h mit ganz leichter Ausprägung durch die Erhöhung der Ausfallrate von APU2 von 0,04 h^{-1} auf 0,05 h^{-1} fort.

Nach 50 h erhöht sich die Ausfallrate der APU1 und nach 60 h die Ausfallrate der VU. Zu diesen Zeitpunkten nimmt die Erhöhung der Zustandswahrscheinlichkeit gegenüber

der Wahrscheinlichkeit ohne Alterung noch etwas zu. Nach 70 h erfährt die Ausfallrate von APU2 nochmals eine erhebliche Erhöhung was sich in einem deutlicheren Anstieg der Zustandswahrscheinlichkeit gegenüber der ohne Alterung ausdrückt.

Obwohl die APUs sowie die VU einer Alterung unterworfen sind, liegen die Wahrscheinlichkeiten für die Zustände, dass ein Systemausfall nur durch die APUs bzw. nur durch die VU-Komponente verursacht wird, ab gewissen Zeitpunkten unter den Wahrscheinlichkeiten der Zustände ohne Alterung. Dies ist darin begründet, dass die Wahrscheinlichkeiten für die Zustände eines Systems voneinander abhängig sind. Je mehr die Wahrscheinlichkeit des Zustands für den Ausfall aller drei Komponenten zunimmt, desto geringer werden die Beiträge der anderen Zustände für den Systemausfall. Eine Begründung dieses Verhaltens wurde bereits in Beispiel 1 gegeben.

Die Auswirkung der in diesem Beispiel angenommenen Alterung auf die Wahrscheinlichkeit eines Systemausfalls erscheint relativ gering. Hierbei ist jedoch zu berücksichtigen, dass die Wahrscheinlichkeit eines Systemausfalls ohne Alterung schon nach 40 h relativ hohe Werte annimmt, so dass sich eine Alterung, die zu späteren Zeitpunkten stattfindet, nicht mehr ganz so stark auswirkt.

Durch die oben beschriebenen Beispiele sollte demonstriert werden, dass sich das Markov-Programm der GRS gut eignet, um Auswirkungen verschiedener Systemarchitekturen zu modellieren und zu quantifizieren. Der Vorteil liegt darin, dass Änderungen im System relativ einfach und schnell modelliert werden können und die Ergebnisse verschiedener Systeme ausgewertet und miteinander verglichen werden können.

Um die Vorteile des Markov-Methode auch für größere Systeme (mehr als 20 Komponenten) nutzbar zu machen, wäre die Entwicklung eines Konzepts zur Erweiterung des Programms RAMESU zweckmäßig, um es auch für die Analyse größerer Systeme einsetzen zu können. Allein die Vergrößerung der entsprechenden Arrays im Programm wäre nicht zielführend, da diese wieder sehr schnell durch ungezähmtes Wachstum des Zustandsraums an ihre Grenzen stößt. Erfolgsversprechender wäre die Umsetzung eines Konzepts, dass die Analyse eines größeren Systems auf der Basis des Zusammenspiels kleinerer Teilsysteme durchgeführt wird. Zur Ausarbeitung und Implementierung eines solchen Konzepts bedarf es einer entsprechenden Weiterentwicklung des RAMESU-Programms.

5 Analysen

5.1 Grundlegende Vorgehensweise

Bevor Sensitivitätsanalysen (durch die gezielte Variation unterschiedlicher Parameter) für alle Modellsysteme durchgeführt werden, soll zunächst am Modellsystem A222 (siehe Abb. 3.2) dargelegt werden, auf welche Weise welche Ergebnisse erzielt und wie diese interpretiert werden können. Für alle anderen Modellsysteme findet man die entsprechenden Tabellen und Abbildungen gesammelt im Anhang.

Ausgangspunkt aller Analysen ist stets eine Ausfalleffektanalyse (u. a. Ermittlung von Ausfallkombinationen der Rechner), welche für die in diesem Bericht untersuchten Leittechnikmodelle in separaten Tabellen für die unterschiedlichen Leittechnikebenen durchgeführt werden kann. Dabei beziehen sich die einzelnen Tabellen auf die möglichen Ausgangssignale einer Leittechnikebene und deren Auswirkungen auf die unterlagerten Ebenen im Anforderungsfall.

Auf der untersten Ebene aller Modellsysteme befindet sich jeweils ein analoger Logikbaustein (AL – Analog Logic), im Fall des Modellsystems A222 eine 1-von-2-Auswahl („1oo2“). Da dieser Baustein nicht Teil der digitalen Leittechnik ist, kann dieser nur entweder korrekt funktionieren („OK“, Tab. 5.1) oder nichtselbstmeldend ausgefallen („NSF“, Tab. 5.1) sein. Die Fehlererkennung kann nur bei WKP erfolgen oder die Komponente fällt bei Anforderung aus.

Tab. 5.1 Der Ausfallzustand der AL-Logik des Modellsystems A222

AL (1v2)	
Ausgangssignal	**Qualität**
1	OK
0	NSF

Neben dem Ausfall der AL selbst, kann ein fehlerhaftes Ausgangssignal aber auch bereits auf den darüberliegenden Ebenen verursacht werden. So kann z. B. jede VU ihrerseits selbstmeldend oder nichtselbstmeldend ausfallen (Tab. 5.2). Zwei gleichzeitige Fehler auf der Ebene der VUs führen dazu, dass die AL im Anforderungsfall kein auslösendes Signal („1, OK“) erzeugt.

Für die einfachere Lesbarkeit werden in Tab. 5.2 und in allen folgenden Tabellen die folgenden Hintergrundfarben für die einzelnen Zellen verwendet:

- korrekte Signale sind grün,
- nichtselbstmeldend fehlerhafte Signale sind rot und
- selbstmeldend fehlerhafte Signale sind gelb hinterlegt.

Tab. 5.2 Mögliche Ausfallkombinationen der beiden VUs des Modellsystems

VU1.A		VU2.A		AL (1v2)
Ausgangssignal, Qualität	**Flag**	**Ausgangssignal, Qualität**	**Flag**	**Ausgangssignal, Qualität**
1, OK	0	1, OK	0	1, OK
0, SF	1	1, OK	0	1, OK
1, OK	0	0, SF	1	1, OK
0, NSF	0	1, OK	0	1, OK
1, OK	0	0, NSF	0	1, OK
0, SF	1	0, SF	1	0, SF
0, SF	1	0, NSF	0	0, NSF
0, NSF	0	0, SF	1	0, NSF
0, NSF	0	0, NSF	0	0, NSF

Anmerkung:
Die VUs können nichtselbstmeldend (NSF) oder selbstmeldend (SF) ausfallen. Bei zwei gleichzeitigen VU-Ausfällen gibt die AL dann fehlerhaft kein Auslösesignal aus.

In diesem speziellen Fall ist zu beachten, dass die AL zwar nur nichtselbstmeldend („NSF“) ausfallen kann, aber der selbstmeldende Ausfall beider VUs („0, SF“) insgesamt zu einem selbstmeldenden Ausfall des Auslösesignals führt.

Neben Ausfällen der VUs selbst, können deren fehlerhafte Ausgangssignale im Anforderungsfall aber auch auf der Ebene der PUs verursacht werden. Tab. 5.3 zeigt diesen Zusammenhang. So führt beispielsweise der gleichzeitige nichtselbstmeldende Ausfall beider PUs (unterste Zeile in Tab. 5.3) dazu, dass die zwei Eingangssignale in die beiden VUs (VUx.A, x = 1, 2) jeweils valide „0“-Signale sind (mit Flag 0 gekennzeichnete Eingangssignale sind aus Sicht der VUs „korrekte“ Eingangssignale). Bei zwei validen Eingangssignalen ist die interne Wertungslogik der VUs eine 1-von-2-Auswahl und somit das Ausgangssignal beider VUs eine fehlerhafte Null („0, NSF“).

Tab. 5.3 Mögliche Ausfallkombinationen der beiden PUs und deren Auswirkungen auf die Ausgabesignale der VUs für das Modellsystem A222

PU1.A		PU2.A		VUx.A (x = 1, 2)		
Ausgangs-signal	**Flag**	**Ausgangs-signal**	**Flag**	**Valide Eingangs-signale (Flag 0)**	**Wertungs-logik**	**Ausgangs-signal, Qualität**
1 (> limit)	0	1 (> limit)	0	1; 1	1v2	1, OK
beliebig	1	1 (> limit)	0	1	1v1	1, OK
1 (> limit)	0	beliebig	1	1	1v1	1, OK
0 (< limit)	0	1 (> limit)	0	0; 1	1v2	1, OK
1 (> limit)	0	0 (< limit)	0	1; 0	1v2	1, OK
beliebig	1	beliebig	1	keine	keine	0, SF
beliebig	1	0 (< limit)	0	0	1v1	0, NSF
0 (< limit)	0	beliebig	1	0	1v1	0, NSF
0 (< limit)	0	0 (< limit)	0	0; 0	1v2	0, NSF

Anmerkung:
Die Umschaltung der VU-Wertungslogik von einer 1-von-2-Auswahl auf eine 1-von-1-Auswahl spielt für dieses einfache Modellsystem keine Rolle, da sich eine 1-von-2-Auswahl bei nur einem validen Eingangssignal exakt genauso wie eine 1-von-1-Auswahl verhält. Dies wurde nur der Vollständigkeit halber in der Tabelle angegeben. Entsprechende Umschaltungen können für komplexere Modellsysteme aber durchaus relevant sein.

Zuletzt müssen noch die Auswirkungen möglicher Ausfälle der AUs näher betrachtet werden (Tab. 5.4). Die AUs können ebenfalls selbstmeldend („SF“) oder nichtselbstmeldend („NSF“) ausfallen. Selbstmeldend ausgefallene Signale der AUs werden von den PUs nicht berücksichtigt, bei nur einem validen Eingangssignal wird dann statt dem 2. Maximum („2. Max“) der Eingangssignale das Maximum („Max“) des verbliebenen Eingangssignals (also das einzige Signal direkt) für den internen Vergleich mit dem Grenzwert („limit“) herangezogen. Diese Unterscheidung erscheint für dieses relativ einfache Modellsystem unnötig kompliziert, macht aber bei komplexeren Architekturen Sinn, da durch solche Umschaltungen beispielsweise fehlerhafte Auslösungen verhindert werden können.

Insgesamt ist die Verwendung des zweiten Maximums bei einem lediglich zweifach redundanten System wie das Modellsystem A222 sogar extrem ungünstig. Dies führt nämlich dazu, dass bereits eine einzelne nichtselbstmeldend ausgefallene AU („< limit, NSF“) zu einem Gesamtausfall des Systems führt (siehe hierzu auch die Minimalschnitte des Modellsystems A222 in der Fehlerbaumanalyse, Tab. 5.4). Denn bereits

bei einem einzelnen nichtselbstmeldenden Ausfall einer AU (bei noch funktionierender zweiter AU) erschienen zwar beide Eingangssignale in die PUs als valide („Flag 0“), einer der Werte liegt dabei jedoch oberhalb des Grenzwertes („> limit“), der zweite nicht („< limit“), da für nichtselbstmeldend ausgefallene AUs angenommen wurde, dass diese zu einem Wert unterhalb des überwachten Grenzwerts ausfallen (siehe Kapitel 3). Das 2. Maximum liegt in diesen Fällen somit immer unter dem Grenzwert und es kommt zu keiner Auslösung.

Tab. 5.4 Mögliche Ausfallkombinationen der AUs und deren Auswirkungen auf die von den PUs ausgegebenen Signale für das Modellsystem A222

AU1.A		**AU2.A**		**PUx.A (x = 1, 2)**		
Ausgangs-signal, Qualität	**Flag**	**Ausgangs-signal, Qualität**	**Flag**	**Eingangs-signale**	**“2. Max”**	**Ausgangs-signal, Qualität**
> limit, OK	0	> limit, OK	0	> limit; > limit	2. Max	1
beliebig, SF	1	> limit, OK	0	> limit	Max	1
> limit, OK	0	beliebig, SF	1	> limit	Max	1
< limit, NSF	0	> limit, OK	0	< limit; > limit	2. Max	0
> limit, OK	0	< limit, NSF	0	> limit; < limit	2. Max	0
beliebig, SF	1	beliebig, SF	1	keine	kein	kein
beliebig, SF	1	< limit, NSF	0	< limit	Max	0
< limit, NSF	0	beliebig, SF	1	< limit	Max	0
< limit, NSF	0	< limit, NSF	0	< limit; < limit	2. Max	0

Das Modellsystem A222 wird daher in den späteren Auswertungen zusätzlich in einer modifizierten Form („A222 mod“) berücksichtigt, in der die PUs grundsätzlich den größten Wert („Max“) für den Vergleich mit dem überwachten Grenzwert verwenden. Dieses modifizierte Modellsystem hat eine wesentlich höhere Zuverlässigkeit.

Die in Tab. 5.1 bis Tab. 5.4 dargestellten Ausfallkombinationen können direkt in einen Fehlerbaum übertragen werden. So sieht z. B. der Teil des Fehlerbaums, der die Ausfälle der AL beschreibt (Tab. 5.1), wie in Abb. 5.1 gezeigt, aus: Die AL kann nur nicht-

selbstmeldend ausgefallen sein oder die von den VUs kommenden Eingangssignale sind fehlerhaft.

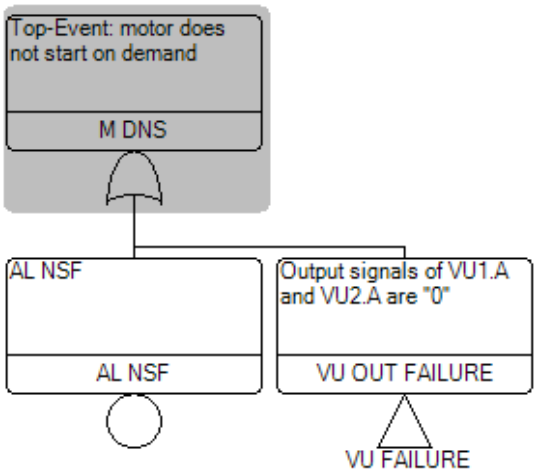

Abb. 5.1 Oberste Ebene („Top-Event“) des Fehlerbaums des Modellsystems A222 in RiskSpectrum

Entsprechend finden sich die Inhalte der weiteren Tabellen (Tab. 5.2, Tab. 5.3 und Tab. 5.4) ebenfalls im Fehlerbaum des Modellsystems A222. So stellen sich die möglichen Ausfälle der PUs im Fehlerbaum beispielsweise wie in Abb. 5.2 gezeigt dar. Diese Darstellung berücksichtigt allerdings noch keine gemeinsam verursachten Ausfälle („GVA“, bzw. „CCF – Common Cause Failure“ im Fehlerbaummodell). Diese ließen sich z. B. berücksichtigen, indem die entsprechenden Basisereignisse zusätzlich mit den entsprechenden GVA-Ereignissen mit ODER-Gates verknüpft würden. Da diese zusätzlichen GVA dann in allen beitragenden Fehlerkombinationen auftauchen würden, werden diese wegen besserer Übersichtlichkeit, wie in Abb. 5.3 dargestellt, berücksichtigt.

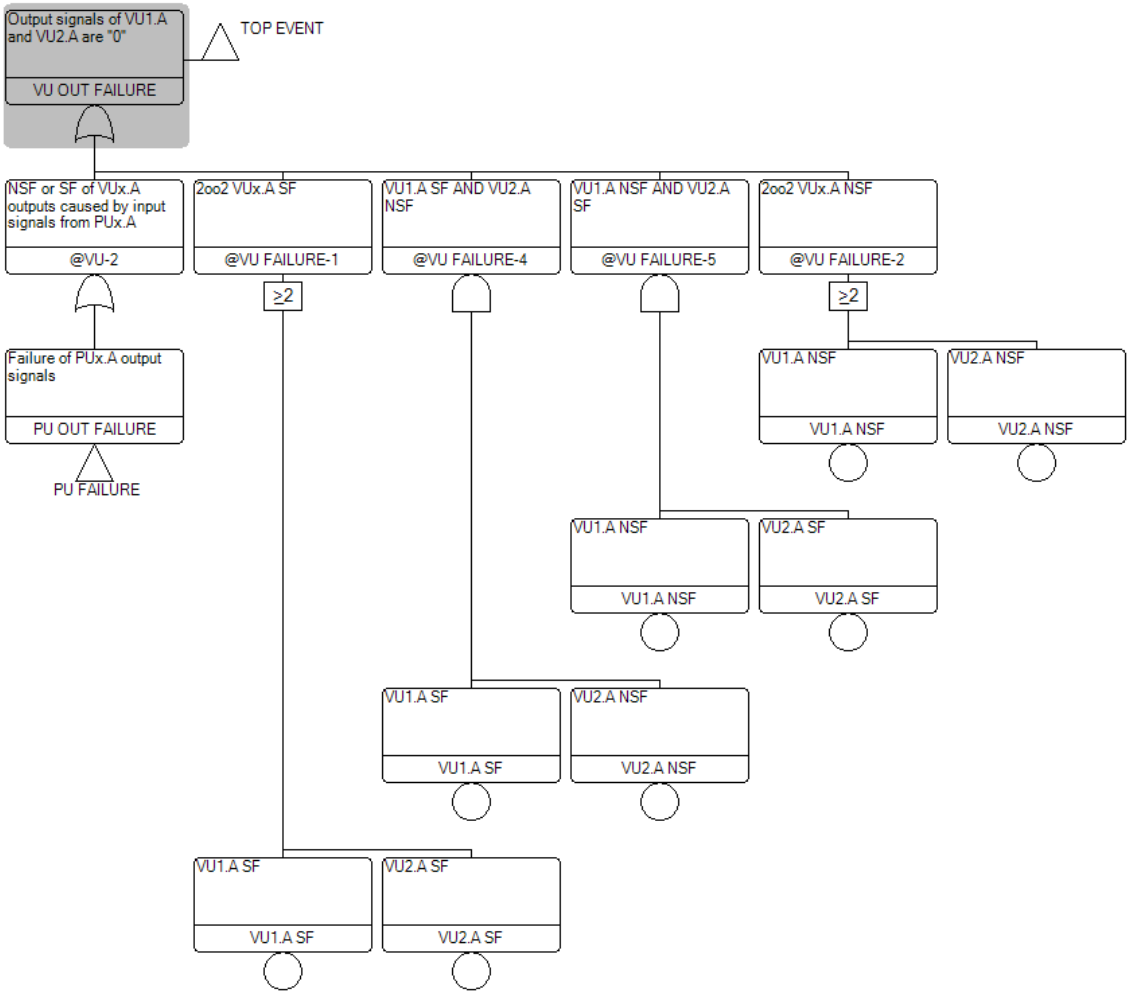

Abb. 5.2 Ausschnitt aus dem Fehlerbaum des Modellsystems A222, der die Ausfallkombinationen der PUs berücksichtigt (vgl. hierzu Tab. 5.2)

Anmerkung:

In diesem Fehlerbaummodell sind noch keine GVAs berücksichtigt

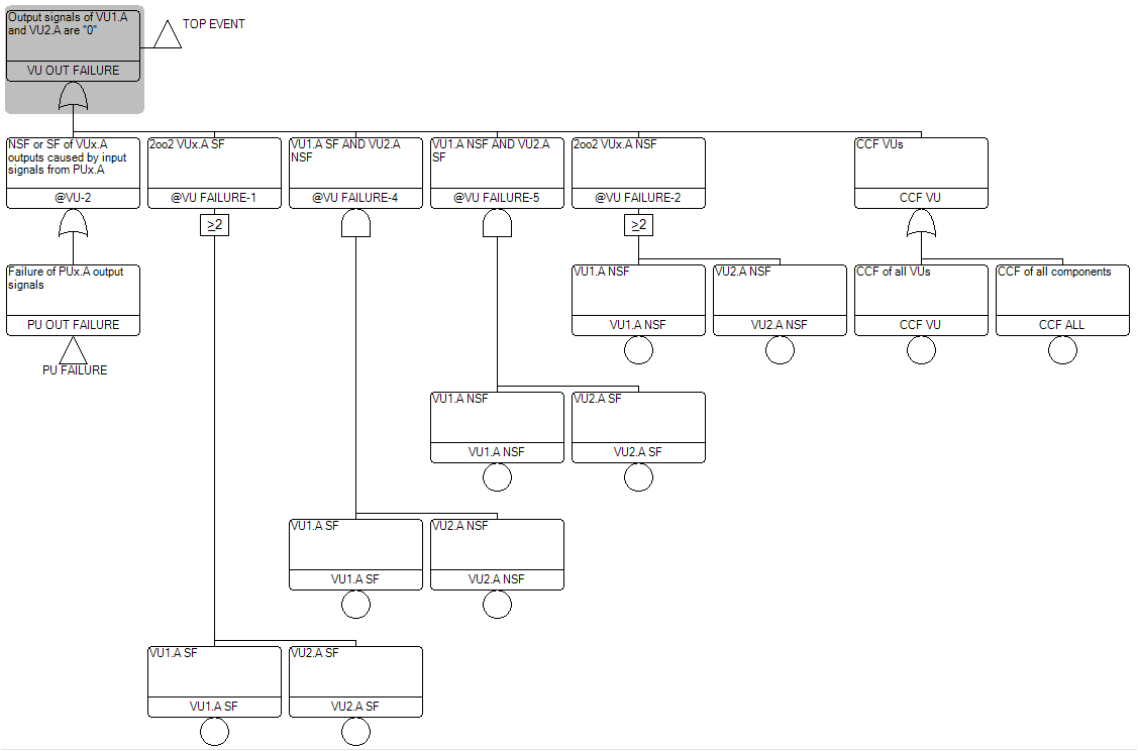

Abb. 5.3 Erweiterung des Fehlerbaums des Modellsystems A222 in Abb. 5.2 um GVA

Der restliche Fehlerbaum des Modellsystems A222, der die Inhalte der verbliebenen beiden Tabellen (Tab. 5.3 und Tab. 5.4) berücksichtigt, ist in Abb. 5.4 und Abb. 5.5 dargestellt.

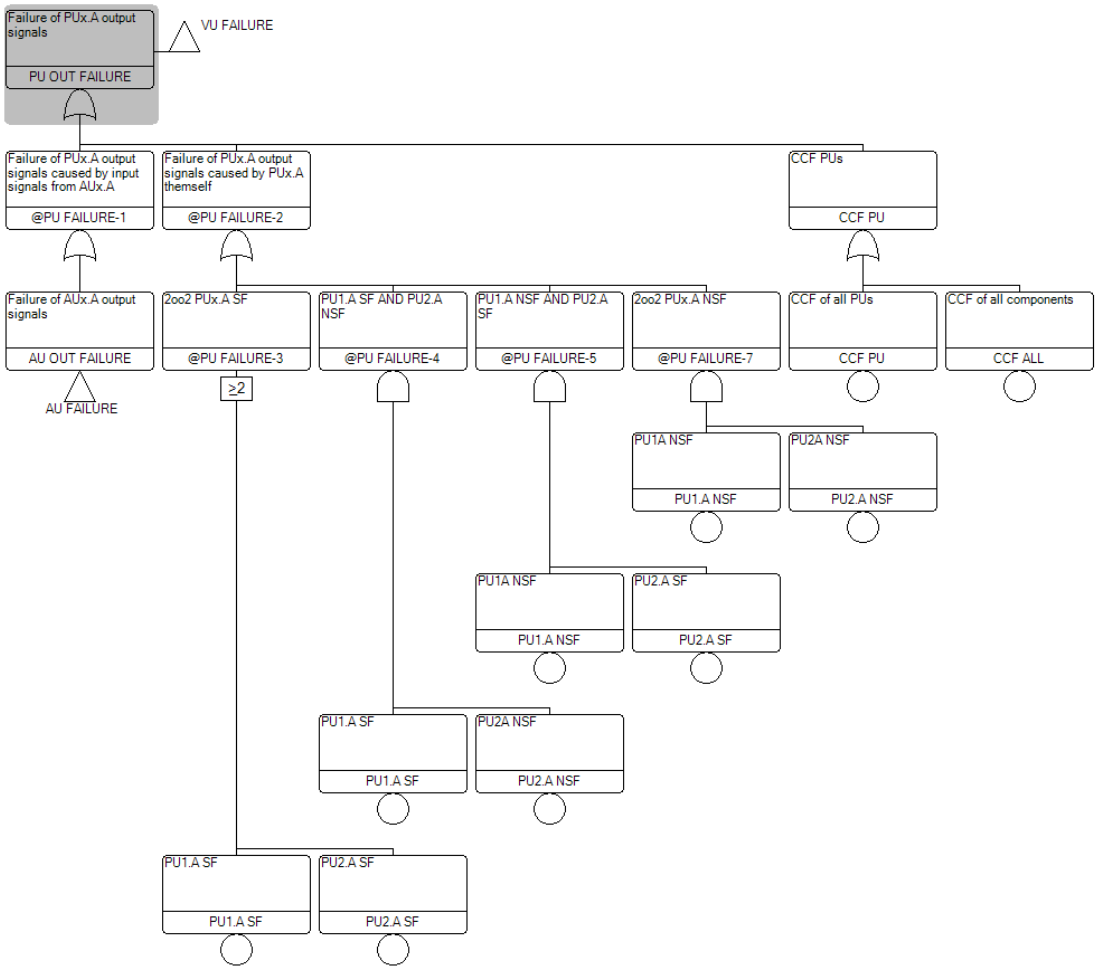

Abb. 5.4 Mögliche Ausfallkombinationen von PUs (vgl. Abb. 5.3) im Fehlerbaum des Modellsystems A222 (unter Berücksichtigung von GVA)

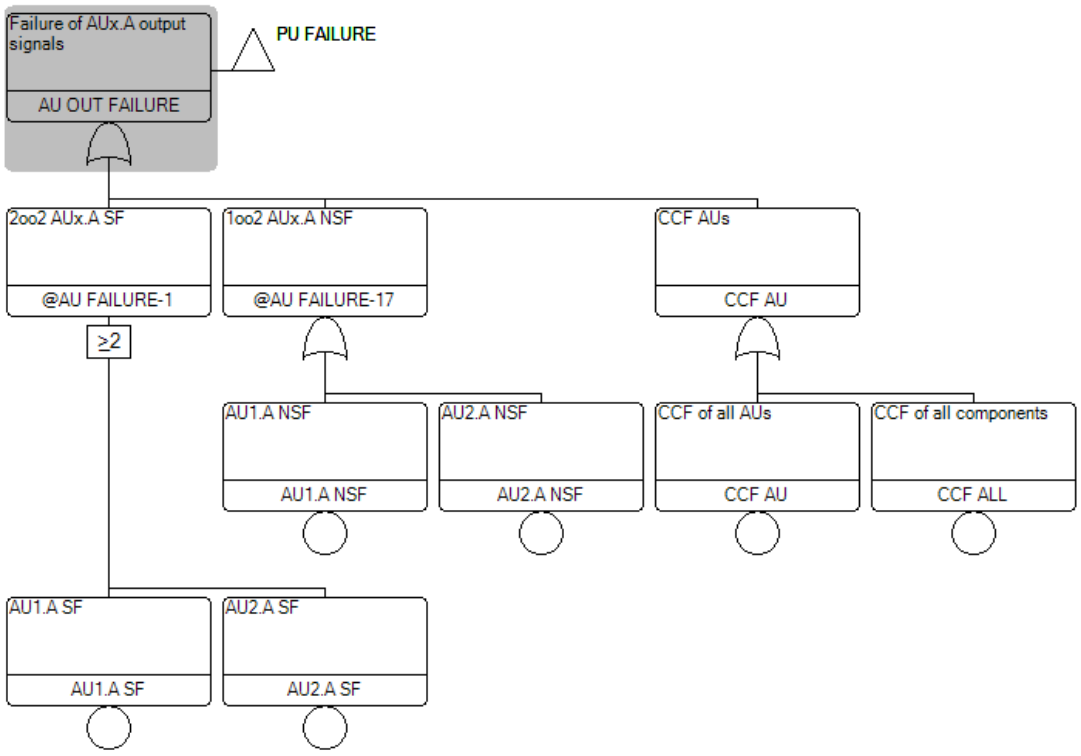

Abb. 5.5 Mögliche Ausfallkombinationen von AUs (vgl. Tab. 5.4) im Fehlerbaum des Modellsystems A222 (unter Berücksichtigung von GVA)

Bei Nominalwerten der verwendeten Parameter (z. B. einer Reparaturzeit von acht Stunden, einem vier-Wochen-Testrhythmus der Redundanzen und einem 5%-Anteil GVA an den Fehlerraten) ergeben sich die in Tab. 5.5 angegebenen Minimalschnitte des Modellsystems A222.

Tab. 5.5 Minimalschnitte (MCS - Minimal Cut Set) des Modellsystems A222 für Nominalwerte der verwendeten Parameter

Nr.	Wahrscheinlichkeit	%	Event 1	Event 2
1	5,60E-05	48,66	AU1.A NSF	
2	5,60E-05	48,66	AU2.A NSF	
3	7,46E-07	0,65	CCF VU	
4	7,46E-07	0,65	CCF ALL	
5	7,46E-07	0,65	CCF PU	
6	7,46E-07	0,65	CCF AU	
7	3,44E-08	0,03	AL NSF	
8	2,82E-08	0,02	AU1.A SF	AU2.A SF
9	1,58E-08	0,01	PU1.A SF	PU2.A SF

Nr.	Wahrscheinlichkeit	%	Event 1	Event 2
10	7,03E-09	0,01	PU1.A NSF	PU2.A SF
11	7,03E-09	0,01	PU1.A SF	PU2.A NSF
12	3,14E-09	0	PU1.A NSF	PU2.A NSF
13	3,14E-09	0	VU1.A NSF	VU2.A NSF
14	3,12E-09	0	VU1.A NSF	VU2.A SF
15	3,12E-09	0	VU1.A SF	VU2.A NSF
16	3,11E-09	0	VU1.A SF	VU2.A SF

Die berechnete Gesamtwahrscheinlichkeit des Top-Events („keine Auslösung im Anforderungsfall“: Motor startet nicht) beträgt $Q_{MCS} = 1{,}151 \cdot 10^{-4}$

Wie bereits zuvor erwähnt, werden die Ausfälle des Modellsystems A222 fast ausschließlich durch Einzelausfälle der AUs verursacht. Diese Schwäche lässt sich beseitigen, indem man in den PUs den eingestellten Grenzwert grundsätzlich mit dem Maximum der Eingangswerte (anstatt dem 2. Maximum) vergleicht. Für das modifizierte Modellsystem (A222 mod) ergeben sich dann die Minimalschnitte in Tab. 5.6.

Tab. 5.6 Minimalschnitte des Modellsystems A222 mod. Die Gesamtwahrscheinlichkeit eines Versagens beträgt $Q_{MCS} = 3{,}116 \cdot 10^{-6}$

Nr.	Wahrscheinlichkeit	%	Event 1	Event 2
1	7,46E-07	23,96	CCF AU	
2	7,46E-07	23,96	CCF ALL	
3	7,46E-07	23,96	CCF VU	
4	7,46E-07	23,96	CCF PU	
5	3,44E-08	1,1	AL NSF	
6	2,82E-08	0,91	AU1.A SF	AU2.A SF
7	1,58E-08	0,51	PU1.A SF	PU2.A SF
8	9,41E-09	0,3	AU1.A NSF	AU2.A SF
9	9,41E-09	0,3	AU1.A SF	AU2.A NSF
10	7,03E-09	0,23	PU1.A SF	PU2.A NSF
11	7,03E-09	0,23	PU1.A NSF	PU2.A SF
12	3,14E-09	0,1	AU1.A NSF	AU2.A NSF
13	3,14E-09	0,1	PU1.A NSF	PU2.A NSF
14	3,14E-09	0,1	VU1.A NSF	VU2.A NSF
15	3,12E-09	0,1	VU1.A NSF	VU2.A SF
16	3,12E-09	0,1	VU1.A SF	VU2.A NSF
17	3,11E-09	0,1	VU1.A SF	VU2.A SF

RiskSpectrum erlaubt auf Basis dieser Berechnung ebenfalls eine automatisierte Einschätzung der Sensitivität der Ergebnisse auf alle verwendeten Parameter. Hierzu muss im entsprechenden „FT Analysis Case“ im Reiter „Analysis“ die Berechnung der Sensitivitätsanalyse aktiviert werden. In den Spezifikationen kann dann ein sogenannter „Sensitivity Factor“ (oder kurz „*SensFactor*“) festgelegt werden. Als Standardwert ist hier ein Wert von 10 angenommen.

Für die Sensitivitätsanalyse wird jeder Parameter (einzeln) einmal durch den *SensFactor* geteilt, die Wahrscheinlichkeit des Top-Events berechnet, anschließend der jeweilige Nominalwert des Parameters mit dem *SensFactor* multipliziert und die Wahrscheinlichkeit des Top-Events erneut berechnet. Das Verhältnis der beiden Ergebnisse dieser Berechnungen wird in RiskSpectrum „Sensitivity“ (oder kurz „S“) genannt.

Dieser Zusammenhang soll an einem einfachen Beispiel verdeutlicht werden: Der Nominalwert der Ausfallrate der AUs (nichtselbstmeldend – NSF) im Modellsystem A222 beträgt

$$FR_{AU,NSF} = 8{,}26 \cdot 10^{-8}\ h^{-1}$$

Für diese Fehlerrate (und bei allen anderen Parametern auf Nominalwert) ergibt sich eine Gesamtausfallwahrscheinlichkeit von

$$Q_{MCS} = 1{,}151 \cdot 10^{-4}$$

Dividiert man jetzt (ausschließlich) die Ausfallrate $FR_{AU,NSF}$ durch den *SensFactor* = 10, so ergibt sich die geänderte Fehlerrate

$$FR_{AU,NSF,Low} = FR_{AU,NSF} / SensFactor = 8{,}26 \cdot 10^{-8}\ h^{-1} / 10 = 8{,}26 \cdot 10^{-9}\ h^{-1}$$

Die Berechnung der Gesamtausfallwahrscheinlichkeit mit diesem einen geänderten Parameter liefert

$$Q_{MCS,Low} = 1{,}429 \cdot 10^{-5}$$

Multipliziert man die (ursprüngliche) Ausfallrate mit dem *SensFactor* und führt die Berechnung der Gesamtausfallwahrscheinlichkeit erneut durch, so ergeben sich

$$FR_{AU,NSF,High} = FR_{AU,NSF} \cdot SensFactor = 8{,}26 \cdot 10^{-8}\ h^{-1} \cdot 10 = 8{,}26 \cdot 10^{-7}\ h^{-1} \quad (5.1)$$

und

$$Q_{MCS,High} = 1{,}122 \cdot 10^{-3}$$

Das Verhältnis der beiden Ausfallwahrscheinlichkeiten ist dann der in RiskSpectrum definierte Sensitivitätswert S:

$$S = \frac{Q_{MCS,High}}{Q_{MCS,Low}} = \frac{1{,}122 \cdot 10^{-3}}{1{,}429 \cdot 10^{-5}} \approx 78{,}52 \quad (5.2)$$

In diesem Fall führt also die Variation der Ausfallrate der AUs (NSF) um zwei Größenordnungen zu einer Änderung des Gesamtergebnisses von ebenfalls beinahe zwei Größenordnungen (genauer um den Faktor 79, s. o.). Dies ist in diesem Fall (A222) eine Folge der Tatsache, dass die Gesamtausfallwahrscheinlichkeit fast vollständig durch diese Ausfallrate dominiert wird (siehe Tab. 5.5).

Berechnungen dieser Art führt das RiskSpectrum-Programm automatisch für alle verwendeten Parameter durch. Für das Modellsystem A222 ergeben sich beispielsweise die in Tab. 5.7 dargestellten Sensitivitäten, deren erste Zeile der wie oben vorgestellten Beispielberechnung entspricht.

Tab. 5.7 Berechnete Sensitivitäten (RiskSpectrum)

Parameter	Sensitivität S	$Q_{MCS,High}$	$Q_{MCS,Low}$
FR AU NSF	78,50	1,12E-03	1,43E-05
Testintervall Red. 1	9,39	6,13E-04	6,53E-05
Testintervall Red. 2	9,39	6,13E-04	6,53E-05
Testintervall AL	1,26	1,42E-04	1,12E-04
Mittl. Reparaturzeit AU NSF	1,12	1,27E-04	1,14E-04
FR GVA AU	1,06	1,22E-04	1,14E-04
FR GVA VU	1,06	1,22E-04	1,14E-04
FR GVA ALL	1,06	1,22E-04	1,14E-04
FR GVA PU	1,06	1,22E-04	1,14E-04
Mittl. Reparaturzeit AU SF	1,02	1,18E-04	1,15E-04
FR AU SF	1,02	1,18E-04	1,15E-04

Parameter	Sensitivität S	$Q_{MCS,High}$	$Q_{MCS,Low}$
Mittl. Reparaturzeit PU SF	1,01	1,17E-04	1,15E-04
FR PU SF	1,01	1,17E-04	1,15E-04
FR AL NSF	1,00	1,15E-04	1,15E-04
Mittl. Reparaturzeit PU NSF	1,00	1,15E-04	1,15E-04
Mittl. Reparaturzeit VU NSF	1,00	1,15E-04	1,15E-04
FR PU NSF	1,00	1,16E-04	1,15E-04
FR VU NSF	1,00	1,15E-04	1,15E-04
FR VU SF	1,00	1,15E-04	1,15E-04
Mittl. Reparaturzeit VU SF	1,00	1,15E-04	1,15E-04
Mittl. Reparaturzeit AL NSF	1,00	1,15E-04	1,15E-04
Zeit bis erster Test AL	1,00	1,15E-04	1,15E-04
Zeit bis erster Test Red. 1	1,00	1,15E-04	1,15E-04
Zeit bis erster Test Red. 2	1,00	1,15E-04	1,15E-04

Im Folgenden wird davon ausgegangen, dass Änderungen des Ergebnisses von deutlich weniger als einer Größenordnung bei einer Parametervariation von zwei Größenordnungen (d. h. $S << 10$ für *SensFactor* = 10) auf eine geringe Sensitivität des jeweiligen Modellsystems bezüglich dieses Parameters hindeutet. Insbesondere bedeutet dies im Fall des Modellsystems A222, dass lediglich die Ausfallrate der AUs (für nichtselbstmeldende Fehler) und die Länge der Testintervalle für die einzelnen Redundanzen einen signifikanten Einfluss auf das Ergebnis haben. Ändert man beispielsweise alle Fehlerraten bis auf die Ausfallrate der AUs (NSF) auf „0“, so ergibt sich immer noch eine Gesamtausfallwahrscheinlichkeit von $Q_{MCS} = 1{,}120 \cdot 10^{-4}$, was sich vom ursprünglichen Ergebnis ($1{,}151 \cdot 10^{-4}$) um weniger als 3 % unterscheidet.

Neben den Ergebnissen aus den Berechnungen zu den Minimalschnitten liefert RiskSpectrum auch zeitabhängige Ergebnisse. Als Beispiel zeigt Abb. 5.6 den zeitlichen Verlauf der Wahrscheinlichkeit eines Versagens des betrachteten Systems im Anforderungsfall als Funktion der Zeit für ein Jahr (52 Wochen = 52·7 Tage = 52·7·24 Stunden = 8736 Stunden). In Abhängigkeit vom betrachteten Zeitraum sowie der Dauer der Testintervalle weicht das zeitabhängige Ergebnis dabei etwas von dem aus den Minimalschnitten ab, grundsätzlich gilt aber allgemein:

$$\lim_{t \to \infty} Q_{Mean} = Q_{MCS} \tag{5.3}$$

Im Folgenden werden daher, außer es ist ausdrücklich etwas anderes angegeben, Ergebnisse aus den Minimalschnittberechnungen herangezogen.

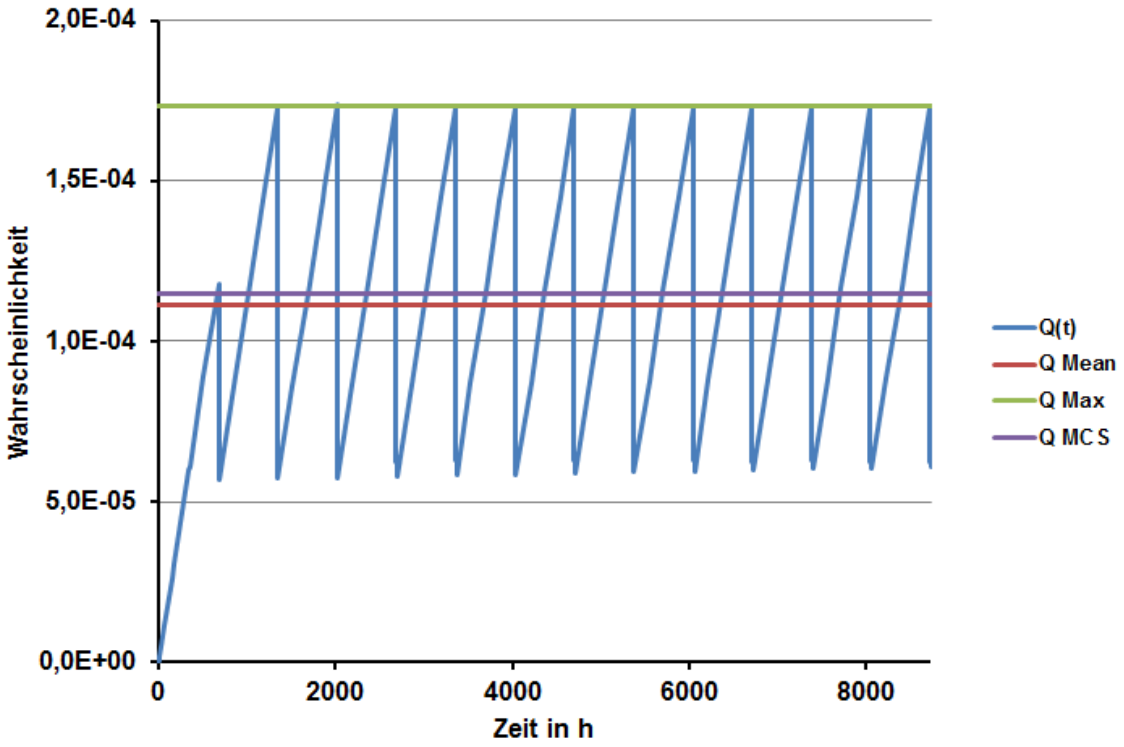

Abb. 5.6 Zeitlicher Verlauf der Fehlerwahrscheinlichkeit Q(t) für das Modellsystem A222

Anmerkung:
In dem Diagramm wurde der Maximalwert (Q Max) und der Mittelwert für den betrachteten Zeitraum (Q Mean) von RiskSpectrum berechnet. Zum Vergleich ist zusätzlich der Wert der Fehlerwahrscheinlichkeit aus den Minimalschnittberechnungen (Q MCS) eingezeichnet

Bevor in Abschnitt 5.4 die Ergebnisse verschiedener Sensitivitätsanalysen dargestellt werden, die unter Verwendung von RiskSpectrum durchgeführt wurden, wird in den Abschnitten 5.2 und 5.3 auf Ergebnisse von Analysen des Systems A222 eingegangen, die unter Verwendung des Markov-Programms RAMESU erzielt wurden.

Diese Abschnitte zeigen, dass Markov-Modelle als Ergänzung für diejenigen Systembeschreibungen eingesetzt werden können, die nur sehr schwer oder gar nicht mit den klassischen Fehlerbaumanalysen modelliert werden können. Dies könnten Systeme sein, wie sie in Abschnitt 5.3 beschrieben werden und zeitabhängige Veränderungen von Reparaturwahrscheinlichkeiten oder Alterungseffekte betreffen.

5.2 Markov-Analyse der Modellsysteme A222 und A222-mod

Für das im vorigen Abschnitt beschriebene System A222 soll zunächst gezeigt werden, dass die Modellierung des Systems durch ein Markov Modell die gleiche Ausfallwahrscheinlichkeit des Systems liefert wie über die Fehlerbaumanalyse mit RiskSpectrum. Während in der Fehlerbaumanalyse eine Log-Normalverteilung für die Reparaturzeiten spezifiziert wurde, sind die Reparaturzeiten im Markov-Modell exponential verteilt mit einer mittleren Reparaturzeit von 8 h. Ansonsten wurden für das Markov-Modell die in Abschnitt 3.1.2 definierten versetzten Tests und GVA-Ausfälle berücksichtigt. Die unterschiedlichen Verteilungen bzgl. der Reparaturzeiten haben keine relevanten Auswirkungen auf die berechneten Ausfallwahrscheinlichkeiten.

In der folgenden Abb. 5.7 werden sowohl die Nichtverfügbarkeit des Systems sowie die Beiträge der nichtselbstmeldenden Ausfälle durch AUs, PUs und VUs im zeitlichen Verlauf dargestellt. Entsprechende Analysen werden in Abb. 5.8 für das System A222-mod gezeigt, in dem statt des 2. Maximums der maximale Wert der AUs als Bewertungsgrundlage verwendet wurde.

Da sich die Systemnichtverfügbarkeiten in Abhängigkeit der Zeit ergeben, soll im Rahmen der Markov-Analysen zur Bewertung der Nichtverfügbarkeit des Systems nicht auf die Mittelwerte zwischen den Testzeitpunkten, sondern vielmehr auf die Maximalwerte der Nichtverfügbarkeiten Bezug genommen werden, die sich unmittelbar vor den jeweiligen Tests einstellen. Durch die zeitlichen Abhängigkeiten erscheint dies sinnvoller, da durch die Angabe der Maximalwerte eine obere Grenze der Nichtverfügbarkeit während des Beobachtungszeitraums genannt werden kann. Bei der Angabe der Mittelwerte der Nichtverfügbarkeiten wird nicht deutlich, wie weit der Mittelwert im betreffenden System überschritten werden kann und stellt deshalb eine ungenauere und zu optimistische Bewertung der Systemnichtverfügbarkeit dar.

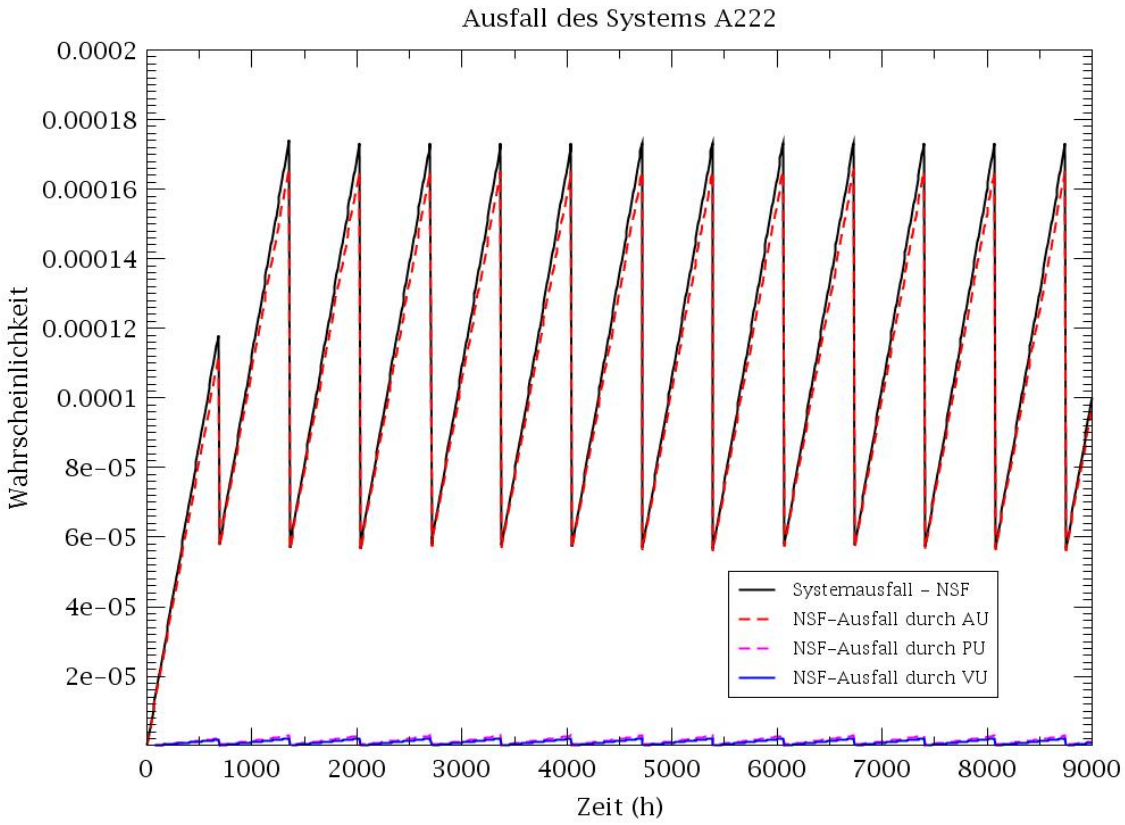

Abb. 5.7 Zeitabhängige Nichtverfügbarkeit des Systems A222 und Wahrscheinlichkeit eines nichtselbstmeldenden Ausfalls durch AU, PU und VU

Wie in Abb. 5.7 zu erkennen ist, trägt der Ausfall der AUs wesentlich zur Systemnichtverfügbarkeit bei. Die Ausfälle der PUs und VUs spielen dagegen eine eher untergeordnete Rolle, da die Verwendung des 2. Maximums als Bewertungskriterium dazu führt, dass sich das System bereits im ausgefallenen Zustand befindet, wenn entweder AU1 oder AU2 nichtselbstmeldend ausgefallen ist. Die maximale Wahrscheinlichkeit der Systemnichtverfügbarkeit liegt bei $1{,}73 \cdot 10^{-4}$ und tritt jeweils unmittelbar vor den geplanten monatlich versetzten Tests auf. Die maximalen Wahrscheinlichkeiten eines nichtselbstmeldenden Ausfalls der AUs liegt bei ca. $1{,}65 \cdot 10^{-4}$. D. h., das Ausfallverhalten der AUs trägt mit ca. 95 % zur Nichtverfügbarkeit des Systems bei. Die im zeitlichen Verlauf maximal erreichte Ausfallwahrscheinlichkeit der PUs bzw. VUs liegen jeweils unter $3 \cdot 10^{-6}$.

Das Ausfallverhalten des Systems ändert sich grundlegend, wenn anstatt des 2. Maximums der maximale Wert der AUs als Bewertungskriterium verwendet wird. In diesem Fall fällt das System durch die AUs aus, wenn entweder

- AU1 sich im nichtselbstmeldend ausgefallenen und AU2 sich im selbstmeldend ausgefallenen Zustand befindet oder
- AU1 sich im selbstmeldend ausgefallenen und AU2 sich im nichtselbstmeldend ausgefallenen Zustand befindet oder
- beide AUs sich im nichtselbstmeldend ausgefallenen Zustand befinden.

Für den Systemausfall, der durch die AUs verursacht wird, müssen sich beide AUs in einem ausgefallenen Zustand befinden, entweder beide nichtselbstmeldend oder eine selbstmeldend und die andere nichtselbstmeldend. Die Ausfallrate für einen nichtselbstmeldenden Ausfall ist mit $8{,}265 \cdot 10^{-8}\ h^{-1}$ relativ klein. Die vergleichsweise hohe Ausfallrate von $2{,}098 \cdot 10^{-8}\ h^{-1}$ für einen selbstmeldenden Ausfall wird dadurch kompensiert, dass ein selbstmeldender Ausfall einer Komponente sofort registriert wird und mit einer mittleren Reparaturzeit von 8 h repariert wird. Die sofort einsetzende Reparatur eines selbstmeldenden Ausfalls trägt dazu bei, dass auch die Wahrscheinlichkeit eines selbstmeldenden Ausfalls sehr gering ist.

In Abb. 5.8 sind die Nichtverfügbarkeit des Systems A222-mod und die Ausfallwahrscheinlichkeiten der AUs, PUs und VUs im zeitlichen Verlauf dargestellt. Außerdem wird auch der durch GVA verursachte Beitrag zur Systemnichtverfügbarkeit dargestellt.

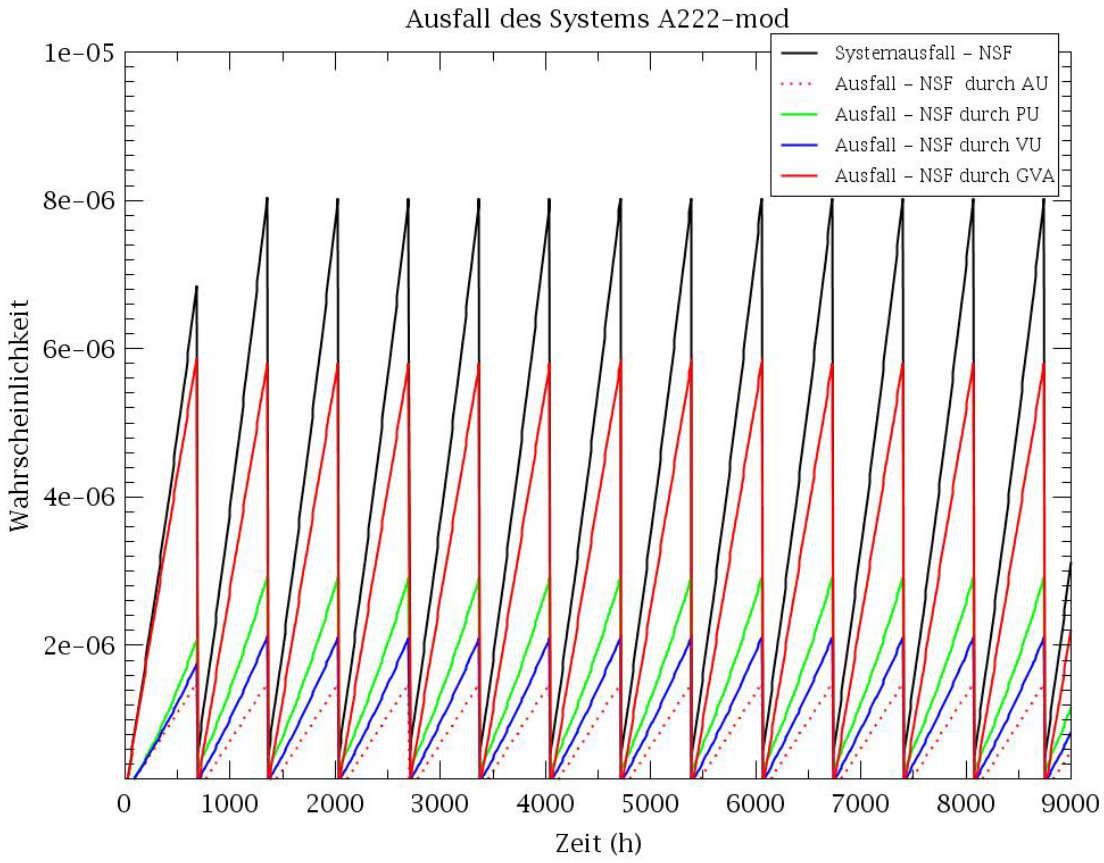

Abb. 5.8 Zeitabhängige Nichtverfügbarkeit des Systems in Abhängigkeit des Systems A222-mod und Wahrscheinlichkeitsbeiträge durch AU, PU, VU und GVA

Durch die Wahl des Maximalwertes der AUs als Bewertungskriterium für das System A222-mod kann die im zeitlichen Verlauf maximal erreichte Systemnichtverfügbarkeit auf ca. $8 \cdot 10^{-6}$ gegenüber dem System A222 gesenkt werden. Der größte Beitrag wird durch GVA verursacht, der zu ca. 70 % zur Systemnichtverfügbarkeit beiträgt. Danach folgen mit größerem Abstand die Beiträge der NSF-Ausfälle der PUs und VUs. Der NSF-Ausfall der AU, der im System A222 noch den größten Beitrag zur Systemnichtverfügbarkeit geliefert hat, trägt im System A222-mod am wenigsten zur Systemnichtverfügbarkeit bei.

Bei den Markov-Analysen wurde insbesondere Wert daraufgelegt, die Abhängigkeit der Systemzuverlässigkeit von der Zeit zu verdeutlichen. Da sich die Wahrscheinlichkeit, dass sich das System im ausgefallenen Zustand befindet, in Abhängigkeit der Zeit ergibt, ist die Frage zu diskutieren, ob es zur Bewertung der Nichtverfügbarkeit eines Systems sinnvoll ist, sich auf die Mittelwerte zwischen den Testzeitpunkten und sich

somit auf die mittlere Nichtverfügbarkeit des Systems zu beziehen. Der Nachteil der Mittelwertangabe der Nichtverfügbarkeit ist, dass die mittlere Nichtverfügbarkeit eines Systems in bestimmten Zeitintervallen unterschritten und in anderen Zeitintervallen überschritten wird. Bezieht man sich nur auf die mittlere Nichtverfügbarkeit bleibt die Ungewissheit, wie weit die mittlere Nichtverfügbarkeit im betreffenden System überschritten werden kann. Die mittlere Nichtverfügbarkeit stellt deshalb eine ungenauere und zu optimistische Bewertung der Nichtverfügbarkeiten der Systeme dar.

Bei den durchgeführten Markov-Analysen wurden nicht die mittleren Nichtverfügbarkeiten des Systems als Bewertungsgrundlage, sondern vielmehr die Maximalwerte der Systemnichtverfügbarkeiten genommen. Bei einigen Analysen haben sich die Maximalwerte der Systemnichtverfügbarkeit, die sich unmittelbar vor den jeweiligen Tests eingestellt haben, einem konstanten Wert angenähert. In anderen Analysen hat sich im zeitlichen Ablauf ein Trend zu höheren Maximalwerten gezeigt. In diesen Fällen, die sich insbesondere bei der Modellierung von Alterungsprozessen ergeben haben, wird das Maximum der Nichtverfügbarkeit eines Systems unmittelbar vor dem letzten Test vor Beobachtungsende erreicht.

Durch die zeitlichen Abhängigkeiten erscheint die maximale Nichtverfügbarkeit als Bewertungskriterium zumindest eine sinnvolle Zusatzinformation zur Angabe der mittleren Nichtverfügbarkeit zu sein, da durch die Angabe der Maximalwerte eine obere Grenze der Nichtverfügbarkeit während des Beobachtungszeitraums genannt werden kann.

5.3 Markov-Analyse zur Sensitivität von Reparaturwahrscheinlichkeiten und Alterungseffekten

In der Fehlerbaumanalyse wird von der Annahme ausgegangen, dass eine Komponente nach einem Test oder einer Reparatur so gut wie neu (‚As Good As New') ist. Diese für die Fehlerbaumanalyse charakteristische ‚As Good As New'-Annahme ist aber nicht in jedem Falle gerechtfertigt. Beispiele aus der Realität belegen, dass nach der Durchführung von Reparatur-, Instandhaltungs- und Wartungsarbeiten die betroffenen Komponenten durch menschliche Fehler in einem Zustand vorliegen können, der mit einer erhöhten Ausfallrate der Komponente verbunden ist oder bei dem die Reparatur nicht erfolgreich ist. Die ‚As Good As New'-Annahme der Fehlerbaumanalyse führt in solchen Fällen somit zu einer zu optimistischen Einschätzung der Reparaturmaßnahmen und zu einer Unterschätzung der Systemnichtverfügbarkeit.

Im Folgenden soll eine Situation modelliert werden, in der Reparaturen, die zu den jeweiligen Testzeitpunkten stattfinden, mit einer gewissen Wahrscheinlichkeit nicht erfolgreich durchgeführt werden. Die Auswirkung einer nicht erfolgreich durchgeführten Reparatur kann auf unterschiedliche Arten modelliert werden:

1. Die betroffene Komponente wird nach der Reparatur nicht als neu (‚As Good As New') betrachtet, sondern der Zustand der Komponente wird so berücksichtigt, als ob keine Reparatur stattgefunden hätte. In diesem Fall ändert sich die Ausfallrate der Komponente nicht. Durch den Wegfall bzw. die nicht erfolgreiche Reparatur verlängert sich das Zeitintervall, in dem die Ausfallrate der Komponente wirkt. Damit ist eine Erhöhung der Ausfallwahrscheinlichkeit des Systems verbunden.

2. Die Komponente befindet sich nach der Reparatur in einem Zustand, mit dem eine Erhöhung der Ausfallrate der Komponente verbunden ist. D. h., nach der Reparatur wird das weitere Ausfallverhalten der Komponente unter Verwendung der erhöhten Ausfallrate berechnet. In ähnlicher Weise, können auch Alterungen von Komponenten, die zu bestimmten Zeitpunkten einsetzen, berücksichtigt werden.

Im Folgenden wird für das System A222-mod untersucht, wie sich Reparaturen, die mit einer gewissen Wahrscheinlichkeit nicht erfolgreich durchgeführt werden, auf die Ausfallwahrscheinlichkeit des Systems auswirken.

Um zu demonstrieren, welche Modellierungen mit dem Markov-Programm RAMESU durchgeführt werden können, sollen die Auswirkungen folgender Situationen auf die Systemnichtverfügbarkeit dargestellt werden:

Fall 1: Es wird angenommen, dass die Reparaturen sowohl der Komponenten von Strang 1 (d. h. AU1, PU1, VU1) als auch die Reparaturen der Komponenten von Strang 2 (d. h. AU2, PU2, VU2) pro Test mit einer Wahrscheinlichkeit von jeweils 90 % erfolgreich durchgeführt werden. D. h., mit einer Wahrscheinlichkeit von 10 % wird davon ausgegangen, dass die Reparatur nicht erfolgreich ist, und die Komponenten des jeweiligen Stranges in ihrem Zustand bleiben, den sie vor dem Test hatten.

Fall 2: In der ersten Jahreshälfte (d. h. bis 4500 h) werden die Reparaturen der Komponenten von Strang 1 und Strang 2 zu jeweils 90 % erfolgreich durchgeführt. In der zweiten Jahreshälfte (d. h. nach 4500 h) werden die Komponenten von Strang 1 nur noch zu 70 % und die Komponenten von Strang 2 nur noch zu 60 % erfolgreich repariert.

Fall 3: Es wird angenommen, dass die Reparaturen der Komponenten von Strang 1 und Strang 2 im Rahmen der periodischen Tests zu 100 % erfolgreich repariert werden. Allerdings unterliegen die Raten für die nichtselbstmeldenden Ausfälle einer Alterung. In diesem Fall wird davon ausgegangen, dass sich ab einer Betriebszeit von 6500 h die Ausfallraten der Komponenten für die nichtselbstmeldenden Ausfälle von $8{,}265 \cdot 10^{-8}\ h^{-1}$ auf $5 \cdot 10^{-7}\ h^{-1}$ erhöhen.

In Abb. 5.9 wird die zeitabhängige Nichtverfügbarkeit des Systems bei 100%iger Reparaturwahrscheinlichkeit der Systemnichtverfügbarkeit gegenübergestellt, bei der Reparaturwahrscheinlichkeit von 90 % für die Komponenten der jeweiligen Stränge vorliegt.

Es erhöhen sich die Maximalwerte der Ausfallwahrscheinlichkeit des Systems unmittelbar vor den Testzeitpunkten von ca. $8 \cdot 10^{-6}$ auf ca. $1{,}5 \cdot 10^{-5}$, wenn für die Wahrscheinlichkeit einer erfolgreichen Reparatur ein Wert von 90 % anstatt 100 % angenommen wird. Außerdem liegt die Nichtverfügbarkeit des Systems unmittelbar nach einem Test auf einem entsprechend höheren Niveau. Sowohl die Maximalwerte der Systemnichtverfügbarkeit unmittelbar vor den Tests als auch die Minimalwerte unmittelbar nach den Testzeitpunkten bleiben im zeitlichen Verlauf auf einem konstanten Niveau.

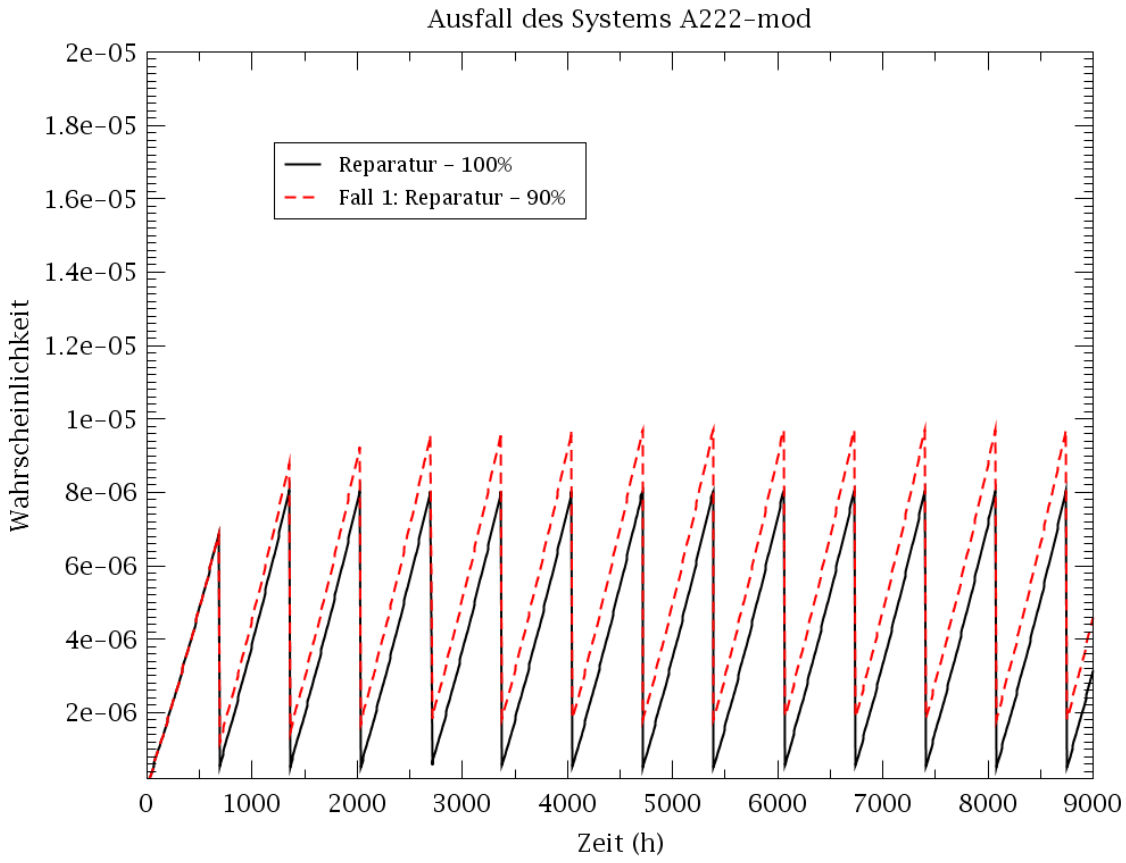

Abb. 5.9 Zeitabhängige Nichtverfügbarkeit des Systems in Anhängigkeit der Wahrscheinlichkeit, dass eine Reparatur erfolgreich durchgeführt wird

In Abb. 5.10 wird der zeitliche Verlauf der Systemnichtverfügbarkeit für den Fall 2 (Verringerte Wahrscheinlichkeit einer erfolgreichen Reparatur in der zweiten Jahreshälfte) und für den Fall 3 (erhöhte Ausfallrate eines nichtselbstmeldenden Ausfalls nach 6500 h Betriebszeit) dargestellt.

Der Fall 2 kann gewissermaßen als eine Alterung bzgl. der Reparaturmöglichkeit betrachtet werden, die nach der ersten Jahreshälfte (bei 4500 h) eintritt. Die verringerte Reparaturwahrscheinlichkeit für die Komponenten könnte sich z. B. daraus ergeben, dass die Schädigungen der Komponenten mit zunehmender Zeit immer komplexer werden und schwieriger zu reparieren sind.

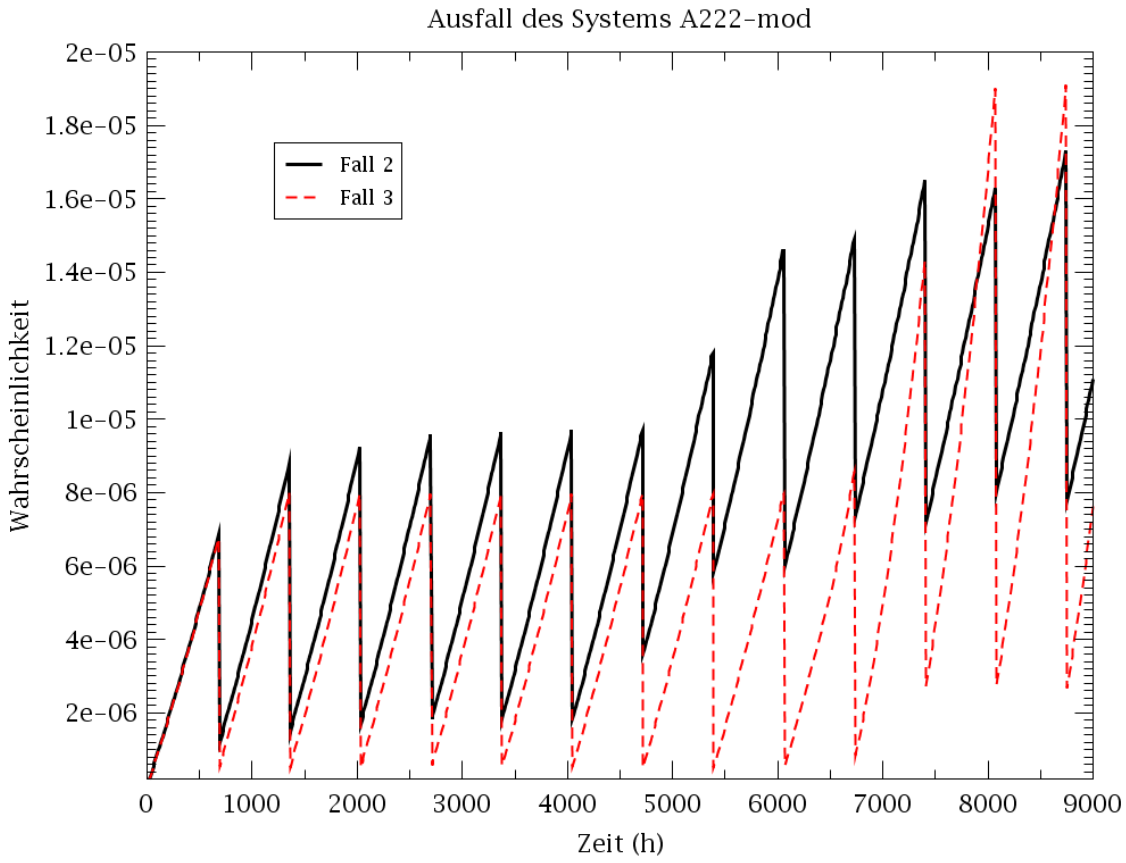

Abb. 5.10 Zeitabhängige Nichtverfügbarkeit des Systems in Abhängigkeit von Alterungseffekten

Aufgrund der verringerten Reparaturwahrscheinlichkeiten in der 2. Jahreshälfte, steigen die Maximalwerte der Systemnichtverfügbarkeiten nach einer Betriebszeit von 4500 h merklich an, wie aus Abb. 5.10 aus dem Verlauf der schwarzen Kurve deutlich wird. Zwischen 4500 h und dem Beobachtungsende (9000 h) weisen die Spitzenwerte der Systemnichtverfügbarkeit dabei eine steigende Tendenz auf. Während in den ersten 4500 h Betriebszeit die Nichtverfügbarkeit bei einer 90%igen Reparaturwahrscheinlichkeit den maximalen Wert von ca. 1.E-5 erreicht, steigt durch die Verringerung der Reparaturwahrscheinlichkeit auf 70 % für Strang 1 bzw. 60 % für Strang 2 der maximale Wert der Nichtverfügbarkeit des Systems in der Zweit zwischen 4500 h und 9000 h bis auf ca. 1.7E-5 an. Dieser maximale Wert wird kurz vor dem letzten Test im Beobachtungszeitraum erreicht.

Aufgrund der alterungsbedingten erhöhten Ausfallrate steigen im Fall 3 die Maximalwerte der Systemnichtverfügbarkeit nach 6.500 Betriebsstunden deutlich an. Während in den ersten 6.500 h die Maximalwerte $8 \cdot 10^{-6}$ nicht überschreiten, liegt der Maximalwert kurz vor Ende der Beobachtungzeit bei ca. $1{,}9 \cdot 10^{-5}$.

Durch die Analysen des Systems A222 in den Abschnitten 5.2 und 5.3 wurde gezeigt, dass Systemanalysen unter Verwendung von Markov-Modellen als sinnvolle Ergänzung zur Fehlerbaumanalyse eingesetzt werden können. Dies gilt insbesondere für Systemkonfigurationen, die nur sehr schwer oder nur mit groben vereinfachenden Annahmen mit dem klassischen Fehlerbaum zu modellieren sind. Solche Systemkonfigurationen betreffen z. B. Systeme, in denen Alterungseffekte von Komponenten berücksichtigt werden sollen.

5.4 Sensitivitätsanalysen mittels RiskSpectrum-Programm

In den folgenden Unterkapiteln werden die Sensitivitäten der Modellsysteme auf Änderungen sämtlicher für die Berechnung verwendeter Parameter untersucht. Dabei werden zwei Ziele verfolgt. Zum einen soll untersucht werden, dass welche Parameter bzw. welche Parameterwerte für die modellbasierte Ermittlung der Systemzuverlässigkeit bedeutend sind. Zum anderen soll die Eigenschaften (z. B. Robustheit) der unterschiedlichen Architekturen der Modellsysteme hinsichtlich Variation von realitätsnahen Parametern (z. B. Länge von Testintervallen, Reparaturzeiten) oder von künstlich festgelegten Parametern (u. a. GVA-Annahmen) untersucht werden.

5.4.1 Sensitivität der Modellsysteme hinsichtlich der Ausfallraten

Die Untersuchung der Sensitivität der Modellsysteme auf Veränderung der angenommenen Ausfallraten („FR“ – „Failure Rates“) erfolgt unmittelbar mit Hilfe des im Abschnitt 5.1 vorgestellten Sensitivitätsfaktors („*SensFactor*“) von RiskSpectrum. Tab. 5.8 listet die Sensitivität S aller Ausfallraten für sämtliche Modellsysteme auf. Die höchste Sensitivität S hat die Ausfallrate von nichtselbstmeldenden Ausfällen von AUs („FR AU NSF“) im Modellsystem A222. Wie im vorangegangenen Abschnitt bei der Einführung des Sensitivitätsfaktors gezeigt, liegt das in diesem Fall hauptsächlich daran, dass die Gesamtausfallwahrscheinlichkeit des Modellsystems A222 fast völlig von dieser (Einzel-)Fehlerrate dominiert wird. Ändert man in den beiden PUs des Modellsystems A222 lediglich die Auswahl des 2. Maximums in eine grundsätzliche Auswahl des („1.“) Maximums (Modellsystem A222-mod), so wird diese Schwäche beseitigt.

Die relativ hohen Sensitivitäten der Ausfallraten der VU („FR VU NSF“ und „FR VU SF“) des Modellsystems A133 haben ähnliche Ursachen. Da dieses System nur über eine einzige VU verfügt, führen hier ebenfalls Einzelfehler bereits zu einem

Gesamtausfall, weswegen diese Parameter ein hohes Gewicht bei der Bestimmung der Gesamtausfallwahrscheinlichkeit haben.

Tab. 5.8 Die Sensitivität S der Modellsysteme (RiskSpectrum) hinsichtlich Änderungen der Ausfallraten (für einen *SensFactor* von 10)

Parameter	**A2MC(2)44**	**A2MC(1)33**	**A133B133**	**A133A133**	**A333**	**A133**	**A222-mod**	**A222**
FR AL NSF	1,11	1,11	15,30	1,11	1,11	1,00	1,98	1,00
FR AU NSF	1,00	1,97	1,01	1,00	1,95	1,02	1,55	78,50
FR AU SF	1,00	1,27	1,00	1,00	1,27	1,01	1,16	1,02
FR PU NSF	1,00	1,68	1,01	1,00	1,67	1,01	1,15	1,00
FR PU SF	1,00	1,00	1,00	1,00	1,00	1,00	1,12	1,01
FR VU NSF	-	-	3,70	1,04	1,76	13,40	1,12	1,00
FR VU SF	1,00	1,22	2,65	1,03	1,38	6,94	1,11	1,00

Ein gewisser Sonderfall ist die relativ hohe Sensitivität des Modellsystems A133B133 gegenüber Änderung der Ausfallrate der AL („FR AL NSF“). Wie man in den nachfolgenden Abschnitten sehen kann, ist die Gesamtausfallwahrscheinlichkeit dieses Modellsystem in weiten Bereichen deutlich kleiner als für alle anderen Modellsysteme. Dies führt dazu, dass die bewusst sehr kleine (und willkürlich festgelegte) Ausfallrate der AL (mit $1 \cdot 10^{-10}$ h^{-1}) eine zunehmende Bedeutung bekommt (da hier ja auch ein Einzelausfall einen Gesamtausfall verursacht). In diesem Sinne ist die Sensitivität des Systems gegenüber dieses Parameters eher als Qualitätsmerkmal des Modellsystems zu verstehen, insbesondere da die AL in allen Modellsystemen nicht Teil der eigentlich untersuchten digitalen Leittechnik-Architekturen ist.

Darüber hinaus zeigen die sehr kleinen Sensitivitäten der übrigen Ausfallraten, dass deren Bestimmung hinreichend genau ist, da selbst größere Ungenauigkeiten (z. B. um den Faktor 2) keinen signifikanten Einfluss auf die erzielten Ergebnisse haben.

5.4.2 Sensitivität der Modellsysteme hinsichtlich der Reparaturzeiten

Um den Einfluss der angenommenen Reparaturzeiten (der Komponenten) auf die Ausfallwahrscheinlichkeiten der Modellsysteme zu untersuchen, wurde die Reparaturzeit sukzessive von 0 h bis auf über 500 h (jeweils für alle AUs, PUs und VUs sowie beide Ausfallarten (NSF und SF) gemeinsam) angehoben. Grundsätzlich steigt dabei die Wahrscheinlichkeit eines Ausfalls für alle Modellsysteme mit längeren Reparaturzeiten an (Abb. 5.11).

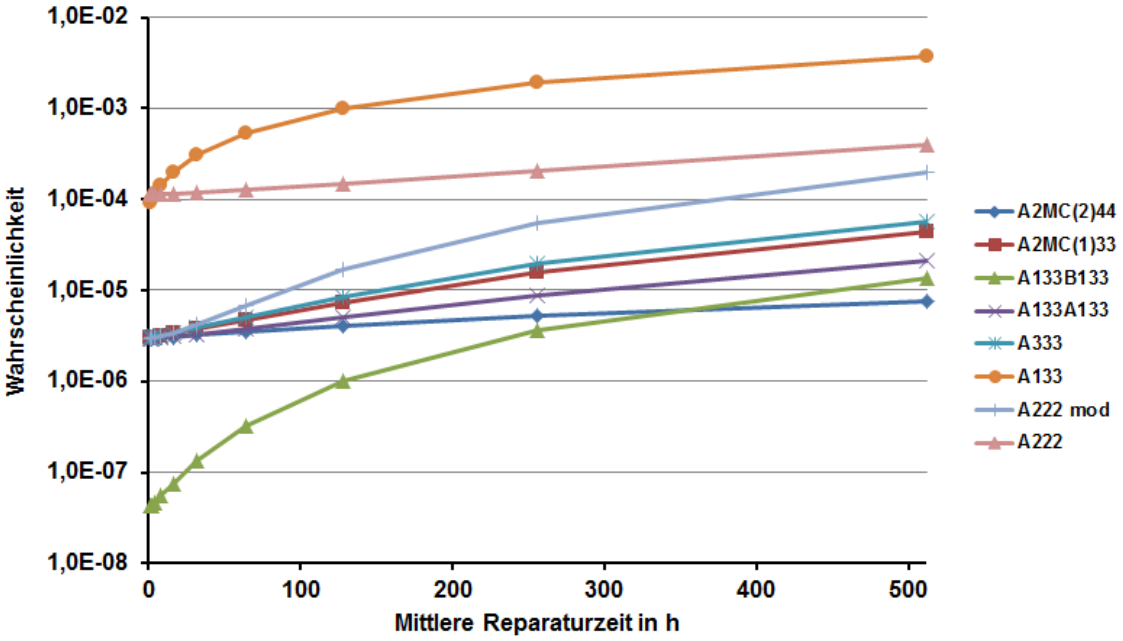

Abb. 5.11 Sensitivität der Modellsysteme hinsichtlich der mittleren Reparaturzeiten

Die relative Änderung der Ausfallwahrscheinlichkeit mit zunehmender Reparaturzeit ist für das Modellsystem A133B133 am größten, aber nicht wesentlich. Dieses Modellsystem büßt seine Spitzenstellung als zuverlässigstes Modellsystem (mit der kleinsten Ausfallwahrscheinlichkeit) erst oberhalb von ca. 350 h (> 2 Wochen) mittlerer Reparaturzeit ein, was deutlich oberhalb der realistischerweise zu erwartenden Reparaturzeiten liegen dürfte.

Daneben wurde ebenfalls untersucht, ob die Varianz der Reparaturzeiten (d. h. deren Streuungsbreite und Asymmetrie) einen Einfluss auf die Ergebnisse hat. Es zeigt sich, dass die Varianz für alle mittleren Reparaturzeiten und Modellsysteme keinerlei Einfluss auf die Gesamtausfallwahrscheinlichkeiten hat. Die Abb. 5.13 und Abb. 5.13 zeigt

dies repräsentativ für das Modellsystem A222, identische Ergebnisse liefern ebenso Berechnungen mit allen anderen Modellsystemen.

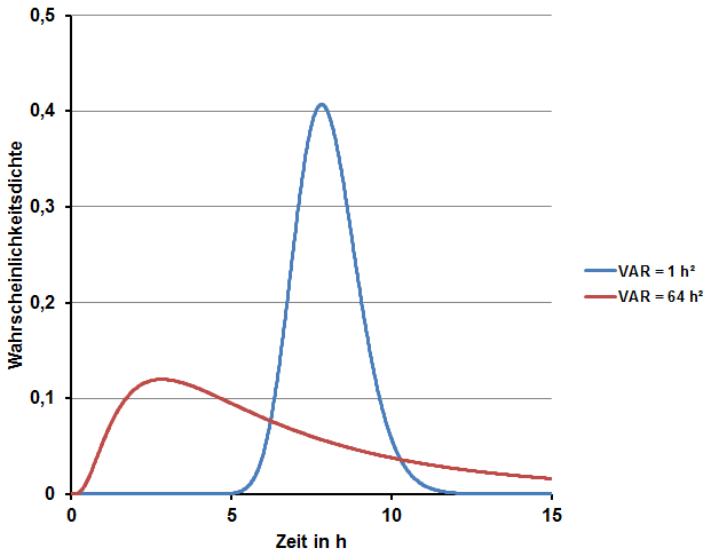

Abb. 5.12 Beispiele für Wahrscheinlichkeitsdichtefunktionen von Reparaturzeiten

Anmerkung:
Beide (logarithmisch normalverteilte) Kurven repräsentieren eine mittlere Reparaturzeit von 8 h, haben allerdings sehr unterschiedliche Varianzen (blau: 1 h², rot: 64 h²).

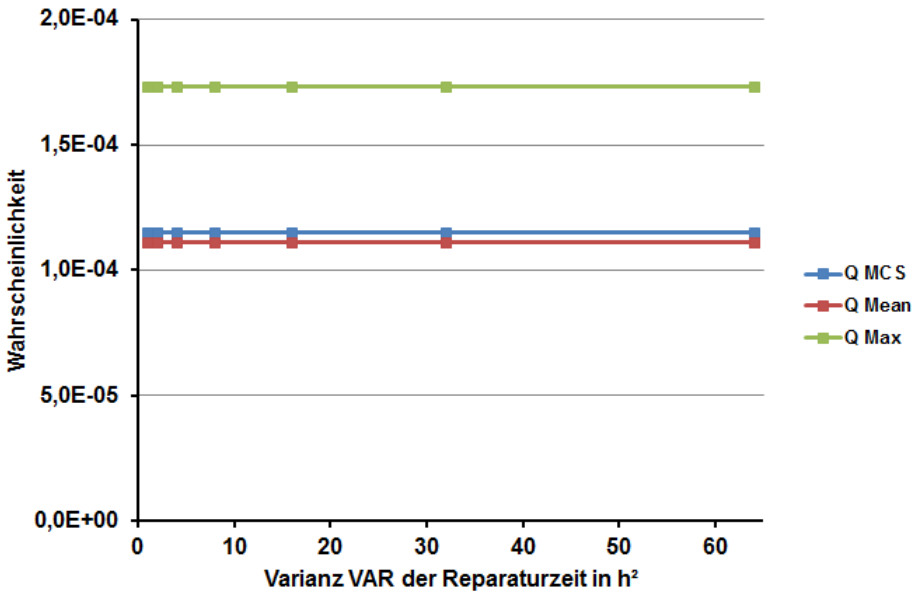

Abb. 5.13 Ausfallwahrscheinlichkeiten des Modellsystems A222 für eine mittlere Reparaturzeit von 8 h bei unterschiedlichen Varianzen

Anmerkung:
Maximale (Q Max), mittlere (Q Mean) und aus Minimalschnitten bestimmte (Q MCS) Ausfallwahrscheinlichkeiten des Modellsystems

5.4.3 Sensitivität der Modellsysteme hinsichtlich der Testintervalle

Für die Untersuchung der Sensitivität der Modellsysteme auf die Dauer der Testintervalle (Zeiträume zwischen zwei (wiederkehrenden) Prüfungen) wurden die folgenden Annahmen gemacht:

Ist beispielsweise für ein zweifach redundantes Modellsystem (A222) ein Testintervall von vier Wochen angegeben, so wird alle vier Wochen eine der beiden Redundanzen (abwechselnd) überprüft. Dabei werden sämtliche nichtselbstmeldende Ausfälle in der überprüften Redundanz und sämtliche redundanzübergreifende GVA entdeckt und entsprechend der angenommenen Reparaturzeiten repariert. Zusätzlich wird bei jeder Prüfung (jeder Redundanz) die AL zusätzlich überprüft und gegebenenfalls ebenfalls repariert. Bei dreifach oder vierfach redundanten Systemen bedeutet das, dass jede einzelne Redundanz z. B. bei einer monatlichen Prüfung nur alle drei bzw. vier Monate überprüft wird.

Es zeigt sich, dass alle Modellsysteme gleichartig und erwartungsgemäß mit einer höheren Ausfallwahrscheinlichkeit auf die Verlängerung der Testintervalle reagieren (siehe Abb. 5.14).

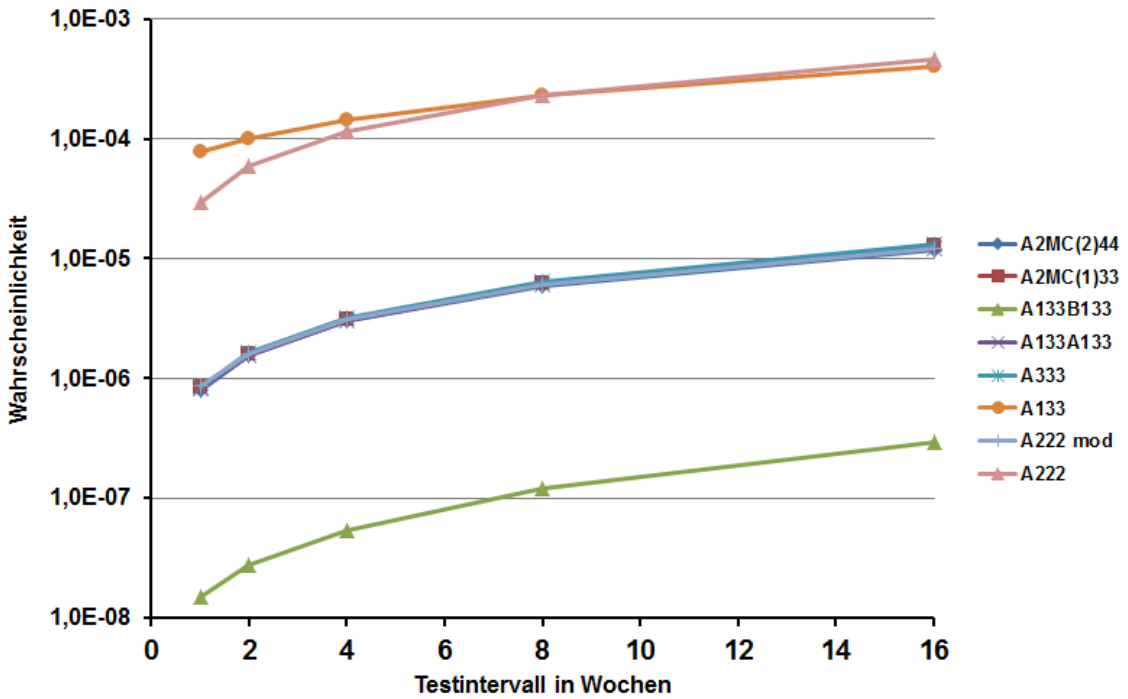

Abb. 5.14 Sensitivität der Modellsysteme hinsichtlich der Testintervalle

5.4.4 Sensitivität der Modellsysteme hinsichtlich des GVA-Anteils

Der variierende Anteil gemeinsam verursachter Ausfälle (GVA) an den Ausfallraten der Einzelkomponenten wurde wie folgt berechnet:

Ausgangspunkt ist eine bekannte oder angenommene Fehlerrate (in der Realität z. B. aus der Betriebserfahrung oder in unserem Fall aus einer Modellierung eines Systems /HEJ 15/) für eine bestimmte Komponenten- und Ausfallart (z. B. nichtselbstmeldend (NSF)). Ein unbekannter Anteil dieser Ausfallrate geht auf GVA zurück. Für diesen Anteil (x %) wurde jeweils angenommen, dass er zur Hälfte auf GVA des Gesamtsystems (d. h. aller Komponenten) und zur anderen Hälfte auf GVA dieses bestimmten Typs von Komponente (z. B. AUs) beruht.

Konkret bedeutet dies z. B. für Komponenten des Typs AU für einen angenommenen Anteil von 5 % GVA bei einer Fehlerrate von $8{,}70 \cdot 10^{-8}\ h^{-1}$:

Ausfallrate Einzelfehler von AUs:	$8{,}27 \cdot 10^{-8}\ h^{-1}$ (95 %)
Ausfallrate GVA von AUs:	$2{,}17 \cdot 10^{-9}\ h^{-1}$ (2,5 %)
Ausfallrate GVA Gesamtsystem:	$2{,}17 \cdot 10^{-9}\ h^{-1}$ (2,5 %)

Für einen GVA-Anteil von 10 % ergeben sich vergleichsweise folgende Ausfallraten:

Ausfallrate Einzelfehler von AUs:	$7{,}83 \cdot 10^{-8}\ h^{-1}$ (90 %)
Ausfallrate GVA von AUs:	$4{,}35 \cdot 10^{-9}\ h^{-1}$ (5 %)
Ausfallrate GVA Gesamtsystem:	$4{,}35 \cdot 10^{-9}\ h^{-1}$ (5 %)

Da die Gesamtfehlerrate für die einzelnen Komponenten bei unterschiedlichen GVA-Anteilen konstant bleibt, bedeutet dies für größere GVA-Anteile gleichzeitig, dass die Ausfallraten für Einzelfehler kleiner werden.

In der Regel steigt die Wahrscheinlichkeit eines Systemversagens deutlich mit dem Anteil der GVA für die verschiedenen Modellsysteme. Ausnahmen bilden hier die beiden Modellsysteme, deren (relativ hohe) Gesamtausfallwahrscheinlichkeit durch Einzelfehler dominiert werden (A222 und A133), und das Modellsystem A133B133. Deren Ausfallwahrscheinlichkeiten bleiben annähernd konstant (siehe Abb. 5.15), allerdings für die beiden Modellsysteme A222 und A133 auf vergleichsweise hohem Niveau. Lediglich das Modellsystem A133B133 hat eine für alle GVA-Anteile konstant niedrige Aus-

fallwahrscheinlichkeit auf Grund seines Aufbaus aus relativ unkomplizierten, aber diversitären Teilsystemen.

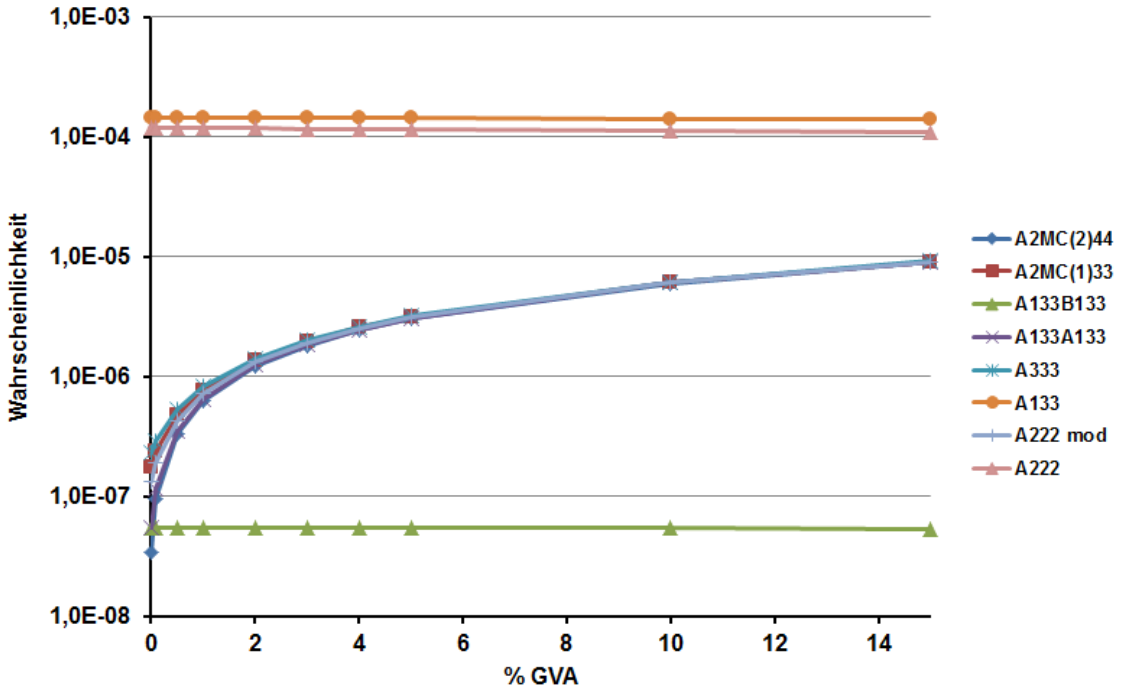

Abb. 5.15 Sensitivität der Modellsysteme hinsichtlich des GVA-Anteils

Zwar ist bisher nicht genau bekannt, wie groß genau der Anteil von GVA für digitale Leittechniksysteme ist, aber wie Abb. 5.15 deutlich zeigt, haben Architekturen mit dem Einsatz diversitärer Leittechnik (Annahme: keine GVA zwischen diversitärer Hardware bzw. Software) in der bereits bei sehr kleinen GVA-Anteilen (< 1 %) einen deutlichen Vorteil, auch gegenüber sehr komplexen und hochredundanten Systemen, wie z. B. Modellsystem A2MC(2)44.

6 Zusammenfassung und Schlussfolgerungen

Im Rahmen des Vorhabens 3615R01343 „Entwicklung und Erprobung der Werkzeuge zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik“ wurden umfangreiche Arbeiten zur Modellierung von unterschiedlichen Architekturen digitaler Leittechniksysteme mittels Fehlerbaum- und Markov-Prozess-Methoden durchgeführt. Für die Markov-Prozess-Analysen wurde das GRS-Programm RAMESU (**R**eliability **A**nalysis of **M**arkov-Models **E**xtended by **S**ensitivity and **U**ncertainty Analysis) eingesetzt.

Des Weiteren wurden auf der Basis der modellbasierten Vorgehensweise Sensitivitätsuntersuchungen durchgeführt, wobei unterschiedliche Parameter (u. a. Zuverlässigkeitskennwerte, Architektur-Aspekte, Test- und Reparaturstrategien) variiert wurden. Die Zwischenergebnisse der Analysen und periodische Vergleiche beider Analyseansätze (Fehlerbaumanalyse vs. Markov-Prozess-Analysetool RAMESU) trugen dazu bei, die Modellierungstechniken und die Interpretation der Ergebnisse zu verbessern.

Die Sensitivitätsanalysen lieferten folgende allgemeine Erkenntnisse:

- Die Sensitivität der Modellsysteme gegenüber der Variation von Ausfallraten einzelner Komponenten hat erwartete Auswirkungen auf die Gesamtzuverlässigkeit der Systemfunktion und ist damit eher als Qualitätsmerkmal des analysierten Modellsystems zu verstehen und weniger geeignet unterschiedliche Architekturen zu vergleichen.
- Grundsätzlich steigt die Wahrscheinlichkeit eines Systemausfalls für alle Modellsysteme mit längeren Reparaturzeiten an, wobei Architekturen mit höherer Redundanz der Signalverarbeitung (ohne Berücksichtigung der AL-Logik) wesentlich unempfindlicher auf die Variation von Reparaturzeiten reagieren. Es zeigte sich auf ähnliche Weise, dass alle Modellsysteme gleichartig und erwartungsgemäß mit einer höheren Ausfallwahrscheinlichkeit auf die Verlängerung der Testintervalle reagieren, wobei Architekturen mit höherer Redundanz grundsätzlich unempfindlicher auf die Variation der Testintervalle einzelner Teilsysteme reagieren.
- Die Sensitivitätsanalyse hinsichtlich GVA zeigte auf, dass die Wahrscheinlichkeit eines Systemversagens generell deutlich mit dem Anteil der GVA steigt. Eine Ausnahme stellte das Modellsystem A133B133 dar, dessen Architektur aus diversitären Teilsystemen (Annahme: vollständige Diversität der Hard- und Software) be-

stand. Dieses wies eine für alle GVA-Anteile konstant niedrige Ausfallwahrscheinlichkeit auf. Ungeachtet der Tatsache, dass bisher keine gesicherten Erkenntnisse hinsichtlich des Anteils von GVA für digitale Leittechniksysteme existieren, haben diese Untersuchungen gezeigt, dass diversitäre Leittechnikarchitekturen bereits bei sehr kleinen GVA-Anteilen (< 1 %) einen deutlichen Vorteil, auch gegenüber sehr komplexen und hochredundanten Systemen haben.

Es stellte sich heraus, dass mittels der Werkzeuge der Fehlerbaumanalyse (u. a. separate Ausfalleffektanalyse der nicht-binären Logik, Fehlerbaummodellierung, Analyse der Minimalschnitte, integrierte Sensitivitätsanalyse der RiskSpectrum-Software) sehr effizient eine Vielzahl unterschiedlicher Architekturen digitaler Leittechnik modelliert und analysiert werden kann. Damit lassen sich auch vielfach redundante Architekturen moderner digitaler Leittechnik mit vielen Komponenten untersuchen, wobei auch die GVA in der Hard- und Software nachvollziehbar berücksichtigt werden können.

Mit Hilfe der der Markov-Methode (RAMESU) wurden Untersuchungen für Systemkonfigurationen durchgeführt, bei denen dynamische Veränderungen von Randbedingungen für das System auftreten, z. B. in Form von wechselseitigen Umschaltungen von Komponenten, die zu bestimmten Zeitpunkten mit gewissen Wahrscheinlichkeiten oder in Form von Alterungsprozessen im zeitlichen Ablauf auftreten können. Die Untersuchungen haben gezeigt, dass unter Verwendung des Markov-Programms RAMESU solche dynamischen Aspekte des Systemverhaltens modelliert und analysiert werden konnten. Des Weiteren können in RAMESU zusätzlich auch Unsicherheiten bzgl. aller Modellparameter (z. B. Ausfallraten von Komponenten, Reparaturzeiten und Wahrscheinlichkeiten der singulären Matrizen) berücksichtigt werden.

Für Sensitivitätsanalysen, die den Einfluss unterschiedlicher Systemarchitekturen quantifizieren sollen, ist die Verwendung des Markov-Programms dann vorteilhaft, wenn dabei auch spezielle dynamische Eigenschaften des Systems analysiert werden sollen, die mit der Fehlerbaumanalyse nur schwierig zu berücksichtigen sind.

Der Nachteil der Markov-Modell-Analyse besteht darin, dass die Modellierung größerer Systeme schnell an ihre Grenzen stößt. Die Ursache liegt darin, dass der Zustandsraum eines Systems mit wachsender Zahl an Komponenten exponentiell anwächst und somit sehr schnell zu einer Größenordnung von Zuständen führt, die auch mit einem Rechenprogramm nicht mehr praktikabel zu bearbeiten ist. In der aktuellen Entwicklungsstufe ist das GRS-Programm RAMESU in der Lage, Systeme mit ca. 20 Kompo-

nenten zu modellieren, bei denen der Zustandsraum bereits auf mehrere hunderttausend Zustände anwachsen kann. Die Anzahl der Übergänge ist in der Regel dabei noch wesentlich höher.

Um die Vorteile des Markov-Programms auch für größere Systeme nutzbar zu machen, wäre die Entwicklung eines Konzepts zur Erweiterung des Programms RAMESU sinnvoll, um es auch für die Analyse größerer Systeme einsetzen zu können.

Die Detailergebnisse aller Modellsysteme (u. a. Ausfalleffektanalyse, Bestimmung von Ausfallraten, Fehlerbäume) sind auf einer CD zusammengefasst und werden bei Bedarf zur Verfügung gestellt.

Es ist geplant, die Weiterentwicklung der Analysemethoden und -werkzeuge in einem Nachfolgevorhaben fortzuführen.

Literaturverzeichnis

/ALD 06/ Aldemir T. et al.
Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments
NUREG/CR-6901,
Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, Washington, February 2006.

/BRO 88/ Brox, T.:
Ein Programmpaket für Zuverlässigkeitsberechnungen mit Markov-Modellen, GRS-A-1457,
Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, 1988.

/DIN 06/ Deutsches Institut für Normung (DIN) e. V.
Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)
DIN IEC 60812:2006; November 2006.

/DIN 07/ Deutsches Institut für Normung (DIN) e. V.
Fehlzustandsbaumanalyse
DIN IEC 61025:2006; August 2007.

/DIN 07a/ Deutsches Institut für Normung (DIN) e. V.
Anwendung des Markov-Verfahrens
DIN EN 61165:2007-02, Februar 2007.

/FAH 81/ Fahrmeir, L.; Kaufmann, H.; Ost, F.
Stochastische Prozesse
Carl Hanser Verlag München Wien, 1981.

/FRE 06/ Frey, W., et al.
Erprobung und Bewertung der Methoden einer PSA für SWR-Anlagen der Baulinie 69 nach Stand von Wissenschaft und Technik (PSA SWR 69) Gesellschaft für Anlagen- und Reaktorsicherheit,
Fachbände GRS-A-3292, GRS-A-3293, Garching, 2006.

/GMA 09/ Gmal, B; Kilger, R.; Krzykacz-Hausmann, B.; Herbert, H.-J.; Moser, F.-E. Peschke, J.
"Weiterführende Bearbeitung spezieller Themen im Rahmen generischer Sicherheitsanalysen zur Kritikalität von Kernbrennstoffen in der Nachverschlussphase eines geologischen Endlagers",
GRS-A-3486, August 2009.

/HEJ 15/ Herb, J. et al.
Entwicklung eines Ansatzes zur Analyse der Netzwerktechnologien in sicherheitsrelevanten Leittechniksystemen hinsichtlich Verbreitung und Auswirkung postulierter Fehler
Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) gGmbH,
Bericht GRS-377, ISBN 978-3-944161-58-7, Juni 2015.

/JOP 17/ Jopen, M, et al.
Zuverlässigkeitsbewertung digitaler leittechnischer Einrichtungen
Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) gGmbH, GRS-A-3890, August 2017.

/KIL 13/ Kilger, R, et al.
„Weiterführende Bearbeitung spezieller Themen im Rahmen generischer Sicherheitsanalysen zur Kritikalität von Kernbrennstoffen in der Nachverschlussphase eines geologischen Endlagers“, GRS-A-3707, Abschlussbericht, Juli 2013.

/KLS 14/ Kloos, M., Cester, F.
„Weiterentwicklung des Analysewerkzeugs SUSA für Unsicherheits- und Sensitivitätsanalysen im Rahmen einer fortschrittlichen PSA“,
GRS-A-3735, Juni 2014.

/KTA 12/ Kerntechnischen Ausschusses (KTA)
Prüfung und Betrieb von Hebezeugen in Kernkraftwerken
KTA 3903, Sicherheitstechnische Regel des KTA, Fassung 2012-11.

/KTA 15/ Kerntechnischen Ausschusses (KTA)
Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik
KTA 3503, Sicherheitstechnische Regel des KTA, Fassung 2015-11.

/NAS 17/ NASA
Mean Time to Repair Predictions
Johnson Space Center (NASA), Technique AT-2,
https://engineer.jpl.nasa.gov/practices/at2.pdf, 2017.

/NEA 15/ NEA/ CSNI
Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis
Nuclear Safety
NEA/ CSNI/ R(2014)16, February 2015.

/NRC 81/ U.S. Nuclear Regulatory Commission
Fault Tree Handbook
U.S. Nuclear Regulatory Commission, January 1981.

/PES 91/ Peschke, J: Erweiterung des Programmpakets für Zuverlässigkeitsberechnungen mit Markov-Modellen um eine Option zur Durchführung von Unsicherheits- und Sensitivitätsanalysen, GRS-A-1743,
Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, 1991.

/PIL 10/ Piljugin, E., Herb, J.
Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH,
GRS-A-3550, Garching, August 2010.

/PIL 14/ Piljugin E. et al.
Entwicklung einer Bewertungsmethode für das GVA-Potenzial in der digitalen Leittechnik mit dissimilarer/diversitärer Architektur
GRS-A-3746, GRS mbH, 2014.

/SCA 12/ Scandpower AB
RiskSpectrum Analysis Tools
Theory Manual, Version 3.2.1, © Scandpower AB 1984 – 2012

Abbildungsverzeichnis

Tabellenverzeichnis

A Anhang

A.1 Bestimmung der Ausfallraten der Modell-Komponenten

Repräsentativ wird im Folgenden die Vorgehensweise für die Ausfallrate FRAUSF (FR – Failure Rate; AU – Acquisition Unit; SF – Selbstmeldende Fehler) demonstriert.

RiskSpectrum liefert die folgenden zeitabhängigen Ergebnisse für selbstmeldende Fehler von AUs für das in /HEJ 15/ beschriebene Modell:

Tab. A. 1 Zeitabhängige Ergebnisse von RiskSpectrum für die Erfassungsrechner (AU)

No	Time T	Q(t)	W(t)	L(t)	E(T1,T2)	F(T1,T2)
	[h]	Unavailability	Uncond. failure int.	Cond. failure int.	Expected no. of failures	Prob. of >= 1 failures
1	0,00E+00	0,00E+00	1,26E-05	1,26E-05	0,00E+00	0,00E+00
2	8,74E-01	1,09E-05	1,26E-05	1,26E-05	1,10E-05	1,10E-05
3	2,51E+00	3,02E-05	1,26E-05	1,26E-05	3,18E-05	3,18E-05
4	5,58E+00	6,30E-05	1,26E-05	1,26E-05	7,06E-05	7,06E-05
5	1,13E+01	1,14E-04	1,26E-05	1,26E-05	1,43E-04	1,43E-04
6	2,21E+01	1,83E-04	1,26E-05	1,26E-05	2,80E-04	2,80E-04
7	4,23E+01	2,51E-04	1,26E-05	1,26E-05	5,35E-04	5,35E-04
8	8,02E+01	2,93E-04	1,26E-05	1,26E-05	1,01E-03	1,01E-03
9	1,51E+02	3,03E-04	1,26E-05	1,26E-05	1,91E-03	1,91E-03
10	2,84E+02	3,03E-04	1,26E-05	1,26E-05	3,59E-03	3,58E-03
11	5,33E+02	3,03E-04	1,26E-05	1,26E-05	6,74E-03	6,72E-03
12	1,00E+03	3,03E-04	1,26E-05	1,26E-05	1,26E-02	1,26E-02

Stellt man die erwartete Anzahl von Ausfällen („Expected no. of failures, E(T1, T2)“) als Funktion der Zeit dar, so ergibt sich eine Ursprungsgerade, deren Ableitung (Steigung) die gesuchte Ausfallrate für diese Komponente ist:

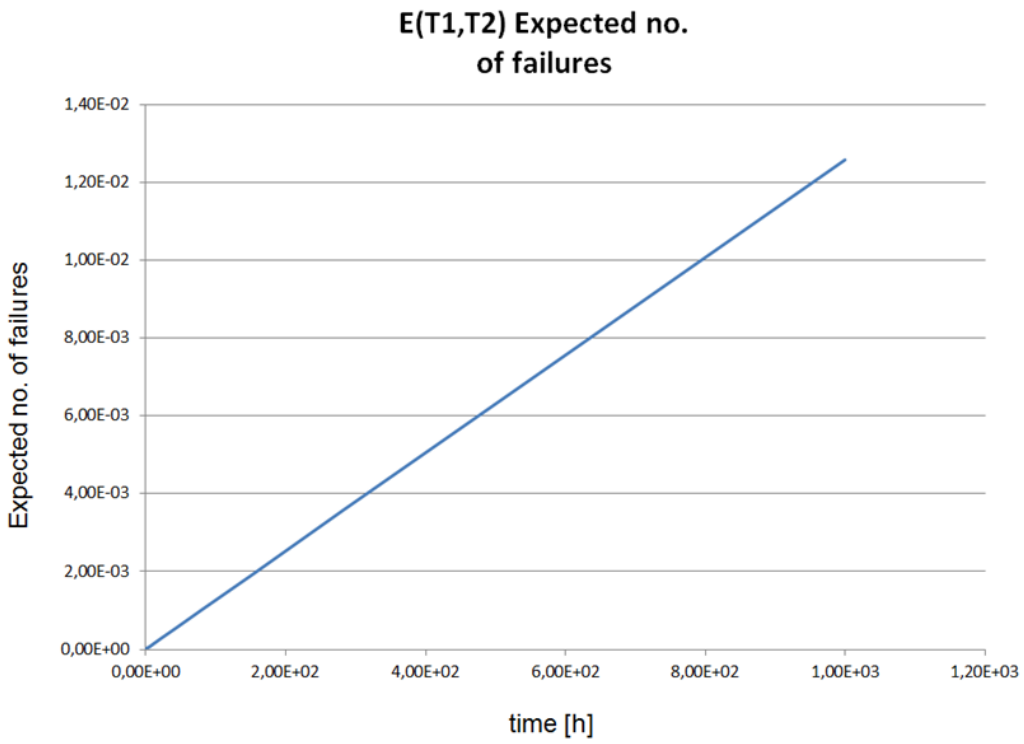

Abb. A. 1 Die erwartete Anzahl von Ausfällen einer AU als Funktion der Zeit

Eine lineare Regression (d. h. Anpassung einer Ursprungsgerade) mittels Excel liefert die folgenden Ergebnisse:

AUSGABE: ZUSAMMENFASSUNG

Regressions-Statistik	
Multipler Ko	0,99999873
Bestimmthe	0,99999745
Adjustiertes	0,90908836
Standardfeh	7,1696E-06
Beobachtung	12

ANOVA

	Freiheitsgrade (d	*ratsummen*	*Quadratsum*	*Prüfgröße (F)*	*F krit*
Regression	1	0,00022213	0,00022213	4321377,42	1,633E-29
Residue	11	5,6544E-10	5,1404E-11		
Gesamt	12	0,00022214			

	Koeffizienten	*tandardfehle*	*t-Statistik*	*P-Wert*	*Untere 95%*	*Obere 95%*	*Untere 95,0%*	*Obere 95,0%*
Schnittpunkt	0	#NV	#NV	#NV	#NV	#NV	#NV	#NV
X Variable 1	1,2612E-05	6,0672E-09	2078,7923	4,0098E-32	1,2599E-05	1,2626E-05	1,2599E-05	1,2626E-05

Abb. A. 2 Ergebnisse der linearen Regressionsanalyse für die Kurve in Abb. 4.11

Die Ausfallrate (SF) für AUs beträgt demnach $1{,}26125 \cdot 10^{-5}\ h^{-1}$.

Auf dieselbe Weise wurden für alle Komponenten und Netzwerk-Kommunikationsfehler die Fehlerraten bestimmt. Es ergibt sich die nachfolgende Tabelle:

Tab. A. 2 Mit RiskSpectrum bestimmte Ausfallraten der einzelnen Komponenten und für die Kommunikation zwischen den Komponenten

Basisereignis	**Beschreibung des Basisereignisses**	**Ausfallrate FR (λ)**
AU1A.P1.1_SF	self-signaling failure of AU1.A	1,26125E-05 h^{-1}
AU1A.P1.1_NSF	non self-signaling failure of AU1.A	8,6997E-08 h^{-1}
COM_AU1.A_PU1.A	loss of communication between AU1.A and PU1.A	8,37078E-06 h^{-1}
PU1A.SF	self-signaling failure of PU1.A	7,35869E-06 h^{-1}
PU1A.NSF	non self-signaling failure of PU1.A	8,6997E-08 h^{-1}
COM_PU1.A_VU1.A	loss of communication between PU1.A and VU1.A	8,37078E-06 h^{-1}
VU1A.SF	self-signaling failure of VU1.A	6,97175E-06 h^{-1}
VU1A.NSF	non self-signaling failure of VU1.A	8,6997E-08 h^{-1}

Für unsere Betrachtungen werden die Kommunikationsfehler im Netzwerk nicht gesondert betrachtet, sondern der jeweils oberen Ebene der Leittechnik zugeordnet. Insgesamt ergibt sich daher die folgende Liste an Parametern:

Tab. A. 3 Für diesen Bericht relevante Ausfallraten der Komponenten (AU, PU, VU) in den Modellsystemen

Parameter	**λ (Ausfallraten aus RiskSpectrum)**	**Anmerkungen**
FRAUSF	2,09832E-05 h^{-1}	incl. COM_AU1.A_PU1.A
FRAUNSF	8,6997E-08 h^{-1}	
FRPUSF	1,57295E-05 h^{-1}	incl. COM_PU1.A_VU1.A
FRPUNSF	8,6997E-08 h^{-1}	
FRVUSF	6,97175E-06 h^{-1}	
FRVUNSF	8,6997E-08 h^{-1}	

Da zusätzlich gemeinsam verursachte Ausfälle (GVA) berücksichtigt werden sollen, wird im Folgenden angenommen, dass jeweils 2,5 % der nichtselbstmeldenden Ausfälle einer Komponente durch GVA der entsprechenden Komponentenart (z. B. AUs) und weitere 2,5 % durch einen GVA aller Komponenten des Teilsystems (einer Diversität, z. B. A) verursacht werden. Es ergeben sich dann die Ausfallraten in Tab. 5.4.

Tab. A. 4 Ausfallraten bei Berücksichtigung von GVA /CCF – Common Cause Failures)

Parameter	λ (Ausfallraten aus RiskSpectrum)	Anmerkungen
FRAUSF	2,09832E-05 h^{-1}	incl. COM_AU1.A_PU1.A
FRAUNSF	8,26472E-08 h^{-1}	
FRPUSF	1,57295E-05 h^{-1}	incl. COM_PU1.A_VU1.A
FRPUNSF	8,26472E-08 h^{-1}	
FRVUSF	6,97175E-06 h^{-1}	
FRVUNSF	8,26472E-08 h^{-1}	
FRAUCCF	2,17493E-9 h^{-1}	CCF of all AUx.A
FRPUCCF	2,17493E-9 h^{-1}	CCF of all PUx.A
FRVUCCF	2,17493E-9 h^{-1}	CCF of all VUx.A
FRALLCCF	2,17493E-9 h^{-1}	CCF of all components of A

A.2 Bestimmung der Ausfallrate der VU-Komponenten in Master-Checker-Konfiguration

Ausgangspunkt für die folgende Betrachtung ist das Modell, dass im GRS-Bericht /HEJ 15/ beschrieben wird. In diesem Bericht wird die Architektur der Voter, wie in Abb. 4.13 gezeigt, dargestellt.

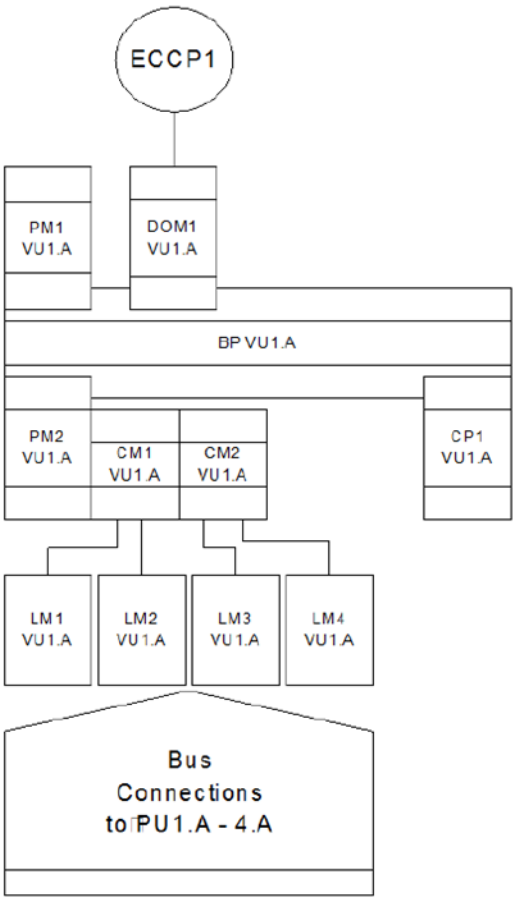

Abb. A. 3 Architektur der Voter (VU)

Der entsprechende Fehlerbaum sieht dann, angepasst an die Betrachtung für die VUs in diesem Bericht, wie folgt aus:

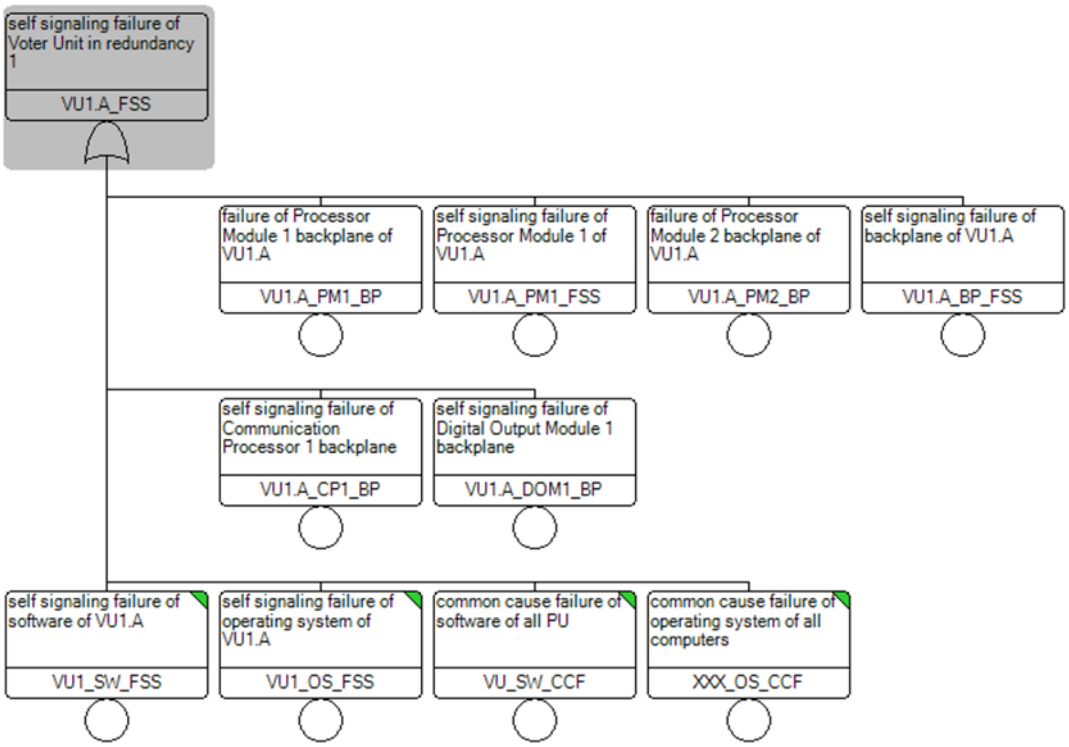

Abb. A. 4 Selbstmeldende Ausfälle der VUs im Fehlerbaum /HEJ 15/

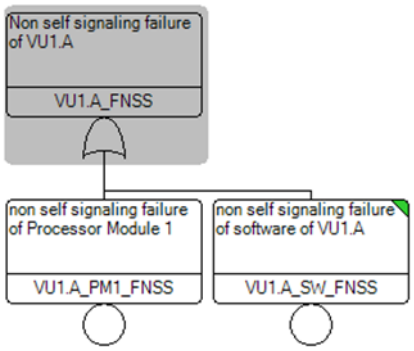

Abb. A. 5 Nichtselbstmeldende Ausfälle der VUs im Fehlerbaum /HEJ 15/

Dabei werden für die Betrachtungen in diesem Bericht die mit einer grünen Ecke markierten Basisereignisse fest auf „False“ gesetzt.

Vereinfachend wird jetzt angenommen, dass anstatt des einzelnen Prozessormoduls (PM1) für die Berechnung der Auswahl innerhalb des Voters, zwei Prozessormodule (PM1 und PM3 (die Bezeichnung PM2 ist bereits vergeben, s. o.)) als Master und Checker für die Berechnungen herangezogen werden (in realen Leittechniksystemen, z. B. TXS, steht dafür eine eigene Variante des Prozessormoduls mit zwei Prozessoren zur Verfügung). Jeder „nichtselbstmeldende“ Ausfall eines der beiden Prozessoren wird durch den Vergleich zwischen Master und Checker erkannt und damit ein selbstmeldender Ausfall. Damit verändern sich die Fehlerbäume wie folgt:

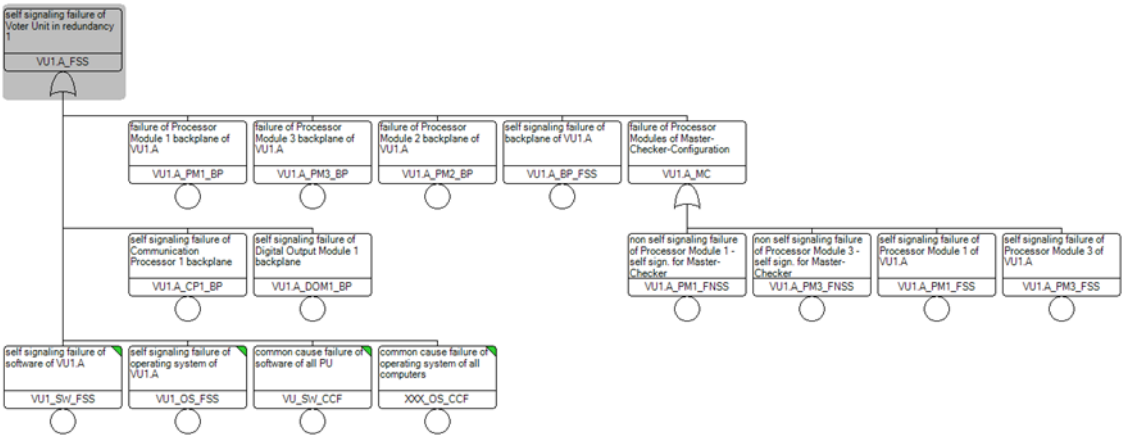

Abb. A. 6 Selbstmeldende Ausfälle der VUs (Master-Checker-Konfiguration)

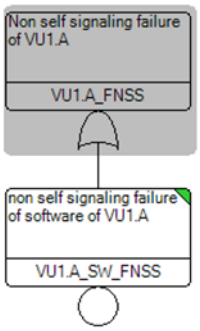

Abb. A. 7 Nichtselbstmeldende Ausfälle der VUs im Fehlerbaum (Master-Checker-Konfiguration)

Da die vormals nichtselbstmeldenden Basisereignisse VU1.A_PMx_FNSS (x = 1, 3) durch die Master-Checker-Konfiguration selbstmeldend werden, wurden die Berechnungsmodelle in RiskSpectrum für diese Ereignisse zusätzlich von „Tested“ auf „Repairable“ geändert. Der gleichzeitige Ausfall von PM1 und PM3 wird dabei nicht berücksichtigt, weil als sehr unwahrscheinlich eingeschätzt wird.

Werden, wie hier, Software-Fehler nicht explizit berücksichtigt, sind somit alle Ausfälle der VUs dadurch als selbstmeldend zu betrachten. Die lineare Regression an die zeitabhängigen Ergebnisse aus RiskSpectrum (erwartete Ausfälle als Funktion der Zeit) ergibt eine Ausfallrate für selbstmeldende Ausfälle (SF) von $1{,}0288 \cdot 10^{-5}\ h^{-1}$.

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-946607-79-3