

	DIN IEC 62551 (VDE 0050-4)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 29.020 Einsprüche bis 2008-12-31 Entwurf Analysemethoden für Zuverlässigkeit – Petrinetz-Modellierung (IEC 56/1266/CD:2008) Analysis techniques for dependability – Petri net modeling (IEC 56/1266/CD:2008) Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2008-10-20 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informations-technik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 96 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 56/1266/CD:2008 „Analysis techniques for dependability – Petri net modeling“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 56 „Dependability“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
	IEC 60050(191):1990 + A1:1999 + A2:2002	IEV Teil 191:2005	

Nationaler Anhang NB (informativ)

Literaturhinweise

IEV Teil 191, *Internationales Elektrotechnisches Wörterbuch – Teil 191: Zuverlässigkeit und Dienstgüte*

Analysemethoden für Zuverlässigkeit – Petrinetz-Modellierung

Inhalt

	Seite
Einleitung.....	7
1 Anwendungsbereich	7
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	8
5 Allgemeine Beschreibung von Petrinetzen.....	10
5.1 Zeitlose Low-level-Petrinetze	10
5.2 Zeitbehaftete Low-level-Petrinetze.....	10
5.3 High-level-Petrinetze	11
6 Beziehung zu RAMS-Konzepten.....	11
7 Zuverlässigkeitsmodellierung und -analyse mit Petrinetzen	11
7.1 Die auszuführenden Schritte im Allgemeinen	11
7.2 Die durchzuführenden Schritte im Detail.....	12
8 Verhältnis zu anderen Modellen der Zuverlässigkeit	17
Anhang A (informativ) Struktur und Dynamik von Petrinetzen	18
A.1 Allgemeines Petrinetz-Konzept und seine Beziehung zur Zuverlässigkeit	18
A.1.1 Petrinetz-Struktur.....	18
A.1.2 Kausale Dynamik in Low-level-Petrinetzen	18
A.1.3 Erreichbarkeitsgraph (en: reachability graph)	20
A.2 Zeitbehaftete Petrinetze	22
A.2.1 Spezifische Transitionen für zeitbehaftete, niedrige Petrinetze	22
A.2.2 Dynamik in zeitbehafteten niedrigen Petrinetzen	22
A.2.3 Verschiedene Kategorien von zeitbehafteten Petrinetzen	23
A.3 Methoden zur Analyse von Petrinetzen.....	24
A.3.1 Qualitative Analyse	24
Anhang B (informativ) m aus n.....	27
B.1 Lokale und globale Zustände	27
B.2 Globale Zustände und Systemaufbau	28
Anhang C (informativ) Abstraktes Beispiel	31
C.1 Lokale, globale und aggregierte globale Zustände	31
C.2 Funktionsfähigkeit und Systemfunktion sowie Hierarchisierung	32
Anhang D (informativ) Modellierung typischer Zuverlässigkeitskonzepte	33
Anhang E (informativ) Darstellung der Analyseergebnisse	34
Anhang F (informativ) Beispiel: Bahnübergang	36
Bild 1 – Die Methode besteht im Wesentlichen aus den Schritten „Modellieren“, „Analysieren“ und „Darstellen“	11

	Seite
Bild 2 – Prozess der Zuverlässigkeitsmodellierung und -analyse mit Petrinetzen	12
Bild 3 – Modellierungsstruktur in Bezug auf die zwei Hauptkomponenten „Strecke“ und „Steuerung“ mit Modellen ihrer Funktionen und Zuverlässigkeiten	14
Bild 4 – Angabe der Analysemethode in Abhängigkeit vom PN-Modell	15
Bild 5 – Funktionsfähigkeit „Zustand-Transition“-Zyklus eines Bauelements	18
Bild 6 – Transition „Ausfall“ (en: failure) ist aktiviert	19
Bild 7 – Stelle „Fehlzustand“ (en: faulty) wird durch Schalten von „Ausfall“ markiert	19
Bild 8 – Transition „Element ₁ Instandsetzung“ ist aktiviert	19
Bild 9 – Das Token der Stelle Instandhaltungspersonal ist nicht verbraucht	19
Bild 10 – Transition ist nicht aktiviert	20
Bild 11 – Markierung vor dem Schalten	20
Bild 12 – Markierung nach dem Schalten	20
Bild 13 – Ein Petrinetz mit Anfangsmarkierung	20
Bild 14 – Der zugehörige RG	20
Bild 15 – Transitionen „Element _{1p} Instandsetzung“ und „Element _{1hp} Ausfall“ sind aktiviert	21
Bild 16 – Markierung nach Schaltung der Transition „Element _{1p} Instandsetzung“	21
Bild 17 – Ein zeiterweitertes PN mit exponential verteilten, zeitbehafteten Transitionen	22
Bild 18 – Der zugehörige stochastische Erreichbarkeitsgraph	22
Bild 19 – Petrinetz mit zeitbehafteten Transitionen	23
Bild 20 – Zuverlässigkeitsnetze zweier Elemente mit spezifischen Ausfall- und Instandsetzungsraten	27
Bild 21 – stochastischer RG von Bild 20 (als Abkürzung wird $\bar{c}_i$ für „Element _i Fehlzustand“ genutzt)	27
Bild 22 – Zuverlässigkeitsnetze zweier Elemente mit spezifischen Ausfall- und Instandsetzungsraten	28
Bild 23 – Stochastischer RG von Bild 22 (als Abkürzung wird $\bar{c}_i$ für „Element _i Fehlzustand“ genutzt)	28
Bild 24 – Spezifisch verbundenes 1-aus-3-Zuverlässigkeitsnetz	29
Bild 25 – Spezifisch verbundenes 2-aus-3-Zuverlässigkeitsnetz	29
Bild 26 – Spezifisch verbundenes 3-aus-3-Zuverlässigkeitsnetz	30
Bild 27 – Stochastischer RG mit systemspezifischen Betriebszuständen	30
Bild 28 – Funktionsfähigkeitsmodellierung eines einzelnen Elements	31
Bild 29 – Stochastischer Erreichbarkeitsgraph des Netzes aus Bild 28 mit seinen globalen Zuständen und aggregierten globalen Zuständen in Bezug auf Verfügbarkeit und Sicherheit	31
Bild 30 – Grundlegendes Konzept zur Modellierung von Zuverlässigkeit und Funktion	32
Bild 31 – Allgemeines hierarchisches Netz mit Supertransitionen	32
Bild 32 – Allgemeines hierarchisches Netz mit Supertransitionen und -stellen	32
Bild 33 – Aggregierter Erreichbarkeitsgraph (mit λ_i und μ_i als Ausfall- und Instandsetzungsraten)	34
Bild 34 – Verfügbarkeits-Sicherheits-Diagramm mit logarithmischer Skaleneinteilung. Zuverlässigkeitswerte des m-out-of-n-Systems mit n = 2	35
Bild 35 – Anwendungsbeispiel eines Bahnübergangs und seiner Sicherungseinrichtung	36
Bild 36 – Hauptbestandteile des Bahnübergangsmodells	37

	Seite
Bild 37 – Teilmodelle des Bahnübergangmodells.....	37
Bild 38 – Petrinetz-Modell des Bahnübergangs.....	39
Bild 39 – Datenerhebung zum Straßenverkehrsfluss an einem bestimmten Bahnübergang.....	40
Bild 40 – Werte aus Bild 39 mit einer Wahrscheinlichkeitsfunktion der Zeitintervalle zwischen zwei sich dem Bahnübergang nähernden Fahrzeugen.....	41
Bild 41 – Gemessene Aufenthaltsdauern von Straßenfahrzeugen im Gefahrenbereich des Bahnübergangs.....	41
Bild 42 – Wahrscheinlichkeitsfunktion der Aufenthaltsdauern von Straßenfahrzeugen im Gefahrenbereich des Bahnübergangs.....	42
Bild 43 – Aggregierter Erreichbarkeitsgraph und Informationen über entsprechende Zustände.....	47
Bild 44 – Ergebnisse der quantitativen Analyse zeigen die Verfügbarkeit des Bahnübergangs für Straßennutzer in Abhängigkeit von der Rate gefährlicher Ausfälle der Sicherungseinrichtung für verschiedene Annäherungszeiten T_{AC}	48
Bild 45 – Ergebnisse der quantitativen Analyse zeigen das individuelle Risiko der Bahnübergangsnutzer in Abhängigkeit von der Rate gefährlicher Ausfälle der Sicherungseinrichtung für verschiedene Annäherungszeiten T_{AC}	48
Bild 46 – Verfügbarkeits-Sicherheits-Diagramm, beruhend auf den Ergebnissen der Modellanalyse in den Bildern 44 und 45.....	49
Tabelle 1 – Symbole in zeitlosen Petrinetzen.....	9
Tabelle 2 – Zusätzliche Symbole in zeitbehafteten Petrinetzen.....	9
Tabelle 3 – Superknoten (en: Supernodes) für hierarchisches Modellieren.....	9
Tabelle 4 – Abkürzungen.....	9
Tabelle 5 – Einschlägige Begriffe in Systemen, Petrinetzen und RAMS.....	11
Tabelle 6 – Verbindliche und empfohlene Bestandteile der Dokumentation.....	16
Tabelle 7 – Dazugehörige Bezeichnungen in Systemen, Petrinetzen und Erreichbarkeitsgraphen.....	21
Tabelle 8 – Stellen und Transitionen mit Belohnung.....	26
Tabelle 9 – Zuverlässigkeitskonzepte und ihre PN-Modellierungsstrukturen.....	33
Tabelle 10 – Modellierungskosten von Zuständen und Ereignissen.....	33
Tabelle 11 – Straßenverkehrsbezogene Stellen im Teilmodell „Verkehrsprozess“.....	40
Tabelle 12 – Straßenverkehrsbezogene Transitionen im Teilmodell „Verkehrsprozess“.....	43
Tabelle 13 – Schienenverkehrsbezogene Stellen im Teilmodell „Verkehrsprozess“.....	43
Tabelle 14 – Schienenverkehrsbezogene Transitionen im Teilmodell „Verkehrsprozess“.....	44
Tabelle 15 – Stellen im Teilmodell „Verkehrsunfall“.....	44
Tabelle 16 – Transitionen im Teilmodell „Verkehrsunfall“.....	44
Tabelle 17 – Stellen im Teilmodell „Steuerungsfunktions-Zuverlässigkeit“.....	45
Tabelle 18 – Transitionen im Teilmodell „Steuerungsfunktions-Zuverlässigkeit“.....	45
Tabelle 19 – Stellen im Teilmodell „Steuerungsfunktion“.....	46
Tabelle 20 – Transitionen im Teilmodell „Steuerungsfunktions-Zuverlässigkeit“.....	46
Tabelle 21 – Spezifikation von booleschen Bedingungen, um Zustände zu aggregierten Zuständen zusammenzufassen.....	47

Einleitung

Diese Internationale Norm definiert die Darstellung der Grundelemente von Petrinetzen (PN) und enthält Leitlinien für ihre Anwendung in der Zuverlässigkeitsmodellierung.

Die wesentliche Modellierungsstärke von Petrinetzen basiert auf der Beschreibung des globalen kausalen Verhaltens eines Systems durch Modellieren der Beziehungen zwischen lokalen Zuständen und lokalen Ereignissen. Vor diesem Hintergrund haben Petrinetze breite Akzeptanz in allen Industriezweigen gefunden (z. B. in der Informations-, Kommunikations-, Transport-, Verfahrens-, Fertigungs- und Energietechnik).

Im Vergleich zu anderen automatenbasierten Zuverlässigkeitsmethoden (z. B. Markov-Methode) erlaubt das eindeutige Modellieren von lokalen Zuständen und auch von lokalen unabhängigen Ereignissen ein angemessenes und intuitives Modellieren von Systemen und deren Dynamik. Darüber hinaus wird die Modellierung von stochastischem Verhalten nicht auf exponential verteilte Eigenschaften beschränkt, sondern kann frei gewählt werden.

Diese Norm dient dazu, die etablierten Grundlagen-Prinzipien von Petrinetzen im Kontext der Zuverlässigkeit zu definieren und um die gegenwärtige Anwendung der PN-Modellierung und -Analyse als ein Hilfsmittel zur qualitativen und quantitativen Abschätzung der Zuverlässigkeit und risikobezogener Maße eines Systems anzuwenden.

1 Anwendungsbereich

Diese Internationale Norm gibt Anleitung für eine Petrinetz-basierte Methode für Zuverlässigkeitsbetrachtungen. Sie unterstützt das Modellieren eines Systems, das Analysieren des Modells und die Darstellung der Analyseergebnisse. Diese Methode orientiert sich an zuverlässigkeitsbezogenen Maßen mit allen ihren in Bezug stehenden Eigenschaften wie RAMS (Funktionsfähigkeit (en: reliability), Verfügbarkeit (en: availability), Instandhaltbarkeit (en: maintainability) und Sicherheit (en: safety)).

Daher befasst sich diese Internationale Norm in Bezug auf Petrinetze mit den folgenden Themen:

Definition der entscheidenden Begriffe und Symbole und Beschreibung ihrer Anwendung und Methoden zur grafischen Darstellung;

Kurzdarstellung der Terminologie und ihr Bezug zur Zuverlässigkeit;

Darlegung einer schrittweisen Herangehensweise zur

- a) Zuverlässigkeitsmodellierung mit Petrinetzen;
- b) Anleitung der Nutzung von Petrinetz-basierten Methoden für qualitative und quantitative Zuverlässigkeitsanalysen;
- c) Darstellung und Interpretation der Analyseergebnisse;
- d) Kurzfassung des Bezugs von Petrinetzen zu anderen Modellierungstechniken;
- e) Bereitstellung von Praxisbeispielen.

Diese Internationale Norm bietet keine Anleitung zur Lösung mathematischer Probleme, die im Kontext einer PN-Analyse auftreten.

Diese Internationale Norm ist anwendbar in allen Industrien, bei denen qualitative und quantitative Zuverlässigkeitsanalysen durchgeführt werden müssen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV), chapter 191: Dependability and quality of service*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60050 (191). Die folgenden zusätzlichen Begriffe werden in dieser Norm benutzt.

3.1

Bauelement

en: component

bestimmender Bestandteil eines Gerätes, welches sich nicht physikalisch in kleinere Teile zerlegen lässt, ohne seine jeweilige Funktion zu verlieren

[IEC 60050:151-11-21]

3.2

Ereignis

en: event

etwas, das zu einem Zeitpunkt stattfindet

ANMERKUNG Rein physikalisch gilt ein Ereignis als ein Punkt in der Raumzeit

[IEC 60050:111-16-04]

3.3

Modul

Routine, einzelnes Bauteil oder eine funktionelle Gruppe von zusammengefassten Routinen oder eigenständige zusammengehörende Bestandteile

[IEC 61508-4]

3.4

System

Menge von Elementen, die ihrer Anordnung entsprechend zusammenwirken. Dabei kann ein Element eines Systems ein eigenes System, genannt „Untersystem“, sein, das ein kontrollierendes oder ein kontrolliertes System sein kann und Hardware, Software und menschliche Interaktion beinhalten kann

ANMERKUNG 1 Ein Mensch kann Teil eines Systems sein.

ANMERKUNG 2 Diese Definition unterscheidet sich von IEC 351-01-01.

[IEC 61508-4]

4 Symbole und Abkürzungen

Die grafische Darstellung eines Petrinetzes verlangt, dass Symbole (en: symbols), Bezeichner (en: identifier) und Anschriften (en: labels) auf eine konsistente Weise verwendet werden. Eine Sammlung von allgemein genutzten Darstellungen ist in Tabelle 1, Tabelle 2 und Tabelle 3 enthalten.

Die folgenden Symbole in Tabelle 1 werden für zeitlose Petrinetze (en: untimed PN) empfohlen.

Tabelle 1 – Symbole in zeitlosen Petrinetzen

Bezeichner	Bezeichner	Bezeichner	Bezeichner (Gewicht)	$\xrightarrow{2}$ (normale) Kante $\xleftrightarrow{\quad}$ Testkante $\xrightarrow{\quad}$ Verbotskante
Symbol einer Stelle	Symbol einer markierten Stelle	Symbol einer Transition (zeitlos, auch: kausal)	Symbol einer Transition mit Gewichtung	Symbole von Relationen

Tabelle 2 stellt die für zeitbehaftete Petrinetze (en: timed PN) empfohlenen Symbole dar.

Tabelle 2 – Zusätzliche Symbole in zeitbehafteten Petrinetzen

	Art der Transition		
	deterministisch	stochastisch	
		exponential oder geometrisch verteilt	beliebig verteilt
Parameter	T	λ	ϕ (beliebige Verteilung)
Symbol			

Die Symbole in Tabelle 3 werden für hierarchische Petrinetze (en: hierarchical PN) empfohlen:

Tabelle 3 – Superknoten (en: Supernodes) für hierarchisches Modellieren

Bezeichner	Bezeichner	Bezeichner	
Symbol einer Superstelle	Symbol einer Supertransition	Symbol eines Superknotens	Symbol einer Superkante

Die folgenden Abkürzungen in Tabelle 4 werden in dieser Norm vorgeschlagen:

Tabelle 4 – Abkürzungen

Abkürzung	
ETA	Ereignisbaumanalyse (en: event tree analysis)
FME(C)A	Fehlzustandsart-, -auswirkungs-(und -kritizitäts-)Anlyse (en: Failure, Mode, Effects (and Criticality) Analysis)
FTA	Fehlzustandsbaumanalyse (en: fault tree analysis)
PN	Petrinetz (en: petri net)
RAMS	Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (en: Reliability, Availability, Maintainability, Safety)
RBD	Zuverlässigkeitsblockdiagramm (en: Reliability Block Diagram)
RG	Erreichbarkeitsgraph (en: Reachability Graph)

5 Allgemeine Beschreibung von Petrinetzen

5.1 Zeitlose Low-level-Petrinetze

Petrinetze (PN) sind Graphen, in denen aktive und passive Knoten (en: nodes) unterschieden werden. Die passiven Knoten (auch: „Elemente“) werden Stellen (en: places) genannt und modellieren z. B. lokale Zustände oder Bedingungen und werden mit Token markiert, falls der lokale Zustand erfüllt ist. Die aktiven Elemente nennt man Transitionen (en: transitions). Sie modellieren die möglichen Übergänge von einem Zustand zu einem anderen. Die kausalen Beziehungen zwischen den Stellen und Transitionen werden durch verschiedene Arten von gerichteten Kanten (en: Arcs), die die Knoten verbinden, beschrieben (siehe Tabelle 1 für die grundlegenden Symbole eines Petrinetzes und Anhang A für eine Einführung in PN).

Verbotskanten (en: inhibitor arcs) können nur von Stellen zu Transitionen führen.

Eine Transition ist schaltbereit, wenn alle ihre Eingangsstellen (en: preset places), die mit Normal- oder Testkanten verbunden sind, eine ausreichende Anzahl von Token tragen und alle Eingangsstellen, die mit einer Verbotskante verbunden sind, nicht markiert sind. Die Anzahl der benötigten Token, um eine Transition zu aktivieren, ist an der Kante notiert. Allgemein gilt hierbei, dass diese Kennzeichnung von der Belegung der Markierung abhängen kann (siehe [12]).

Sobald eine Transition aktiviert ist, kann sie feuern bzw. schalten, d. h. sie kann die Markierung des Modells ändern. Das Schalten einer Transition bewirkt nur Änderungen auf die Markierung von Stellen, die mit ihr durch normale Kanten verbunden sind. Dabei werden bei den Eingangsstellen entsprechend der Kantengewichte Token abgezogen und auf die Ausgangsstellen (en: postset places) Token (entsprechend der Kantengewichtung) erzeugt. Gibt es keine nähere Bezeichnung des Kantengewichtes (en: arc label), so ist diese Anzahl 1.

Der RG (en: reachability graph) eines Petrinetzes besteht aus allen globalen Markierungen, die, ausgehend von einer Startmarkierung, durch eine beliebige Sequenz von Transitionsschaltungen erreicht werden können. In diesem Graphen repräsentiert ein Knoten eine bestimmte globale Markierung, und jede Kante repräsentiert das Schalten einer Transition, die eine globale Markierung in eine andere überführt.

Petrinetze können auch nicht-graphisch in einer Inzidenzmatrix dargestellt werden. Ist T die Menge der Transitionen und P die Menge der Stellen, dann hat die Inzidenzmatrix die Dimension $|P| \times |T|$. Für jede Transition wird die Änderung der globalen Markierung infolge ihres Schaltens in einer entsprechenden Spalte angegeben.

5.2 Zeitbehaftete Low-level-Petrinetze

In zeitbehafteten niedrigen PN werden sowohl zeitlose (en: untimed) als auch zeitbehaftete (en: timed) Transitionen genutzt. Um zu Schalten, muss eine zeitbehaftete Transition für eine bestimmte Zeitdauer aktiviert sein, wobei diese Dauer deterministisch oder stochastisch sein kann. Dies ist abhängig von der transitionsspezifischen Verteilungsfunktion (pdf) und von entsprechenden Parametern. Wenn zwei oder mehr Transitionen zeitgleich schaltbereit sind, wird die Schaltreihenfolge entweder durch eine willkürliche Vorauswahl (en: preselection policy) oder durch die Aktivierungszeit-abhängige Vorauswahl (en: race policy) festgelegt^{N1)}. Zusätzlich zu den Verteilungsfunktionen muss Grundsätzliches zur Ausführungsstrategie (en: execution policy) und zum Gedächtnis von Transitionen (en: memory policy) spezifiziert sein (siehe [2]). Die Transition darf schalten, wenn der angegebene Zeitraum abgelaufen ist. Die gängigsten Transitionen in zeitbehafteten Petrinetzen sind in Tabelle 2 dargestellt.

Entsprechend des spezifischen Typs einer zeitbehafteten Transition wird die deterministische Schaltzeit, die konstante Schaltrate (Transitionen mit exponential- oder geometrisch verteilten Schaltzeiten) oder die Wahrscheinlichkeitsverteilung mit ihren Werten (Transitionen mit beliebig verteilten Schaltzeiten) durch Attributieren mit einem Zeitparameter spezifiziert.

^{N1)} Nationale Fußnote: Im Folgenden werden die englischen Ausdrücke „preselection“ und „race policy“ verwendet.

Wie auch beim zeitunabhängigen Fall, besteht der RG eines zeitbehafteten PN aus Knoten, die globale Markierungen repräsentieren und aus Pfeilen, die wiederum das Schalten der Transitionen graphisch darstellen. Zusätzlich zu zeitlosen RG muss der RG eines zeitbehafteten Netzes die spezifischen Parameter von Transitionen berücksichtigen.

5.3 High-level-Petrinetze

In High-level-Petrinetzen besteht eine Markierung aus individuellen, unterscheidbaren Tupeln, anstatt aus anonymen und schwarzen Token. Dadurch modellieren Tupel nicht nur die Erfüllung von Bedingungen oder die Existenz von Zuständen sondern die Informationen selbst. Vor diesem Hintergrund können die Kantenbeschriftungen in Abhängigkeit von den gegebenen Informationen formuliert werden. Eine solche Modellierungsunterstützung ermöglicht selbst bei komplexen Systemen kompakte und intuitive Modelle. Da die in dieser Norm vorgestellte Methodik nicht von diesen Möglichkeiten abhängt, verweisen wir für High-Level-PN auf [ISO/IEC 15909] (siehe [13] und Beispiele in Anhang B und C).

6 Beziehung zu RAMS-Konzepten

Im Rahmen von RAMS können lokale Ereignisse wie zum Beispiel Ausfälle und Reparaturen durch Transitionen und lokale Zustände wie zum Beispiel Fehlzustände durch Stellen dargestellt werden. Aus diesem Grund stellt die zu einem Knoten gehörende Bezeichnung in erster Linie das dazugehörige Zuverlässigkeitsmerkmal dar und spezifiziert bei Bedarf das zugehörige Gerät. Falls die Konzepte von Petrinetzen auf diese Art interpretiert werden, kann man von „Dependability Interpreted PNs“ sprechen.

Tabelle 5 gibt einen Überblick über sich entsprechende Konzepte zwischen Systemen im Allgemeinen, Petrinetzen und RAMS-Konzepten:

Tabelle 5 – Einschlägige Begriffe in Systemen, Petrinetzen und RAMS

Gesichtspunkt	System	Petrinetz	RAMS	
dynamisch	Ereignis	Transition	Ausfall	Reparatur
statisch	lokaler Zustand	Stelle	Fehlzustand	in Betrieb

7 Zuverlässigkeitsmodellierung und -analyse mit Petrinetzen

7.1 Die auszuführenden Schritte im Allgemeinen

Die Analyse eines Systems verlangt im Allgemeinen ein angemessen detailliertes Modell dieses Systems. Der erforderliche Detaillierungsgrad hängt von den durchzuführenden Analysen ab. Im Allgemeinen sind Systeme zu komplex, um sie in nur einem Schritt detailliert und in ihrer Gesamtheit darzustellen. Daher muss bei der Modellierung iterativ vorgegangen werden, beginnend mit einer groben textuellen Beschreibung hin zu einem detaillierten, formalen Modell. Die Analyseergebnisse die auf Basis dieses Modells gewonnen werden, müssen auf benutzerfreundliche Weise dargestellt und vor dem Hintergrund der Analyseaufgabe interpretiert werden (siehe Bild 1).

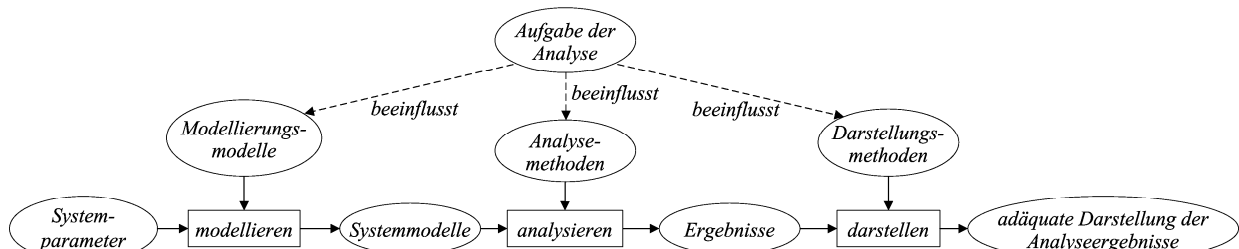


Bild 1 – Die Methode besteht im Wesentlichen aus den Schritten „Modellieren“, „Analysieren“ und „Darstellen“

Bild 2 zeigt die wesentlichen Schritte der Zuverlässigkeitsmodellierung und -analyse mit PN. Obwohl dies scheinbar ein geradliniger Prozess ist, so muss der Analyst bedenken, dass Modellieren im Allgemeinen ein iterativer Prozess ist. Insbesondere der 3. Schritt „Verfeinern des Modells“ benötigt mehrere Iterationen.

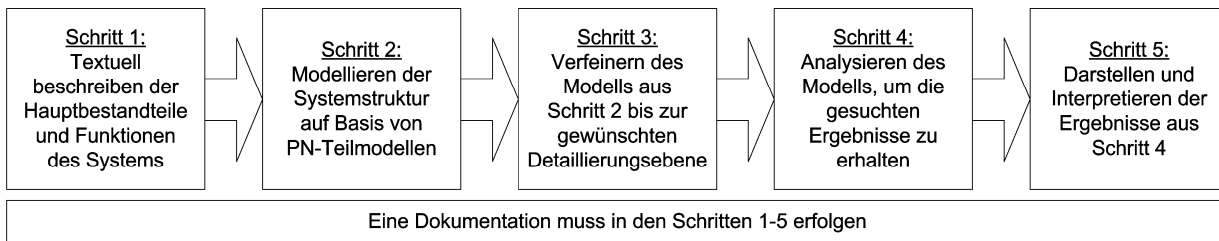


Bild 2 – Prozess der Zuverlässigkeitsmodellierung und -analyse mit Petrinetzen

Schritt 1: Beschreiben der Hauptbestandteile des Systems mit gebräuchlichen Beschreibungsmitteln, z. B. mit Text, mit Tabellen und Bildern etc. (siehe 7.2.1)

Schritt 2: Modellieren der Struktur des Systems, basierend auf PN-Teilmodellen und ihren Beziehungen und Dokumentieren dieses Modells (siehe 7.2.2).

Zum Beispiel sind die wichtigsten Teilmodelle oft

die Strecke d. h. die operative Funktionseinheit, die gesteuert werden muss, und

die Steuerung, d. h. das Teilsystem zur Steuerung der Strecke

Schritt 3: Verfeinern des in Schritt 2 erstellten Modells, bis der gewünschte Detaillierungsgrad erreicht ist, und dokumentieren dieses Modells (siehe 7.2.3).

Eine PN-Darstellung des Systems aus Schritt 2 inklusive der Teilsysteme muss erstellt werden.

Der gewünschte Detaillierungsgrad ist erreicht, sobald alle für die Analyse notwendigen Informationen im Model enthalten sind.

Schritt 4: Analysieren des Modells, um die gewünschten Ergebnisse zu erhalten und Dokumentieren der Analysen (siehe 7.2.4)

Schritt 5: Darstellen und Interpretieren der Analyseergebnisse und Dokumentieren dieser Darstellung (siehe 7.2.5)

Alle einzelnen Schritte werden fortlaufend zu dokumentiert.

7.2 Die durchzuführenden Schritte im Detail

In diesem Absatz werden die Schritte näher beschrieben. In jedem Schritt muss die in diesem Schritt durchgeführte Arbeit dokumentiert werden.

7.2.1 Beschreiben der Hauptbestandteile und Funktionen des Systems (Schritt 1)

Die folgenden Konzepte des zu modellierenden und analysierenden Systems müssen identifiziert und beschrieben werden:

- a) Grenzen, Kontext, Umgebung, vor allem in Hinsicht auf Zuverlässigkeit und Anforderungen;
- b) Hauptbestandteile (z. B. die Strecke und die Steuerungseinrichtungen);
- c) Hauptfunktionen (Betrieb und Steuerung, Sicherung) und Zweck.

Die Beschreibung kann mittels gebräuchlicher Methoden z. B. mit Text, mit Tabellen oder Abbildungen, durchgeführt werden.

7.2.2 Modellieren der Struktur des Systems auf Basis von Petrinetz-Teilmodellen und ihrer Beziehungen (Schritt 2)

Dynamische Systeme, z. B. Automatisierungssysteme, können im Allgemeinen in die Teilsysteme „ungesteuerte Strecke“ und „Steuerung der Strecke“ unterteilt werden. Um zu vermeiden, dass die Strecke in einen unerwünschten Zustand eintritt, wird sie durch die Steuerung der Strecke gesteuert. Ferner kann jedes dieser Teilsysteme aus dem Blickwinkel der Funktion und der Zuverlässigkeit betrachtet werden (siehe Bild 3). Beispielsweise muss man, da die Steuerung der Strecke nicht immer ordnungsgemäß funktioniert, die Zuverlässigkeit der Steuerung in Betracht ziehen – die Zuverlässigkeit des Systems hängt von der Zuverlässigkeit der Steuerung ab. Da das zu entwickelnde Modell von der Komplexität des Systems und der Analyse-Aufgabe abhängt, besteht das globale Modell aus einer Untermenge der folgenden vier Teilmodelle:

- a) Ein Teilmodell, um die Funktionen der Strecke zu spezifizieren;
- b) Ein Teilmodell, um die Zuverlässigkeit der Strecke zu spezifizieren;
- c) Ein Teilmodell, um die Funktion der Steuerung zu spezifizieren;
- d) Ein Teilmodell, um die Zuverlässigkeit der Steuerung zu spezifizieren.

In a) muss das betriebliche Teilsystem, das gesteuert werden soll, modelliert werden. Ohne eine Steuerung würde dieses dynamische Teilsystem eine Vielfalt von Prozessen innerhalb eines riesigen Zustandsraumes, modelliert durch den RG des PN, generieren. Einige Zustände innerhalb dieses RG müssen vermieden werden, weil sie Gefahren darstellen und zu sicherheitskritischen Situationen, zu Blockierungen (en: Deadlocks), Stillständen oder anderen unverfügbaren Zuständen führen.

In b) muss die Zuverlässigkeit der Strecke modelliert werden. In diesem Teilmodell werden Unsicherheiten die das Verhalten der Strecke betreffen, eingeschlossen (z. B. menschliches Verhalten und Umwelteinflüsse).

Da die Zuverlässigkeit der Strecke die Verfügbarkeit, Korrektheit, Sicherheit und andere Funktionen beeinflusst, werden die Teilmodelle aus a) und b) miteinander verknüpft.

In c) muss das Teilsystem, das die Steuerung der Strecke zur Beschränkung des betrieblichen Ablaufes übernimmt, spezifiziert werden. In diesem Teilmodell wird die Möglichkeit von Ausfällen der Steuerung nicht berücksichtigt, man setzt voraus, dass die Steuerung fehlerfrei arbeitet. Auf diese Weise führen die entsprechenden Verbindungen mit den Modellen aus a) und b) zu einem Erreichbarkeitsgraphen ohne unerwünschte Zustände (z. B. Gefährdungen oder Unfälle).

In d) wird das Teilsystem, das die physikalische Realisierung der Steuerung spezifiziert, unter besonderer Beachtung der Zuverlässigkeit modelliert. Dieses Modell hängt von der technischen Umsetzung oder menschlichen Bedienern und Umgebungseinflüssen ab. Mittels einer adäquaten Verknüpfung mit dem Teilmodell aus c), werden mögliche Ausfälle und falsche Abläufe der Steuerung berücksichtigt. Da diese die Steuerungsfunktionen der Modellierung nach c) beeinflussen, werden im globalen Modell, d. h. im Modell, das aus den (verknüpften) Teilmodellen von a) bis d) besteht, sowohl die Strecke als auch die Steuerung und die Zuverlässigkeit der Steuerung berücksichtigt. Auf diese Weise enthält der entsprechende RG gefährliche und unbeabsichtigte Zustände.

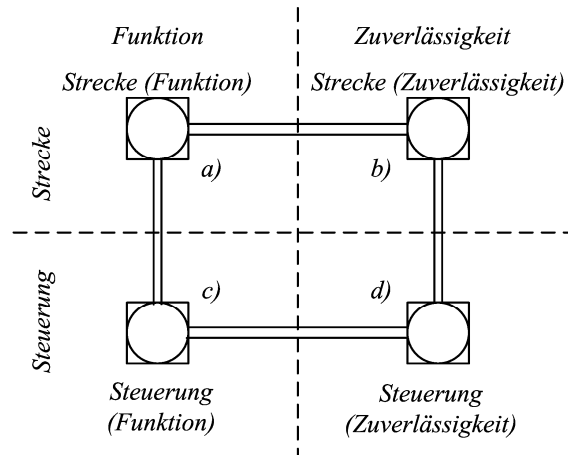


Bild 3 – Modellierungsstruktur in Bezug auf die zwei Hauptkomponenten „Strecke“ und „Steuerung“ mit Modellen ihrer Funktionen und Zuverlässigkeiten

Bild 3 bildet die orthogonale Grundstruktur in Bezug auf die verschiedenen funktionalen Ebenen und ihrer Zuverlässigkeitsaspekte ab.

Ein integriertes Modell des Gesamtsystems kann einfach erstellt werden, falls jedes der Teilsysteme durch einzelne Petrinetze wie in den vorherigen Abschnitten modelliert wird. Die einzelnen PNs werden vorzugsweise durch Test- und Verbotskanten verbunden. Dies erlaubt einen modularen Ansatz. So kann jedes Teilsystem modifiziert und einzeln verändert werden, ohne Seiteneffekte auf benachbarte Modelle.

Bei der Dokumentation dieses Schrittes müssen die wesentlichen Teilmodelle des Systems und ihre Verbindungen identifiziert werden. Hier müssen die Grenzen jedes Teilmodells, seine Hauptbestandteile, Funktionen und sein Zweck mit gebräuchlichen Mitteln beschrieben werden, z. B. mit Text, mit Tabellen oder Abbildungen.

7.2.3 Verfeinern des Modells aus Schritt 2 bis zum Erreichen des gewünschten Detaillierungsgrades (Schritt 3)

In diesem Schritt muss das in Schritt 2 entwickelte Modell verfeinert und die entwickelten Modelle dokumentiert werden. Dies muss iterativ durchgeführt werden. Dies schließt jedes der berücksichtigten Teilsysteme mit ein.

Diese Verfeinerung muss so lange fortgesetzt werden, bis der gewünschte Detaillierungsgrad erreicht ist, d. h. bis alle Informationen für die in Schritt 4 durchzuführenden Analysen enthalten sind (siehe 7.2.4).

- Es ist zwingend notwendig, dass jeder Knoten eindeutig beschriftet ist. Werden zeitbehaftete Netze verwendet, so muss das grundlegende Zeitkonzept symbolisch spezifiziert werden, vorzugsweise mit den Symbolen aus Abschnitt 4.
- Es ist zwingend notwendig, alle weiteren, das Zeitkonzept betreffenden, Details näher zu erläutern, d. h. die spezifischen Parameter (z. B. Gewichte der kausalen Transitionen, feste Zeitdauern, deterministische Transitionen, pdfs mit entsprechenden Parametern der stochastischen Transitionen usw.) sowie alle Transitionsguards, die „preemption policy“, die Stellenkapazität usw. Falls die Lesbarkeit nicht darunter leidet, kann diese Information direkt in das Netz integriert werden. Andernfalls kann dies durch Tabellen oder Matrizen geschehen.

Die Dokumentation dieses Schrittes kann durch schrittweise Verfeinerungen gemäß der Modellierungsverfeinerung erfolgen. Die Dokumentation dieses Schrittes muss Folgendes enthalten:

- eine Petrinetz-Darstellung der Teilsysteme und, sofern angebracht, des ganzen Modells;
- eine verbale Beschreibung der Teilsysteme (zumindest für die unterste Modellierungsebene);
- die Grundlagen der Ausfall- und Wiederherstellungsraten (Annahmen oder statistische Daten) und für die Systemstruktur.

7.2.4 Analyse des Modells auf gesuchte Informationen (Schritt 4)

Bezüglich der Werkzeuge können einige gebräuchliche PN-Werkzeuge unter [1] gefunden werden.

Der zu wählende Ansatz, um das Modell zu analysieren, hängt naturgemäß von der Zielsetzung der Analyse ab. Zudem werden die anwendbaren Analyse-Methoden (siehe Bild 4) durch die zugrunde liegenden Petri-netze und die Verfügbarkeit von Informationen beschränkt. Grundsätzlich unterscheidet man zwischen zwei Alternativen.

- a) Qualitative Analysen beantworten z. B. Fragen bezüglich der Möglichkeit nach der Erreichbarkeit eines (globalen) Zustandes oder danach, eine bestimmte Transitionsreihenfolge wieder und wieder zu schalten.

Qualitative Analysen basieren primär auf dem zeitlosen Erreichbarkeitsgraphen. Ein zeitloser RG kann zumindest theoretisch generiert werden, falls, ausgehend von einer Anfangsmarkierung, nur eine endliche Anzahl an Markierungen erreicht werden kann. Unter bestimmten Bedingungen ist es möglich, von diesem zeitlosen RG auf Eigenschaften der Dynamik für den zeitbehafteten Fall zu schließen (siehe [14]). Ist die Anzahl der erreichbaren Markierungen jedoch zu groß oder gar unendlich, so gibt es alternative Ansätze: Strukturelle Analysen, z. B. Invarianten, Deadlocks und Traps, ermöglichen zumindest Schlüsse über die Qualität des modellierten Systems (siehe [15] und [16]).

- b) Quantitative Analysen beantworten Fragen bezüglich der Wahrscheinlichkeit von qualitativen Ergebnissen, z. B. die Wahrscheinlichkeit, einen bestimmten Zustand zu erreichen oder eine bestimmte Transitionsreihenfolge wieder und wieder zu schalten.

Quantitative Analysen basieren hauptsächlich auf zeitbehafteten oder stochastischen RG. Wie im zeitlosen Fall, kann man auch hier den zeitbehafteten RG untersuchen, sofern die Anzahl der erreichbaren Markierungen nicht zu groß ist. Abhängig von den Transitionen des Petrinetzes gibt es zwei Alternativen.

- i) Falls alle Transitionen im zeitbehafteten PN eine exponential verteilte Schaltdauer haben (d. h. sie haben eine gleich bleibende Schaltrate), kann man den zeitbehafteten Erreichbarkeitsgraphen in eine Markov-Kette überführen und eine stationäre oder transiente Analyse durchführen.
- ii) Andernfalls muss man die Monte-Carlo-Methode benutzen und eine transiente Analyse durchführen.

Ist die Anzahl der erreichbaren Markierungen zu groß, muss man auch die Monte-Carlo-Methode wählen und eine transiente Analyse durchführen.

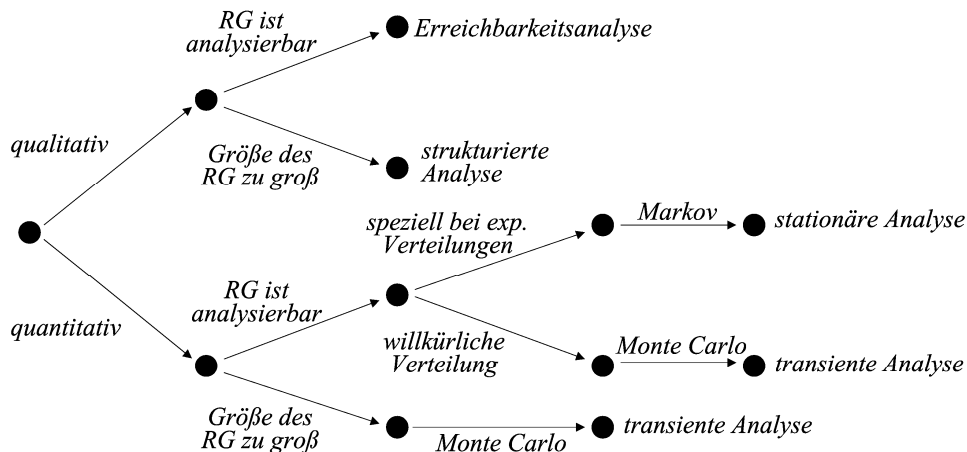


Bild 4 – Angabe der Analysemethode in Abhängigkeit vom PN-Modell

Die Dokumentation dieses Schrittes muss beinhalten:

- a) die (gewählten) Methoden zur Berechnung der erwünschten Ergebnisse müssen skizziert werden;
- b) Die Werkzeuge, die für die Berechnung benutzt wurden, Rechnerumgebung und Bedingungen für die Daten und zur Angleichung müssen angegeben werden.

7.2.5 Darstellung und Interpretation der Ergebnisse der Analyse (Schritt 5)

Die Darstellung dieses Arbeitsschrittes erfordert:

- a) Der Erreichbarkeitsgraph muss adäquat abgebildet sein – im Allgemeinen wird das Konzept der „aggregierten Zustände“ erforderlich sein, da der RG zu groß wird, sollte jeder einzelne Zustand aufgenommen sein.
- b) Die Einflüsse verschiedener Parameterwerte oder Systemstrukturen müssen geeignet dargestellt werden: z. B. der Einfluss unterschiedlicher Instandhaltungs- und Funktionsfähigkeitsgrößen sowie verschiedene Systemstrukturen (z. B. Redundanz-Strukturen) auf die Verfügbarkeit und Sicherheit. Diese können in einem Verfügbarkeits-Sicherheits-Diagramm dargestellt werden (siehe Bild 34).

Die Ergebnisse müssen auf eine klare und deutliche Weise textuell interpretiert werden. Zusätzlich sollten die Analyseergebnisse auf alternative Realisierungsmöglichkeiten (in Hinsicht auf den Systemaufbau oder die Implementierung der Teilmodelle) hinweisen.

7.2.6 Zusammenfassung der Dokumentation (Schritt 6)

Allgemein entspricht die Dokumentation den Voraussetzungen des Qualitätsmanagements. In einigen Gebieten, insbesondere bei sicherheitskritischen Anwendungen, ist eine gesonderte Dokumentation, z. B. im Eisenbahn- und Flugtransportwesen oder in Kernkraftwerken, obligatorisch.

Tabelle 6 – Verbindliche und empfohlene Bestandteile der Dokumentation

Nr.	Schritt	Darstellungsmethoden und Mittel		
		vorgeschrieben	stark empfohlen	empfohlen
1	allgemeine Dokumentation a) allgemeine Beschreibung des Systems, der Funktion, der Teile und der Grenzen b) Zielsetzung und Bereich der Analyse c) Begründung, warum Petrinetze angewendet werden	a) Text und Abbildungen b) Text c) Text		
2	Dokumentation der vier Teilmodelle	Text und Abbildungen	Höhere PN	
3	Detaillierte Dokumentation a) Verfeinerungen der System-Modelle (Abstraktionsebenen) b) Quellen der benutzten Daten (Annahmen oder statistische Daten?) für Ausfall- und Wiederherstellungsraten	a) Text und Abbildungen b) Text	a) Tabellen	
4	Analysemethoden a) Beschreibung der Methoden b) Beschreibung des Computers und benutzter Software	a) Text b) Text	a) Tabellen b) Tabellen	
5	Ergebnisse a) in numerischer und grafischer Form b) Interpretation der Ergebnisse	a) Text und Abbildungen b) Text		

8 Verhältnis zu anderen Modellen der Zuverlässigkeit

Manchmal ist nur die Ursache-Wirkungskette eines beliebigen Ereignisses, wie der Ausfall in einem System, von Interesse. Oder umgekehrt, die Gründe für einen System-Fehlzustand, d. h. ein globaler Zustand mittels eines Basis-Ereignisses oder Zustandes ist von Interesse. Solche Analyseergebnisse erhält man durch FTA, ETA, RBD oder FMEA-Techniken. Der Erreichbarkeitsgraph enthält alle diese Informationen. Also können diese Ursache-Ereignis-Beziehungen aus dem RG abgeleitet werden und auf herkömmliche Weise dargestellt werden (siehe z. B. [10]).

Dies ergibt sich aus der Tatsache, dass die Modellierungsmächtigkeit von PN größer ist als die von FTA, ETA und RBD. Daher kann man zeigen, dass solche Modelle, ohne Informationen zu verlieren, in Petrinetze transformiert werden können (siehe z. B. [10]). Da Markov-Ketten konstante Übergangsraten, was ausschließlich exponential verteilte Zustandsdauer-Verteilungen impliziert, voraussetzen, haben allgemeine stochastische Petrinetze eine höhere Modellierungsmächtigkeit. Die durch eine FMEA oder FMECA gewonnenen Informationen können genutzt werden, um ein PN-Modell zu erstellen. Tatsächlich ist das Durchführen einer FME(C)A ein informeller Prozess und FME(C)As sollten nicht als „Modelle“ bezeichnet werden. Doch als Grundlage, um Daten über das System zu erhalten, können sie ergänzend zu PNs herangezogen werden.

Anhang A (informativ)

Struktur und Dynamik von Petrinetzen

A.1 Allgemeines Petrinetz-Konzept und seine Beziehung zur Zuverlässigkeit

Im Grundsatz können Petrinetze wie folgt charakterisiert und bezogen auf die Zuverlässigkeit interpretiert werden:

Aktive und passive Elemente werden unterschieden (siehe Tabelle 1). Die passiven Elemente nennt man Stellen (en: places), sie modellieren Bedingungen, z. B. unterscheidbare, grundlegende Zustände mit einer bestimmten Verweildauer. Transitionen repräsentieren die aktiven Elemente, die die elementaren (lokalen) Zustände ändern.

Transitionen werden „aktiviert“, sobald die nötigen Bedingungen erfüllt sind, d. h. wenn die entsprechenden Stellen ein Token tragen. Durch Schalten einer Transition, d. h. einem zeitlosen Ereignis, können neue Bedingungen Gültigkeit bekommen und die Vorbedingungen verlieren ihre Gültigkeit.

A.1.1 Petrinetz-Struktur

Da Petrinetze „bipartite“ Graphen sind, ist jede Kante (en: arc) mit zwei unterschiedlichen Knotenarten (en: node) verbunden. Das bedeutet, dass zwischen zwei aufeinander folgenden Zuständen (z. B. „Fehlzustand“ und „in Betrieb“) ein Ereignis existieren muss, welches von einem Zustand in einen anderen überführt (z. B. Instandsetzung). Und zwischen zwei beliebigen Ereignissen (z. B. Ausfall und Instandsetzung) befindet sich stets ein Zustand (z. B. Fehlzustand) – siehe Bild 5. Die Beziehungen zwischen den Zuständen werden mit Hilfe von gerichteten Kanten beschrieben. Der Vorbereich (en: preset) eines Knotens n ist die Menge aller Knoten n' mit einer gerichteten Kante von n' nach n . Der „Nachbereich“ (en: postset) von n ist die Menge aller Knoten n'' mit einer gerichteten Kante von n nach n'' .

Petrinetze modellieren alle relevanten und möglichen Zustände und alle möglichen Ursache-Konsequenz-Relationen, die in Abhängigkeit von Bedingungen, d. h. Mengen von Zuständen, auftreten können.

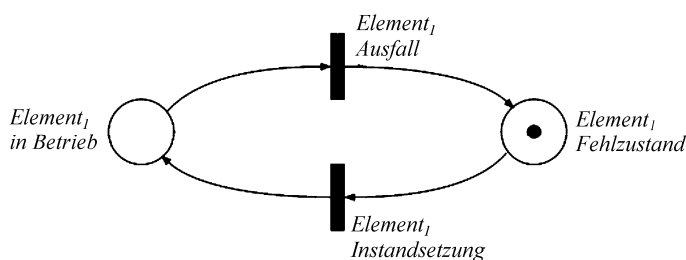


Bild 5 – Funktionsfähigkeit „Zustand-Transition“-Zyklus eines Bauelements

A.1.2 Kausale Dynamik in Low-level-Petrinetzen

In Petrinetzen kann die Dynamik von Systemen durch die Visualisierung der Zustände und dem Wechsel von Systemzuständen in Abhängigkeit ihrer Relationen veranschaulicht werden.

A.1.2.1 Markierung (en: marking)

Stellen können mit Token („schwarze Punkte“) belegt werden, dadurch wird das eigentliche Auftreten eines Zustandes abgebildet (auch „lokale Markierung“). Die Menge aller Markierungen wird „Markierung des Netzes“ (en: net's marking) oder „globale Markierung“ genannt. Bevor eine Transition schaltet, wird die globale Markierung auch „Anfangsmarkierung“ (en: initial marking) genannt.

Die Markierung von Stellen kann durch „Schalten“ oder „Feuern“ von Transitionen verändert werden. Dadurch entsteht die Dynamik der Netze, die durch den „Tokenfluss“ (en: token flow) dargestellt werden kann.

A.1.2.2 Tokenfluss und Schaltregel

Eine Transition ist aktiviert (d. h. sie kann feuern), wenn alle Stellen in ihrem Vorbereich markiert sind. Dabei wird ein Token von jeder Stelle aus dem Bereich vor der Transition entfernt und ein Token auf alle Stellen im Nachbereich erzeugt (siehe Bilder 6 und 7). Im Allgemeinen ändert das Eintreten eines lokalen Ereignisses die lokalen Zustände in der direkten Umgebung. Dies kann folgendermaßen interpretiert werden: tritt ein Ereignis ein (z. B. ein Ausfall ereignet sich), so ändert sich der Zustand des Systems (hier: von „in Betrieb“ zu „Fehlzustand“). Weiterhin können die Transitionen gewichtet werden: Bei einem Zustand mit mehreren aktivierten Transitionen wird die Transition mit der höchsten Gewichtung feuern (siehe [14]).

In Bezug auf die Zuverlässigkeit ändert das Eintreten eines Ausfalls den Zustand des Systems von „in Betrieb“ zu „Fehlzustand“ und der Zustand „Überbelastung“ ist nicht mehr gültig (siehe Bilder 6 und 7).

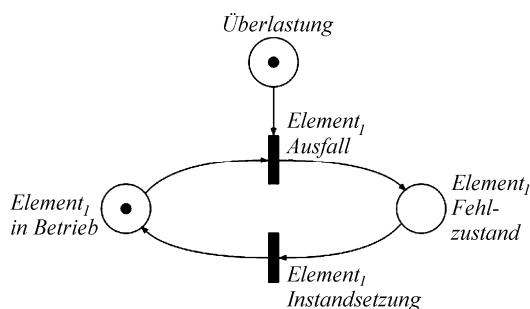


**Bild 6 – Transition „Ausfall“
(en: failure) ist aktiviert**

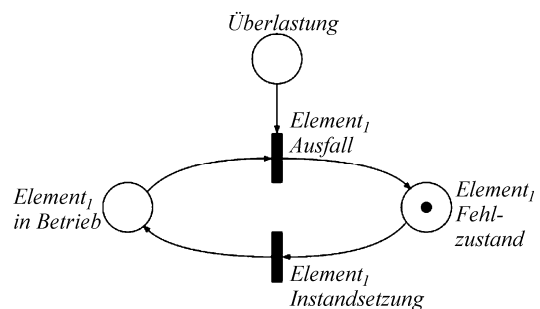


**Bild 7 – Stelle „Fehlzustand“
(en: faulty) wird durch Schalten von
„Ausfall“ markiert**

A.1.2.3 Testkanten

Transitionen, die mit einer Stelle mittels einer „Testkante“ oder „Verbotskante“ verbunden sind, ändern die Anzahl der Token auf dieser Stelle nicht. Testkanten sind als Doppelkanten dargestellt (z. B. zwischen „Instandhaltungspersonal verfügbar“ und „Instandsetzung“ in Bild 8).

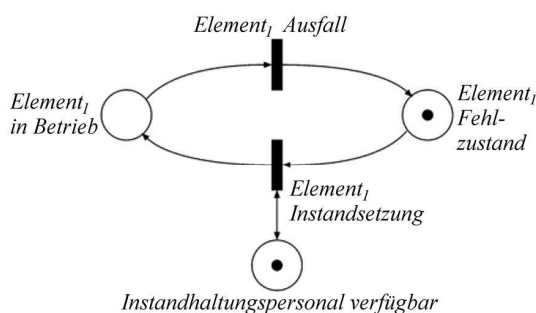


**Bild 8 – Transition „Element₁
Instandsetzung“ ist aktiviert**

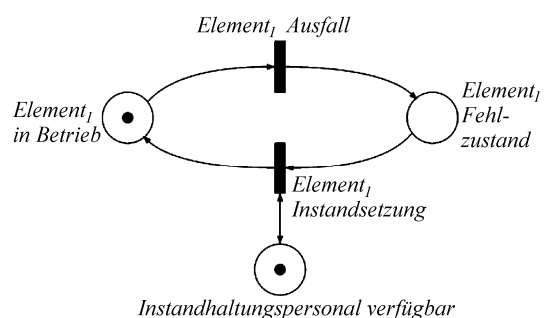


**Bild 9 – Das Token der Stelle
Instandhaltungspersonal
ist nicht verbraucht**

In Bild 8 überprüft die Transition „Instandsetzung“, ob das Instandhaltungspersonal verfügbar ist, d. h. mindestens ein Token muss sich auf dieser Stelle befinden. Hier gelingt der Test. Die Transition ist aktiviert und Feuern führt zur Markierung in Bild 9.

A.1.2.4 Verbotskanten (en: inhibitor arcs)

Transitionen, die durch „Verbotskanten“ (en: inhibitor arcs) mit Vorbereichsstellen verbunden sind, werden nur aktiviert, wenn diese Stellen keine Token tragen. Verbotskanten werden mit einem kleinen Kreis statt einer Pfeilspitze gezeichnet. Ein Schalten einer solchen Transition ändert die Markierung der entsprechenden Stellen im Vorbereich nicht.

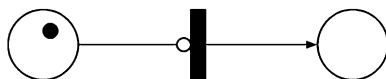


Bild 10 – Transition ist nicht aktiviert

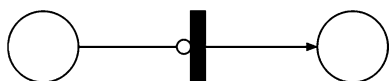


Bild 11 – Markierung vor dem Schalten

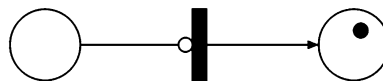


Bild 12 – Markierung nach dem Schalten

Da die Transition in den Netzen der Bilder 10, 11 und 12 nur schaltbereit ist, falls die Stelle in ihrem Vorbereich nicht markiert ist, ist die Transition im Netz in Bild 10 nicht aktiviert. Im Netz in Bild 11 ist die Transition aktiviert und Feuern führt zur Markierung, die im Netz in Bild 12 dargestellt ist. Verbotskanten können, so wie normale Kanten auch, gewichtet werden: Eine n-gewichtete Verbotskante spezifiziert, dass die entsprechende Transition nicht aktiviert ist, wenn die Stelle mit n oder mehr Token markiert ist.

A.1.3 Erreichbarkeitsgraph (en: reachability graph)

Der Erreichbarkeitsgraph (RG) eines Petrinetzes repräsentiert alle globalen Markierungen, die durch Schalten von Transitionen, beginnend mit einer Startmarkierung (en: initial marking), erreicht werden können. Auf diese Weise repräsentiert der RG das mögliche Verhalten eines Systems durch explizites Darstellen seines Zustandsraumes.

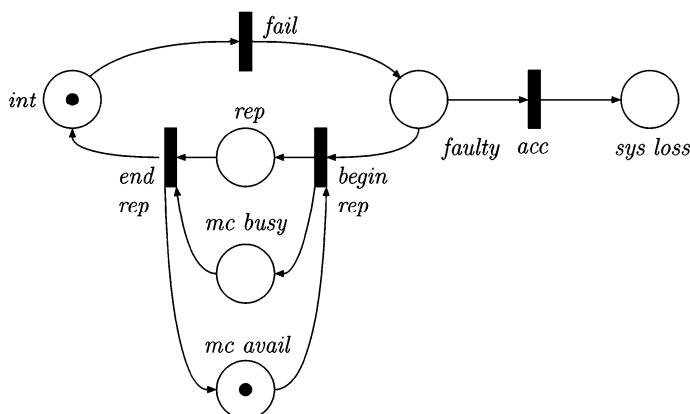


Bild 13 – Ein Petrinetz mit Anfangsmarkierung

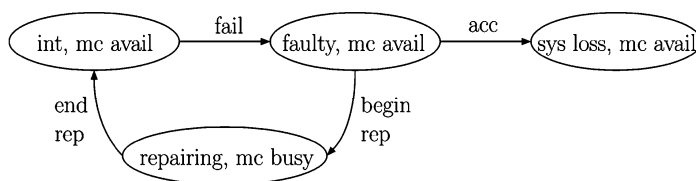


Bild 14 – Der zugehörige RG

Der Raum erreichbarer Zustände des Petrinetzes aus Bild 13 besteht aus vier globalen Zuständen (siehe Bild 14). Jeder globale Zustand ist durch einen Kreis oder eine Ellipse dargestellt, der eindeutig durch die momentane Netzmarkierung spezifiziert ist. Aufgrund der Kantenbeschriftungen spezifiziert der RG, wie der Übergang von einem globalen Zustand in einen anderen vollzogen wird. Bei komplexeren Petrinetzen kann die Anzahl der globalen Zustände innerhalb des RG steigen. Die Erstellung seines RG kann mit Hilfe von Computerprogrammen automatisch erfolgen.

Die folgende Tabelle gibt einen Überblick über sich entsprechende Konzepte bei Systemen im Allgemeinen, Petrinetzen, Erreichbarkeitsgraphen und Zuverlässigkeitskonzepten

Tabelle 7 – Dazugehörige Bezeichnungen in Systemen, Petrinetzen und Erreichbarkeitsgraphen

Aspekt	System	Petrinetz	Erreichbarkeitsgraph	Zuverlässigkeit
Dynamisch	Ereignis	Transition	Kante	Zum Beispiel: Ausfallereignisse oder Fehlerbehandlung
Statisch	lokaler Zustand	Stelle		lokaler Zustand
	globaler Zustand	Markierung = Menge der markierten Stellen	Knoten	globaler Zustand (z. B. Wartung, Gefährdung)
	aggregierter globaler Zustand	Menge von Markierungen	Menge der Knoten	Menge der globalen Zustände (z. B. verfügbar, sicher)

Beispiel

Im Petrinetz der Bild 15 ist die Transition „Element_{lp} Instandsetzung“ (Abkürzung für „Element_{low-priority} Instandsetzung“) aktiviert, weil die Stelle „Element_{low-priority} Fehlzustand“ markiert ist, Instandsetzungs-personal verfügbar ist und die „Element_{hp} in Betrieb“ (Abkürzung für „Element_{high-priority} in Betrieb“) aktiviert, da die Bedingung durch „Element_{high-priority} in Betrieb“ erfüllt ist.

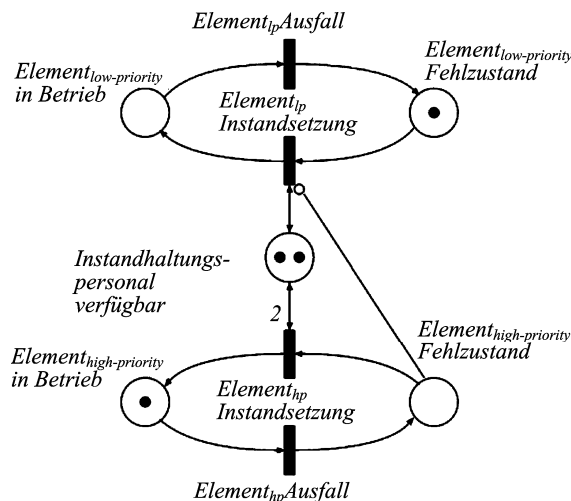


Bild 15 – Transitionen „Element_{lp} Instandsetzung“ und „Element_{hp} Ausfall“ sind aktiviert

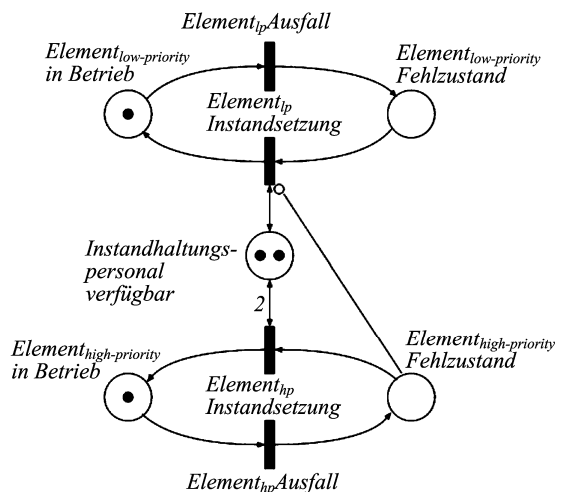


Bild 16 – Markierung nach Schaltung der Transition „Element_{lp} Instandsetzung“

Das Schalten von „Element_i Instandsetzung“ verbraucht ein Token der Stelle „Element_ilow-priority Fehlzustand“ und erzeugt ein Token an der Stelle „Element_ilow-priority in Betrieb“. Da die Stellen „Element_ihigh-priority Fehlzustand“ und „Instandhaltungspersonal verfügbar“ mit der Transition „Element_i Instandsetzung“ durch Test- bzw. Verbotskanten verbunden sind, werden die Markierungen dort nicht verändert (siehe Bild 16).

A.2 Zeitbehaftete Petrinetze

Für Anwendungen in der Zuverlässigkeit ist es sinnvoll, auch zeitliche Aspekte in die Modellierung zu integrieren, z. B. werden Zuständen bestimmte Verfügbarkeits- und Unverfügbarkeitszeiten zugeordnet. Im Gegensatz dazu werden Zustandsänderungen bzw. deren Raten den Transitionen zugeordnet. Hier muss zwischen deterministischem und stochastischem Verhalten unterschieden werden. Diese zwei wesentlichen Kategorien können in zeitbehafteten Petrinetzen mit deterministischen Zeitparametern (z. B. deterministische Dauern von Ereignissen) und stochastischen Zeitparametern (z. B. Exponentialfunktion mit entsprechenden Raten) mit Transitionen dargestellt werden (für stochastische zeitbehaftete PN: siehe [12] und [14]). In allen Fällen gilt, dass Eigenschaften von Transitionen durch unterschiedliche Beschriftungen und zusätzlichen Bedingungen dargestellt werden.

A.2.1 Spezifische Transitionen für zeitbehaftete, niedrige Petrinetze

In zeitbehafteten PN werden beide, zeitlose wie zeitbehaftete Transitionen verwendet. Grundsätzlich gilt für zeitbehaftete Transitionen die gleiche Schaltregel wie für zeitlose Transitionen (siehe die oben genannten zeitlosen Petrinetze). Eine zeitbehaftete Transition muss für einen bestimmten Zeitraum aktiviert sein. Dieser Zeitraum kann deterministisch oder stochastisch sein, abhängig von der Transitions-spezifischen Verteilungsfunktion (pdf = transition-specific distribution function) und ihren Parametern. Nach Ablauf der Zeitspanne darf die Transition feuern. Tabelle 3 zeigt die üblich genutzten Transitionen in zeitbehafteten Petrinetzen.

Entsprechend des spezifischen Typs einer zeitbehafteten Transition ist sie mit einem Zeitparameter attribuiert, der die deterministische Schaltdauer, die (konstante) Schaltrate oder die Wahrscheinlichkeitsverteilung mit ihren Parametern spezifiziert.

A.2.2 Dynamik in zeitbehafteten niedrigen Petrinetzen

Auch in zeitbehafteten Petrinetzen wird die Systemdynamik durch den Markierungsfortschritt modelliert, der durch den zugehörigen RG repräsentiert wird (siehe Bild 14). Entsprechend der verschiedenen Transitionsraten oder stochastischen Verteilungen werden die Zustandsübergangs-Kanten durch ihre spezifischen Zeitsymbole beschriftet. Jeder globale Zustand, der einen bestimmten zuverlässigkeitsbezogenen Zustand modelliert, wird durch eine bestimmte Wahrscheinlichkeit attribuiert, die sich aus dem zeitlichen Verhalten der Transition, z. B. durch stochastisches Feuern, ergibt. Seine Berechnung wird in Kapitel 6 skizziert. Man kann beweisen, dass jedes endliche und markierte stochastische Petrinetz isomorph zu einer Markov-Kette mit diskretem Zustandsraum ist [15].

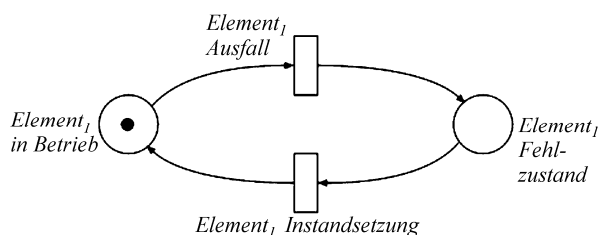


Bild 17 – Ein zeitweitertertes PN mit exponential verteilten, zeitbehafteten Transitionen

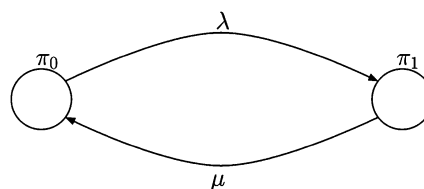


Bild 18 – Der zugehörige stochastische Erreichbarkeitsgraph

In Bild 17 werden die Transitionen mit ihren Raten abgebildet. In Bild 18 sind die globalen Zustände mit π_0 bzw. π_1 benannt.

Beispiel

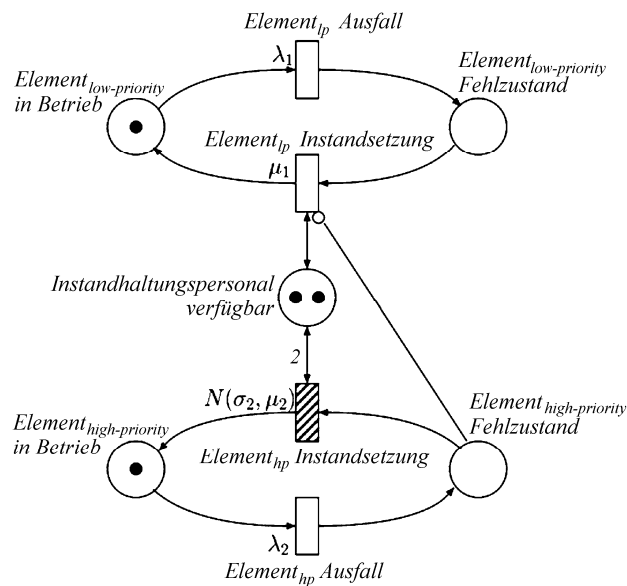


Bild 19 – Petrinetz mit zeitbehafteten Transitionen

Die Transition „Element_{lp} Ausfall“ schaltet mit der Rate λ_1 , d. h. ist dieses Bauelement erst einmal in Betrieb (gekennzeichnet als „Element_{low-priority} in Betrieb“), so verbleibt es für eine exponential verteilte Zeit in diesem Zustand. Wenn Element_{hp} im Fehlzustand ist, verbleibt es dort für eine normal verteilte Zeit (gekennzeichnet durch σ_2, μ_2).

A.2.3 Verschiedene Kategorien von zeitbehafteten Petrinetzen

Es gibt viele Unterklassen von stochastischen Petrinetzen. In einer ersten Klassifizierung kann man sagen, dass die Klasse von der Wahl der Schaltzeitverteilung abhängt, die einen maßgeblichen Einfluss auf die möglichen Analysen hat.

Die folgenden Klassen sind in der Literatur verbreitet (siehe [12]):

- verallgemeinerte stochastische Petrinetze (en: GSPN = generalized stochastic Petri nets): alle zeitbehafteten Transitionen sind exponential verteilt;
- Markov'sche SPN (MSPN): SPNs, für die der zugrunde liegende stochastische Prozess eine Markovkette ist. Dies ist der Fall, wenn alle zeitbehafteten Transitionen entweder eine exponential verteilte oder eine geometrisch verteilte Schaltzeit haben. Der erstgenannte Fall entspricht den GSPNs;
- deterministische und stochastische Petrinetze (en: DSPN = deterministic and stochastic Petri nets): die zeitbehafteten Transitionen sind entweder exponential oder deterministisch, und die deterministischen Transitionen schließen sich gegenseitig aus und besitzen eine besondere preemption policy;
- Markov regenerative stochastische Petrinetze (en: MRSPN = Markov regenerative stochastic Petri nets): SPNs, bei denen der zugrunde liegende stochastische Prozess ein Markov-regenerative-Prozess ist. Eine Unterklasse, auch als erweiterte DSPN bekannt, ist durch SPNs vorgegeben, bei der die zeitbehafteten Transitionen entweder exponentiell verteilt sind oder eine allgemeine Verteilung besitzen und sich die allgemein verteilten Transitionen gegenseitig ausschließen und eine besondere preemption policy haben.
- nicht-Markov'sche stochastische Petrinetze: jedes stochastische Petrinetz, das nicht Markov'scher Natur ist.

A.3 Methoden zur Analyse von Petrinetzen

Allgemein existieren zwei grundsätzlich verschiedene Analysearten:

- a) qualitative Analysen behandeln Fragen bzgl. Möglichkeiten, wie „Ist es möglich, einen bestimmten Zustand zu erreichen?“ oder „Ist es möglich, dass ein bestimmtes Ereignis eintreten kann?“
- b) quantitative Analysen behandeln u.a. Fragen zur Wahrscheinlichkeit, wie „Wie hoch ist die Wahrscheinlichkeit, einen bestimmten Zustand zu erreichen?“ oder „Wie wahrscheinlich ist es, dass ein bestimmtes Ereignis eintritt?“

Aus diesem Grund können Analysen in qualitative und quantitative unterschieden werden.

A.3.1 Qualitative Analyse

Qualitative Analysen können in strukturelle und dynamische Analysen unterteilt werden.

– Strukturelle Analysen berücksichtigen nur die Struktur von Petrinetzen, der RG bleibt unberücksichtigt. Daher sind solche Analysen von der Anfangsmarkierung unabhängig. Der Vorteil solcher Analysen ist, dass die Ergebnisse für jede beliebige Anfangsmarkierung gültig sind. Der Nachteil ist, dass die Ergebnisse oft sehr allgemein sind. Invarianten, Deadlocks und Traps sind bekannte strukturelle Eigenschaften von Petrinetzen (siehe [16]).

– Dynamische Analysen arbeiten mit dem RG eines Petrinetzes. Da der RG von der Anfangsmarkierung abhängt, hängen auch die Ergebnisse von der Anfangsmarkierung ab. Der Vorteil solcher Analysen ist, dass falls der RG erzeugt und damit gearbeitet werden kann, jede qualitative Frage beantwortet werden kann. Der Nachteil hierbei ist, dass es aufgrund seiner Größe oftmals nicht möglich ist, den RG zu erstellen. Dynamische Analysen identifizieren z. B., ob ein gefährlicher oder unbeabsichtigter Zustand erreicht werden kann (siehe [11]).

A.3.1.1 Quantitative Analyse

Häufig stehen Zuverlässigkeitsmerkmale und ihre Maße, wie die „steady-state“ oder „transiente“ Wahrscheinlichkeit des Systembetriebs, im Mittelpunkt des Interesses. Viele der Methoden und Algorithmen, die zur Durchführung einer quantitativen Analyse notwendig sind, haben ihren Ursprung in der Wahrscheinlichkeitstheorie. Selbstverständlich muss man die notwendigen Wahrscheinlichkeitsverteilungen näher bestimmen, bevor man mit den Analysen beginnen kann. Gibt es nur exponentielle Verteilungen im Systemmodell, handelt es sich um ein Markov'sches Modell. Zur Lösung eines solchen Modells können alle Analyseansätze für Markov-Ketten genutzt werden. Ist das Modell nicht Markov'sch, sind andere Methoden notwendig.

A.3.1.1.1 Analyse von Markov'schen Modellen

Um Analysemethoden für stetige Markov-Ketten (en: CTMC = Continuous Time Markov Chains) anzuwenden, muss ein PN in ein CTMC transformiert werden. Hierzu ist es notwendig, dass das stochastische PN ein GSPN ist. Zwei mögliche Lösungen für Markov-Ketten sind von Interesse (siehe [5]): transiente- und „steady state“-Analysen. Die transiente Lösung erhält man durch Lösen der „Kolmogorov-Piscounov-Differentialgleichung“ und die „steady-state“-Lösung erhält man durch Lösen eines linearen Gleichungssystems. Geschlossene analytische Lösungen sind sowohl für sehr strukturierte Markov-Ketten als auch für sehr kleine Markov-Ketten möglich. In den meisten anderen Fällen muss man auf numerische Lösungsansätze zurückgreifen. Es gibt viel Literatur zur Lösung von Markov'schen Modellen. Wir verweisen den Leser auf [11] und [IEC 61165].

A.3.1.1.2 Transiente Analyse

Es seien $p_0(t)$, $p_1(t)$ die Wahrscheinlichkeiten dafür, dass sich das System zum Zeitpunkt t in den Zuständen π_0 bzw. π_1 befindet (siehe Bild 17 für die PN-Darstellung und Bild 18 für die dazugehörige Markov-Kette). Dann wird die Wahrscheinlichkeitsdynamik des Systems ausgedrückt durch:

$$\frac{dp_0(t)}{dt} = -\lambda \cdot p_0(t) + \mu \cdot p_1(t) \quad (1)$$

$$\frac{dp_1(t)}{dt} = \lambda \cdot p_0(t) - \mu \cdot p_1(t) \quad (2)$$

Die analytische Lösung mit $p_0(0) = 1$ und $p_1(0) = 0$ beschreibt die Wahrscheinlichkeit der einzelnen Zustände zum Zeitpunkt t .

$$p_0(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} \cdot e^{-(\mu + \lambda)t} \quad (3)$$

$$p_1(t) = \frac{\mu}{\mu + \lambda} - \frac{\lambda}{\mu + \lambda} \cdot e^{-(\mu + \lambda)t} \quad (4)$$

A.3.1.1.3 „Steady-State“-Analyse

Das System befindet sich in einen eingeschwungenen Zustand, wenn $\lim_{t \rightarrow \infty} p(t)$ existiert und

$$\dot{p} = p \cdot Q = 0; \quad (5)$$

dabei ist $Q = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$ die Transitions-Raten-Matrix, die vom RG oder vom aggregierten RG (siehe Anhang D) abgeleitet werden kann.

Der stationäre Wahrscheinlichkeitsvektor p einer nicht reduzierbaren CTMC einer ergodischen Menge von Zuständen ist eindeutig und kann durch Lösen von

$$p \cdot Q = 0$$

unter der Normalisierungsbedingung $p \cdot \mathbf{1} = 1$ berechnet werden.

A.3.1.2 Analyse von nicht-Markov'schen Modellen

Wird auf die Annahme der Exponentialverteilung verzichtet, können die zugrunde liegenden Modelle mithilfe verschiedener Techniken berechnet werden:

- Markov Renewal Theory:
Bei diesem Ansatz werden Prozesse zu bestimmten Zeitinstanzen betrachtet, bei denen die Prozesse „gedächtnislos“ sind. Man geht davon aus, dass sich ein Prozess in diesen Zeitinstanzen erneuert und dass ein anderer Prozess in diesen Zeitinstanzen eingebettet ist. Es ist möglich, die Zustandsgleichungen des eingebetteten Prozesses auszudrücken und daraus eine Lösung des aktuellen Prozesses abzuleiten, siehe [12].
- Monte-Carlo-Methode:
Die Monte-Carlo-Methode ist eine Methode, um Schätzungen für die Lösung von mathematischen Problemen mittels Zufallszahlen zu erhalten. Diese Methode beruht auf der wiederholten Berechnung von Zufallsvariablen. Der Vorteil dieses Ansatzes besteht darin, dass es auf eine realitätsnahe Weise möglich ist, viele eventuell auftretende Phänomene ohne Verkomplizierung des Lösungsprozesses zu berücksichtigen. Der grundsätzliche Nachteil besteht im Konflikt zwischen der notwendigen Berechnungszeit und der benötigten Genauigkeit.
- Coxian-Stage-Type-Verteilung: Im Jahre 1955 hat Cox [11] gezeigt, dass eine Zufallsvariable X , deren Verteilungsfunktion $F_X(x)$ eine rationale Laplace-Transformierte als seriell-paralleles Netzwerk von Stufen dargestellt werden kann, indem die Zeitverteilung jeder Stufe eine andere negative Exponentialverteilung besitzt.

A.3.1.3 Reward-Funktionen

Auf der Ebene stochastischer Prozesse sind „rate rewards“ Werte, die akkumuliert werden, wenn das Modell Zeit in einem Zustand verbringt, und „impulsiv rewards“ sind Werte, die man erhält, wenn Transitionen in bestimmten Markierungen schalten. Rate rewards können auf Basis der Zustandswahrscheinlichkeiten berechnet werden, während die Berechnung von „impulse rewards“ auf der Basis der Schaltfrequenzen der Transitionen beruht (siehe [12]). Diese Konzepte ermöglichen es, Kosten und Nutzen (en: rewards) bezogen auf Fehlzustände und „In-Betrieb“-Zustände auf einfache Weise zu modellieren. Außerdem können so Reparaturkosten auf einfache Weise berücksichtigt werden.

Tabelle 8 – Stellen und Transitionen mit Belohnung

<i>Bezeichner (rr)</i>	<i>Bezeichner (ir)</i>
	
Stelle mit „rate reward“	Transition (exponential verteilt) mit „impulse reward“

Anhang B (informativ)

m aus n

B.1 Lokale und globale Zustände

Die Fähigkeit jedes Elements (en: component), eine Funktion auszuführen, kann in Petrinetzen durch einen Zustandsübergangs-Zyklus modelliert werden, um die Zuverlässigkeit auszudrücken (z. B. „in Betrieb“ und „Fehlzustand“ – siehe Bild 2).

Das so entstandene System-Zuverlässigkeitsmodell zeigt die kombinatorische Menge der lokalen Zuverlässigkeiten der Elemente durch globale Zustände (siehe Bilder 20 und 21 für ein System bestehend aus zwei Elementen und keiner Beziehung zwischen diesen, und Bilder 22 und 23 für ein System aus drei Elementen, ebenfalls ohne Beziehungen). Diese werden abgeleitet durch Erstellen des Erreichbarkeitsgraphen des gesamten Netzes; hier sind alle globalen Zustände des Systems dargestellt.

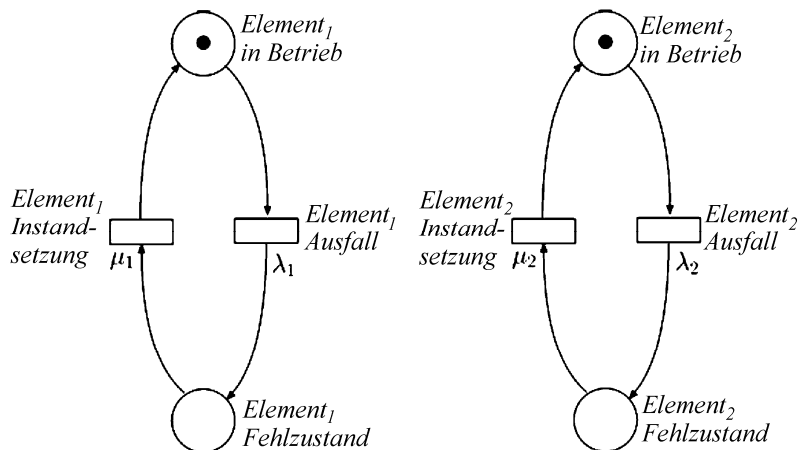


Bild 20 – Zuverlässigkeitsnetze zweier Elemente mit spezifischen Ausfall- und Instandsetzungsraten

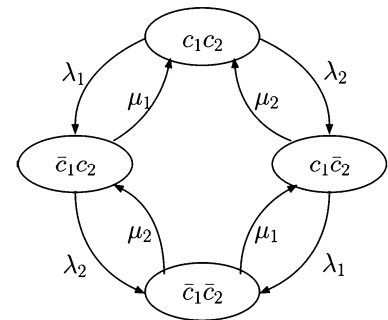


Bild 21 – stochastischer RG von Bild 20 (als Abkürzung wird $\bar{c}_i$ für „Element_i Fehlzustand“ genutzt)

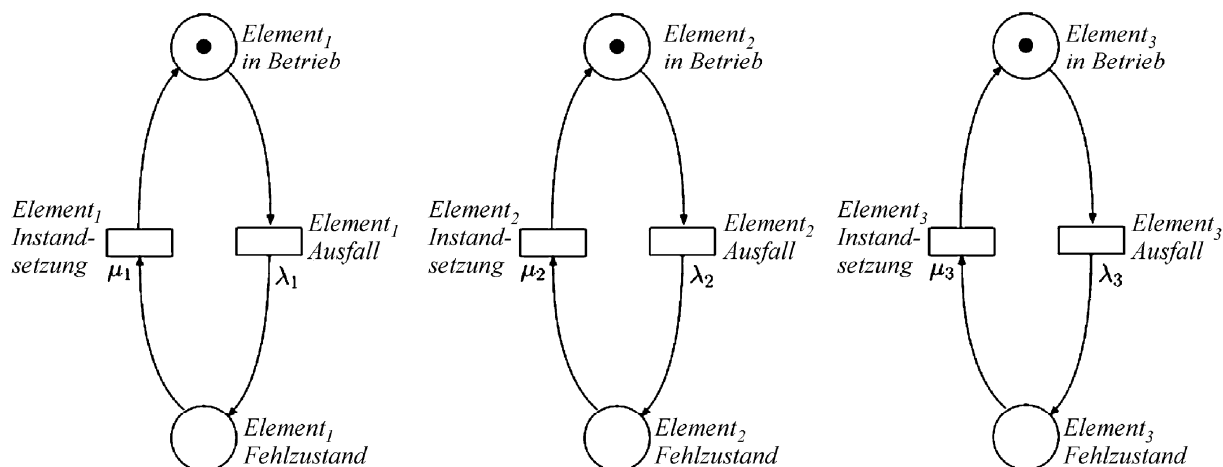


Bild 22 – Zuverlässigkeitsnetze zweier Elemente mit spezifischen Ausfall- und Instandsetzungsraten

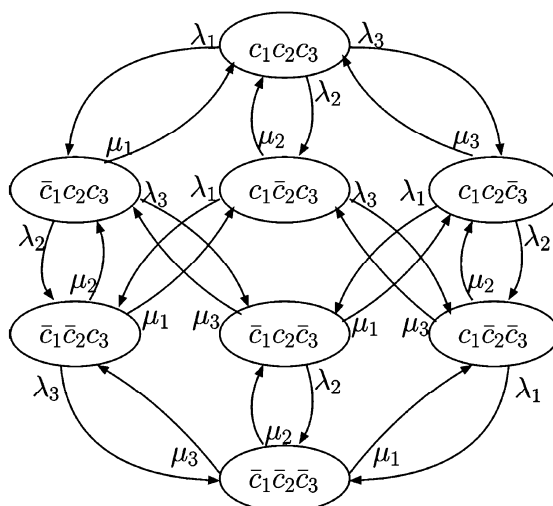


Bild 23 – Stochastischer RG von Bild 22
(als Abkürzung wird $\bar{c}_i$ für „*Element_i Fehlzustand*“ genutzt)

B.2 Globale Zustände und Systemaufbau

Für die Implementierung einer komplexen, funktionalen Systemstruktur, die durch verschiedene verbundene Elemente verwirklicht wird (die wiederum selbst Teilfunktionen realisieren), müssen entsprechende Instanzen des elementaren Modellierungskonzepts mit Rücksicht auf die Gesamtstruktur des Systems verknüpft werden, z. B. serielle-, Redundanzstrukturen. Gemäß dieser logischen Struktur, zeigt der RG implizit alle globalen Zustände der Systemverfügbarkeit und -unverfügbarkeit. Die Bilder 24, 25 und 26 zeigen die Modellierung der Zuverlässigkeitsstrukturen von 1oo3(1-aus-3)-, 2oo3- und 3oo3-Systemen.

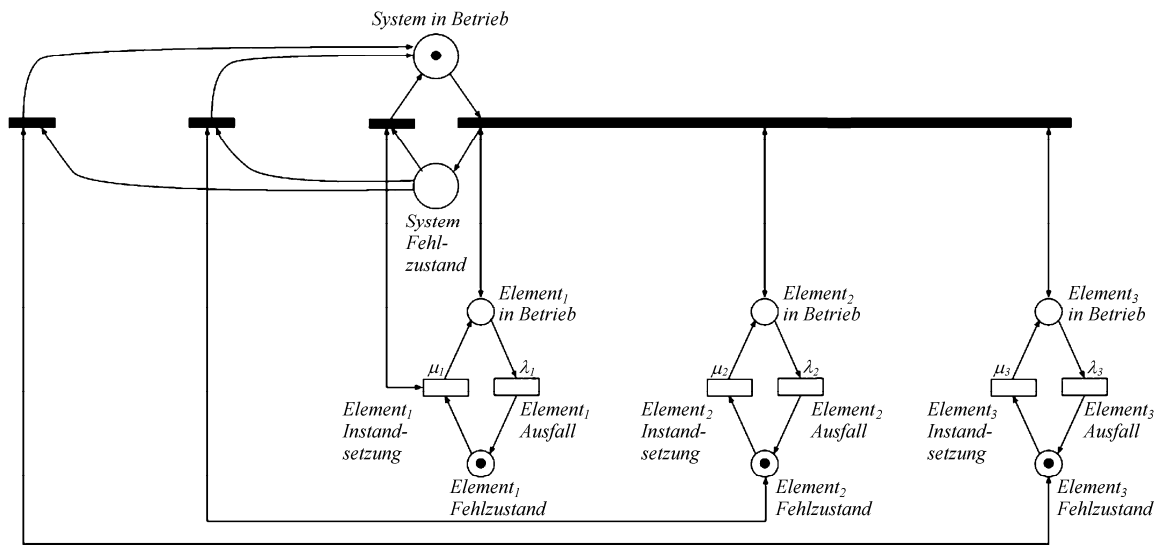


Bild 24 – Spezifisch verbundenes 1-aus-3-Zuverlässigkeitsnetz

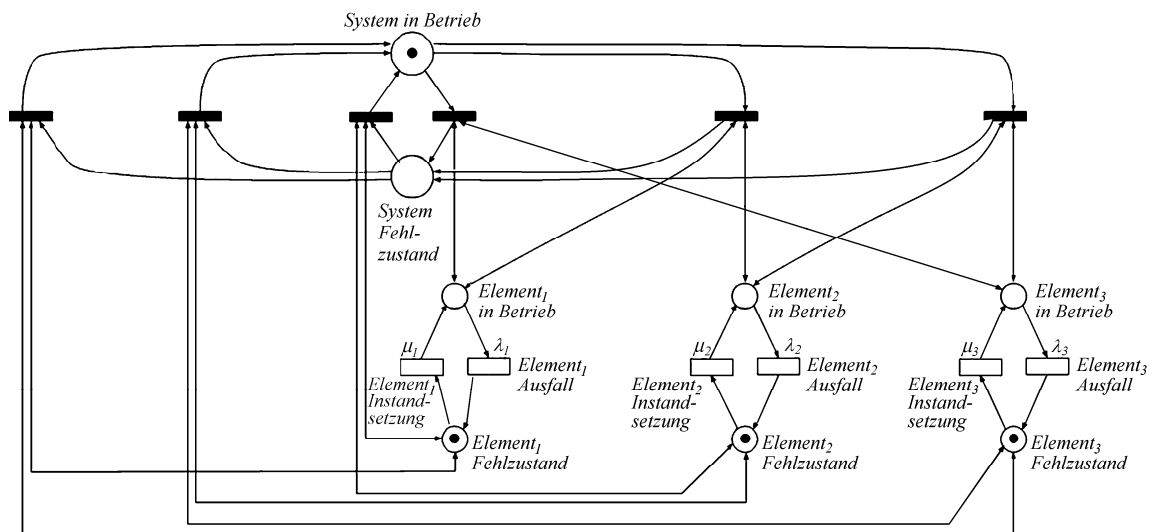


Bild 25 – Spezifisch verbundenes 2-aus-3-Zuverlässigkeitsnetz