

Modellierung hochverfügbarer Systeme unter Berücksichtigung von stochastischen Abhängigkeiten zwischen den Komponenten mit OpenSESAME

Max Walter, Carsten Trinitis
Lehrstuhl für Rechnertechnik und Rechnerorganisation (LRR)
Fakultät für Informatik der Technischen Universität München
Boltzmannstrasse 3
D-85747 Garching bei München
Tel.: +49 (0)89 289 18456
Fax: +49 (0)89 289 17662
E-Mail: walterm@in.tum.de

Zusammenfassung: Das Werkzeug OpenSESAME (Simple but Extensive Structured Availability Modeling Environment) erlaubt die Modellierung der Verfügbarkeit komplexer fehlertoleranter Systeme. Als Eingabe dienen die Eigenschaften der Komponenten des Systems (MTTF- und MTTR-Werte), die Redundanzstruktur in Form von Blockdiagrammen, sowie Informationen über stochastische Abhängigkeiten zwischen den Komponenten des Systems. Durch die Berücksichtigung dieser Abhängigkeiten werden über-optimistische Ergebnisse vermieden, wie sie bei der Verwendung von klassischen Methoden (z. B. herkömmliche Blockdiagramme und Fehlerbäume) auftreten.

Stichworte: Zuverlässigkeitsbewertung, hochverfügbare Systeme, Blockdiagramme, Markovketten, Petrinetze, Werkzeuge

1 Einleitung

Die Verfügbarkeit von fehlertoleranten Systemen wie zum Beispiel Internetservern oder Vermittlungsstellen im Telefonnetz wird üblicherweise mit Hilfe von stochastischen Modellen aus den Eigenschaften ihrer Komponenten abgeschätzt. Weit verbreitet sind in diesem Umfeld kombinatorische Methoden wie zum Beispiel Fehlerbäume und Blockdiagramme. Diese Methoden sind leicht zu erlernen, intuitiv anwendbar und werden durch eine Reihe von ausgereiften, effizienten Computerwerkzeugen unterstützt (siehe, z. B. [Schn99]).

Ein gravierender Nachteil dieser Methoden ist jedoch, dass die klassischen Algorithmen zur Auswertung solcher Modelle auf der Annahme basieren, dass zwischen den Komponenten des Systems keine stochastischen Abhängigkeiten bestehen. Dies ist in der Realität jedoch nicht der Fall. Die Verwendung von kombinatorischen Modellen führt daher zu über-optimistischen Ergebnissen.

Aus diesem Grund werden – insbesondere im Bereich sicherheitskritischer Systeme – vermehrt Zustandsraum-basierte Methoden wie Markovketten, stochastische Petrinetze oder stochastische Prozessalgebren eingesetzt. Mit Hilfe dieser Methoden können stochastische Abhängigkeiten berücksichtigt werden, allerdings geht dies auf Kosten der Benutzerfreundlichkeit. Die Verwendung der Methoden erfordert eine fundierte Kenntniss der mathematischen Hintergründe und formalen Definitionen der eingesetzten Modelle (näheres, z. B. in [AjBaCo95], [GeKeZi95] und [Lind98]). Dies hat einer weiten Verbreitung in Industrie und Praxis bisher im Wege gestanden.

Das hier vorgestellte Werkzeug OpenSESAME (Simple but Extensive Structured Availability Modeling Environment) zielt darauf ab, die Handhabung Zustands-basierten Methoden erheblich zu erleichtern, um sie einem breiten Kreis von Ingenieuren zugänglich zu machen.

Zu diesem Zweck stellt das Werkzeug dem Nutzer eine intuitive Benutzeroberfläche zur Verfügung, die in Abschnitt 2 näher beschrieben ist. Die mit Hilfe dieser Oberfläche erstellten Diagramme und Tabellen werden zur Analyse automatisch in ein entsprechendes Zustands-basiertes Modell umgewandelt und ausgewertet (Unter Verwendung des Werkzeugs DSPNexpress [Lind98]). Details zum Umwandlungsvorgang sind in [WaTr04] und [WaSc05] beschrieben. Die Ergebnisse werden im Kontext des Eingabemodells präsentiert. Auf diese Weise ist es möglich, die Mächtigkeit der Zustands-basierten Methoden nutzen zu können, ohne sich das entsprechende Expertenwissen aneignen zu müssen.

2 OpenSESAME-Eingabediagramme

Das Werkzeug OpenSESAME besitzt eine intuitive Benutzeroberfläche, die trotz der hohen Mächtigkeit des Werkzeuges leicht zu erlernen und zu bedienen ist. Insbesondere Nutzer, die bereits mit klassischen, auf Blockdiagrammen basierenden Werkzeugen gearbeitet haben, können sofort mit der Erstellung von OpenSESAME Modellen beginnen.

Dazu werden zunächst die Komponenten spezifiziert, aus denen das System besteht. In einer Komponententabelle (component table, CT) kann zu jedem Komponententyp die mittlere Lebensdauer (mean time to failure, MTTF), die mittlere Reparaturdauer (mean time to repair, MTTR) sowie die Anzahl der Komponenten dieses Typs angegeben werden.

Die Definition der Redundanzstruktur des Systems erfolgt mit Hilfe von Blockdiagrammen (reliability block diagrams, RBD). OpenSESAME unterstützt beliebige Blockdiagramme, d.h. die Diagramme können auch Brücken enthalten; außerdem können mehrere Kanten eines Blockdiagramms mit ein und derselben Komponente attribuiert werden. Es können daher auch z. B. k -aus- N : G -Systeme¹ modelliert werden. Jedes Blockdiagramm besitzt bei seiner Erzeugung zwei spezielle Knoten s und t . OpenSESAME berechnet im Regelfall die Wahrscheinlichkeit, dass

¹ Ein k -aus- N : G -System besteht aus N Komponenten und ist genau dann verfügbar, wenn wenigstens k Komponenten verfügbar sind.

es eine Verbindung zwischen diesen beiden Knoten gibt (sog. terminal pair availability). Es können jedoch beliebig viele weitere Knotenpaare definiert werden, die alle in einem Lösungsdurchgang evaluiert werden.

Bei großen Systemen empfiehlt sich die Aufteilung der Redundanzstruktur auf mehrere Blockdiagramme, um das Modell übersichtlicher zu gestalten. Dazu erlaubt das Werkzeug eine hierarchische Anordnung mehrerer Blockdiagramme: jede Kante eines Blockdiagramms kann mit einer Referenz auf ein Unterdiagramm attribuiert werden. k-aus-N:G-Systeme, oder Systeme, die k-aus-N:G-Systeme als Komponenten besitzen, können mit Hilfe von sog. k-aus-N:G-Kanten besonders einfach und kompakt modelliert werden. Wie alle Parameter in OpenSESAME können für die Werte k und N neben Konstanten auch freie Variablen eingesetzt werden. So ist es möglich, durch verschiedene Substitutionen in mehreren Analyseläufen die Auswirkung dieser Parameter auf die Gesamtverfügbarkeit des Systems zu untersuchen.

Mit der Definition der Komponenten und der Redundanzstruktur des Systems ist bereits eine erste Analyse des Modells möglich. Wie bei herkömmlichen Werkzeugen erfolgt diese aber unter der Annahme, dass die Lebens- und Reparaturzeiten der einzelnen Komponenten paarweise stochastisch unabhängig voneinander sind. Im Gegensatz zu herkömmlichen Methoden erlaubt OpenSESAME deshalb die Anreicherung des Modells mit diesen Abhängigkeiten, um realistischere Ergebnisse zu erhalten.

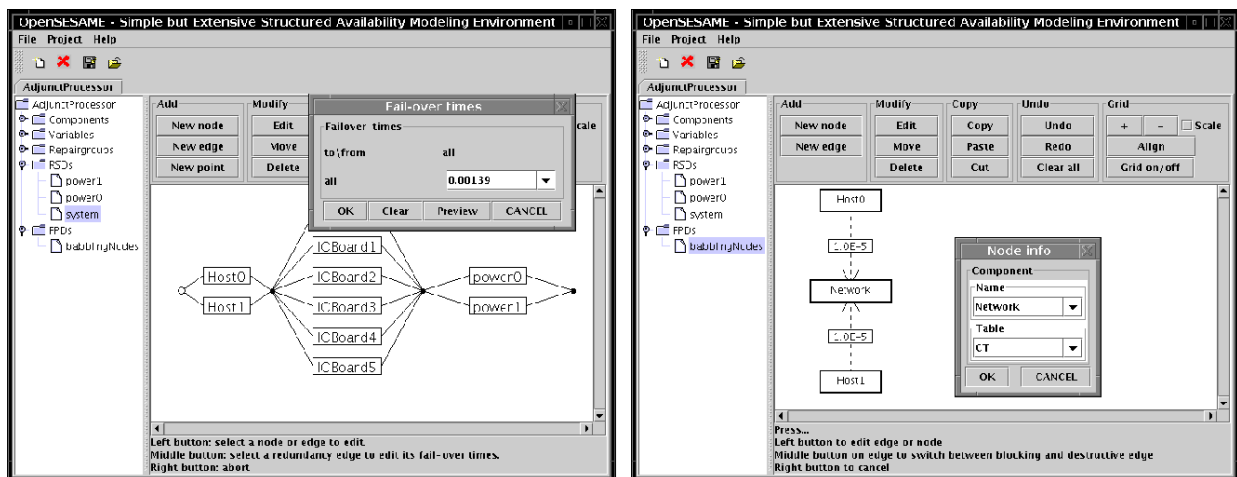


Abb. 1: Blockdiagramm (links) und Fehlerabhängigkeitsdiagramm (rechts).

3 Modellierung stochastischer Abhängigkeiten

OpenSESAME-Modelle können schrittweise um stochastische Abhängigkeiten ergänzt werden. Der Editieraufwand zum Einfügen solcher Abhängigkeiten ist unabhängig von der Größe des Modells, so dass auch große Modelle schnell um Abhängigkeiten erweitert werden können.

Eine Reihe von Abhängigkeiten kommt nur zwischen redundanten Komponenten in fehlertoleranten System vor. Dazu zählen insbesondere Umschaltzeiten bei Systemen mit warmer oder kalter Reserve. Bei diesen Systemen gibt es zwischen dem Ausfall der Primärkomponente und der Aktivierung der Sekundärkomponente ein Zeitintervall, bezeichnet als failover-time, während dessen das Gesamtsystem nicht verfügbar ist. Herkömmliche Modelle vernachlässigen dieses Zeitintervall, was zu überoptimistischen Ergebnissen führt. Die k-aus-N-Kanten von OpenSESAME-Modellen können jedoch mit einer entsprechenden failover-Zeit attribuiert werden.

Eine weitere Klasse von Abhängigkeiten bezieht sich auf das Ausfallverhalten der Komponenten. Beispiele sind gemeinsame Fehlerquellen und Fehlerfortpflanzung. Diese können – unabhängig von der Redundanzstruktur des Systems – zwischen beliebigen Komponenten des Systems auftreten. Es ist deshalb nicht sinnvoll, die Blockdiagramme um diese Informationen anzureichern. Die OpenSESAME-Modellierungsumgebung bietet daher neuartige Diagramme, die speziell zur Beschreibung von Fehlerabhängigkeiten entwickelt wurden.

Diese Fehlerabhängigkeitsdiagramme (failure dependency diagrams, FDD) sind gerichtete Graphen, deren Knoten Komponenten und deren Kanten Fehlerabhängigkeiten symbolisieren. Jede Kante ist mit einer Wahrscheinlichkeit p attribuiert. Fällt die Komponente aus, an der die Kante beginnt, kommt es mit Wahrscheinlichkeit p zu einer Fortpflanzung des Fehlers zur Komponente, bei der die Kante endet. Es wird zwischen folgenden Arten von Fehlerabhängigkeiten unterschieden:

- zerstörende, unabhängige Fehlerfortpflanzung
- zerstörende, abhängige Fehlerfortpflanzung
- blockierende, unabhängige Fehlerfortpflanzung
- blockierende, abhängige Fehlerfortpflanzung

Zerstörende Fehlerfortpflanzungen machen eine Reparatur der von der Fortpflanzung betroffenen Komponente notwendig. Dem gegenüber wird eine von blockierender Fortpflanzung betroffene Komponente wieder unmittelbar verfügbar, sobald die die Fortpflanzung verursachende Komponente repariert wurde.

Eine Unterscheidung zwischen unabhängiger und abhängiger Fehlerfortpflanzung ist nur notwendig, wenn der Ausfall einer Komponente sich auf mehrere Komponenten auswirken kann. Im Falle der unabhängigen Fortpflanzung wird für jede Komponente gesondert bestimmt, ob eine Fortpflanzung stattfindet. Die Wahrscheinlichkeit, dass es zu einer Fortpflanzung kommt, ist also unabhängig davon, ob es zu anderen Fortpflanzungen kommt. Bei abhängigen Fehlerfortpflanzungen gilt hingegen, dass entweder alle Komponenten von der Fortpflanzung betroffen sind, oder keine.

Auch die Reparaturzeiten sind im Allgemeinen nicht stochastisch unabhängig voneinander, da die Anzahl der Reparaturpersonen üblicherweise viel kleiner ist als die Zahl der im System vorhandenen Komponenten. Sind mehrere Komponenten gleichzeitig ausgefallen, kann es daher zu einer Verzögerung der Reparatur kommen. Dieser Tatsache kann in OpenSESAME durch die Einführung von sogenannten Reparaturgruppen (repair group, RG) Rechnung getragen werden. Jede Reparaturgruppe besitzt eine Kapazität, die der Anzahl an Reparaturpersonen entspricht. In der Komponententabelle wird eingetragen, von welcher Reparaturgruppe die entsprechende Komponente repariert wird.

4 Zusammenfassung

Diese Arbeit beschreibt die Sicht des Nutzers auf das Werkzeug OpenSESAME. Es erlaubt die Modellierung fehlertoleranter, hochverfügbarer Systemen auf leicht erlernbare und nachvollziehbare Art und Weise. Ein OpenSESAME-Modell besteht aus Komponenten, Blockdiagrammen, Fehlerabhängigkeitsdiagrammen, Reparaturgruppen und Variablen. Das gesamte Modell wird zur Auswertung in ein semantisch äquivalentes Zustandsraum-basiertes Modell umgewandelt.

5 Literatur

- [Schn99] Schneeweiss, W. G.: The Fault Tree Method, LiLoLe-Verlag, Hagen, 1999
- [Lind98] Lindemann, C.: Performance Modelling with Deterministic and Stochastic Petri Nets. Wiley and Sons, 1998
- [WaSc05] Walter, M. und Schneeweiss, W. G.: The Modelling World of Reliability/Safety-Engineering. LiLoLe-Verlag, Hagen, 2005
- [WaTr04] Walter, M. und Trinitis, C.: How to Integrate Inter-Component Dependencies into Combinatorial Availability Models, in: Proc. of the 50th Annual Reliability and Maintainability Symposium (RAMS), IEEE, 2004, S.226-231
- [GeKeZi95] German, R., Kelling, C., Zimmermann, A., Hommel, G.: TimeNet: A toolkit for evaluating non-Markovian stochastic Petri nets, in: Performance Evaluation, Bd. 24, S. 69ff, 1995
- [AjBaCo95] Ajmone Marsan, M., Balbo, G., Conte, G., Donatelli, S., Franceschinis, G.: Modelling with Generalized Stochastic Petri Nets. Wiley and Sons, 1995