Nachweis hoher Softwarezuverlässigkeit auf der Basis von Test- und Betriebserfahrung mit wiederverwendbaren Komponenten

Sven Söhnlein, Francesca Saglietti

Lehrstuhl für Software Engineering
Universität Erlangen-Nürnberg
Martensstrasse 3
91058 Erlangen, Deutschland
soehnlein@informatik.uni-erlangen.de
saglietti@informatik.uni-erlangen.de

Abstract: Dieser Artikel schildert einen neuen Ansatz zur Bewertung komponentenbasierter Softwaresysteme mit hohen Zuverlässigkeitsanforderungen, wie sie typischerweise zur Steuerung sicherheitskritischer Prozesse eingesetzt werden. Basierend auf der Test- bzw. der Betriebserfahrung, die mit wiederverwendbaren Komponenten gewonnen wurde, wird eine genaue Aussage über die Zuverlässigkeit des aus diesen Komponenten bestehenden Gesamtsystems mit entsprechender Aussagesicherheit hergeleitet. Die Vorteile, die sich gegenüber bereits bekannten Verfahren ergeben, betreffen die Nachweisbarkeit höherer Zuverlässigkeitskenngrößen bei vergleichbarem Aufwand bzw. die Reduktion der zum Nachweis erforderlichen Kosten. Dies wird anhand von Beispielen demonstriert.

1 Einleitung

Angesichts der schwerwiegenden Folgen von Versagen ist für den Einsatz komplexer Softwaresysteme in sicherheitskritischen Anwendungsbereichen ein rigoroser Nachweis hoher Zuverlässigkeit angebracht und meist auch vorgeschrieben. Oft werden für komplexe Anwendungen vorgefertigte Softwarekomponenten aus zweierlei Gründen wiederverwendet: zum einen bieten sich dadurch offensichtliche ökonomische Vorteile und zum anderen deutet die fehlerfreie Funktionsweise, die während einer vorangegangenen Test- oder Betriebsphase beobachtet wurde, auf ein zuverlässiges Produkt hin.

Selbstverständlich setzt der kompositionale Ansatz voraus, dass die Integration der hochqualifizierten, betriebsbewährten Komponenten problemadäquat erfolgt und mittels ausgiebiger Schnittstellenüberprüfungen verifiziert wurde, um schwerwiegende Inkonsistenzen zwischen den Komponenten (z.B. Ariane 5, s. [Li96]) frühzeitig zu erkennen. Darüber hinaus sind allerdings fundierte Methoden notwendig, die die

Zuverlässigkeitsbewertung komponentenbasierter Systeme auf der Grundlage der bisherigen Einsätze wiederverwendeter Komponenten erlauben.

Einen Ansatz für die quantitative Zuverlässigkeitsbewertung bietet die Anwendung der statistischen Stichprobentheorie (s. [Qu85, PSK90, Eh02]). Trotz der Kritik (s. [BF93, LS93, LS00]), die sich vorwiegend auf den damit verbundenen Aufwand bezieht, erlaubt diese Technik fundierte Zuverlässigkeitsaussagen zu gegebenen Aussagesicherheiten zu bestimmen. Während der Einsatz dieser Vorgehensweise für ein neues System tatsächlich zu einem extrem hohen Testaufwand führt, kann die Auswertung bereits gewonnener Betriebserfahrung zu einer deutlichen Ersparnis beitragen. Speziell in der Automobilindustrie gewinnt dieser wirtschaftlich attraktive Ansatz zunehmend an Bedeutung.

Um aus der mit einzelnen Komponenten gewonnen Betriebserfahrung auf die Systemzuverlässigkeit schließen zu können, ist eine statistisch fundierte Kombination komponentenspezifischer Zuverlässigkeitsaussagen notwendig.

In diesem Artikel wird eine Methode zur genauen Bestimmung der Zuverlässigkeit eines Systems hergeleitet, welches aus Komponenten besteht, die alternativ benutzt werden. In Abhängigkeit von der zugrunde liegenden Granularität können diese Komponenten für ganze Softwarepakete, Programmteile oder gar individuelle Kontrollflusspfade stehen.

Der Artikel ist wie folgt gegliedert: In Kapitel 2 werden die wesentlichen Grundlagen der statistischen Stichprobentheorie für softwarebasierte Systeme dargestellt. Kapitel 3 bietet die Herleitung einer genauen Berechnungsmethode zur Bestimmung der Systemzuverlässigkeit für komponentenbasierte Systeme. In Kapitel 4 wird der entwickelte Ansatz anhand von Beispielen illustriert.

2 Softwarezuverlässigkeitsbewertung durch statistisches Testen

In diesem Kapitel werden die wichtigsten Grundlagen des statistischen Testens kurz vorgestellt. Für eine ausführlichere Beschreibung sei z. B. auf [Eh02] verwiesen. Anhand der statistischen Stichprobentheorie wird nach Beobachtung von n korrekt ausgeführten Test- bzw. Betriebsfällen zu einer vorgegebenen Aussagesicherheit β eine obere Schranke $\tilde{p}$ der Versagenswahrscheinlichkeit p eines Systems bestimmt, d.h.

$$P(p \leq \tilde{p}) = \beta \tag{1}$$

Um diese Theorie anzuwenden, müssen allerdings die folgenden Vorraussetzungen erfüllt sein:

1. **Unabhängige Auswahl der Testfälle:** die Auswahl eines Testfalls darf keinen Einfluss auf die Auswahl weiterer Testfälle haben.

2. **Unabhängige Ausführung der Testfälle:** die Ausführung eines Testfalls darf keinen Einfluss auf das Ergebnis weiterer Testfälle haben.

3. **Betriebstreue:** im Laufe des beobachteten Tests bzw. Betriebs kommen Eingangsdaten mit der gleichen Wahrscheinlichkeit zum Zuge, mit der sie im künftigen Betrieb erwartet werden.

4. **Versagensfreie Test- bzw. Betriebserfahrung:** bei keinem der beobachteten Test- bzw. Betriebsfälle werden Versagen beobachtet. Mit dieser Forderung wird die allgemeine Theorie über statistische Konfidenzintervalle (vgl. u.a. [St70]) verschärft, um im Falle sicherheitskritischer Anwendungen besonders hohe Zuverlässigkeitsaussagen zu ermöglichen.

Falls das Betriebsprofil vorgefertigter Komponenten aus einer früheren Betriebsphase von dem zu erwartenden Profil des künftigen Einsatzes in einem neuen System abweicht, ist eine entsprechende Anpassung bzw. Umrechnung zur Sicherstellung von Annahme 3 notwendig (s. [Sa00]).

Eine weitere notwendige Annahme zur Anwendung der Theorie setzt eine konstante Versagenswahrscheinlichkeit p über dem gesamten Eingaberaum voraus. Nach der Theorie von Eckardt und Lee (s. [EL85]) ist diese Annahme für große Systeme mit entsprechend hoher Funktionsvielfalt im Allgemeinen unrealistisch, da in solchen Systemen die Problemkomplexität über dem gesamten Eingaberaum stark variieren kann. Die Annahme wird allerdings bei Betrachtung feingranularer Komponenten beschränkter Funktionalität realistischer, da man hier von einer geringeren Varianz der Eingabekomplexität ausgehen kann.

Falls ein bestimmter Umfang an Test- bzw. Betriebsfällen n gesammelt wurde und die oben genannten Vorraussetzungen als erfüllt betrachtet werden können, lässt sich anhand der statistischen Stichprobentheorie folgender Zusammenhang zwischen n, $\tilde{p}$ und β definieren (s. [Eh02] für eine Herleitung):

$$(1-\tilde{p})^n = 1-\beta \tag{2}$$

Umgekehrt lässt sich somit die erforderliche Anzahl an erfolgreich bearbeiteten Testfällen bestimmen, um Aussage (1) für $\tilde{p} << 1$ nachzuweisen:

$$n \cong \frac{\ln(1-\beta)}{-\tilde{p}} \tag{3}$$

Für die Aussagesicherheit β gilt damit

$$\beta = 1-\exp(-n\cdot\tilde{p}) \tag{4}$$

Unter Berücksichtigung von Gleichung (1) und (4) kann p als exponentialverteilte Zufallsvariable mit Verteilungsfunktion β interpretiert werden:

$$P(p \le \tilde{p}) = F_p(\tilde{p}) = \beta = 1 - \exp(-n \cdot \tilde{p}) \tag{5}$$

3 Zuverlässigkeitsbewertung komponentenbasierter Systeme

Im Folgenden werden Softwaresysteme betrachtet, die aus k funktional unabhängigen Komponenten bestehen, die eingabespezifisch alternativ zum Zuge kommen (siehe Abbildung 1).

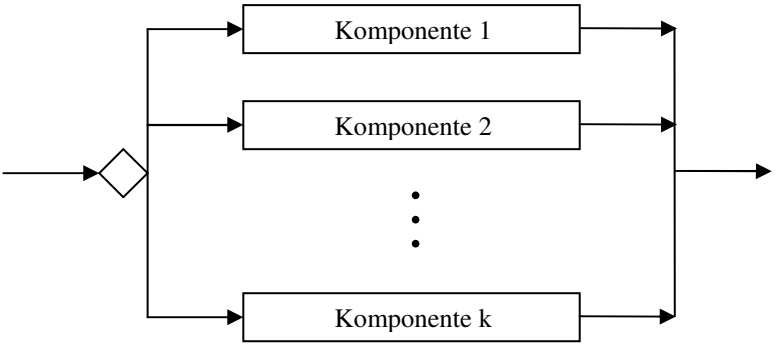

Abbildung 1: Betrachtete Systemstruktur

Für jede Komponente $i \ (i = 1,...,k)$ sei ein bestimmter Umfang n_i an Test- bzw. Betriebserfahrung gesammelt worden. Unter der Annahme, dass alle Voraussetzungen aus Kapitel 2 erfüllt sind, kann für jede Komponente eine obere Schranke $\tilde{p}_i$ für ihre Versagenswahrscheinlichkeit $p_i \ (0 < p_i < 1)$ mit zugehöriger Aussagesicherheit β_i bestimmt werden:

$$P(p_i \le \tilde{p}_i) = \beta_i \tag{6}$$

Falls Komponente $i \ (i = 1,...,k)$ im Betrieb mit Wahrscheinlichkeit γ_i ausgewählt wird ($\sum_{i=1}^{k} \gamma_i = 1$), ergibt sich die Versagenswahrscheinlichkeit p des Gesamtsystems durch

$$p = \sum_{i=1}^{k} \gamma_i p_i \tag{7}$$

3.1 Unscharfe Aussage zur Systemzuverlässigkeit

Ein konservativer Ansatz zur Bestimmung einer oberen Schranke $\tilde{p}$ für die Versagenswahrscheinlichkeit p des Gesamtsystems wurde in [Sa00] beschrieben. Hierzu wurden die oberen Schranken $\tilde{p}_i$ der individuellen Versagenswahrscheinlichkeiten der einzelnen Komponenten addiert und mit den entsprechenden Auswahlwahrscheinlichkeiten γ_i gewichtet:

$$p = \sum_{i=1}^{k} \gamma_i p_i \leq \sum_{i=1}^{k} \gamma_i \tilde{p}_i = \tilde{p} \tag{8}$$

Dabei ist die zugehörige Aussagesicherheit β größer als das Minimum aller individuellen Aussagesicherheiten β_i aus Gleichung (6):

$$\min_i \beta_i < \beta \quad \text{für} \quad i \geq 2 \tag{9}$$

Zur Verschärfung dieser Aussage wird im folgenden Abschnitt ein Ansatz hergeleitet, der es ermöglicht, den Zusammenhang zwischen der Aussagesicherheit β und der oberen Schranke $\tilde{p}$ des Gesamtsystems genau zu bestimmen.

3.2 Scharfe Aussage zur Systemzuverlässigkeit

Um den genauen Zusammenhang zwischen der oberen Schranke $\tilde{p}$ der Versagenswahrscheinlichkeit p auf Systemebene und der zugehörigen Aussagesicherheit β herzuleiten, sei zunächst festgehalten, dass für eine exponentialverteilte Zufallsvariable p (mit Rate n) und eine Konstante γ (mit $0 \leq \gamma \leq 1$) folgendes gilt:

$$P(\gamma \cdot p \leq \tilde{p}) = P\left(p \leq \frac{\tilde{p}}{\gamma}\right) = F_p\left(\frac{\tilde{p}}{\gamma}\right) = 1 - \exp(-\frac{n}{\gamma} \cdot \tilde{p}) \tag{10}$$

Insbesondere ist die Zufallsvariable $\gamma \cdot p$ ebenfalls exponentialverteilt mit Rate $\frac{n}{\gamma}$.

Durch Gleichungen (7) und (10) kann somit die Versagenswahrscheinlichkeit p des Gesamtsystems als Summe exponentialverteilter Zufallsvariablen $\gamma_i p_i$ mit Raten $\frac{n_i}{\gamma_i}$ interpretiert werden.

Angesichts der funktionalen Diversität der Komponenten und ihrer paarweise disjunkten Eingaberäume ist von einer Abhängigkeit zwischen ihren Versagenswahrscheinlichkeiten $p_i\ (1 \le i \le k)$ nicht auszugehen, so dass diese im Weiteren als statistisch unabhängig angenommen werden. Selbst im Falle gemeinsam benutzter Bibliotheken ist diese Annahme im Allgemeinen plausibel, da die Wahrscheinlichkeit, dass sich diese auf unterschiedliche Funktionalitäten mit disjunkten Datenräumen gleichsam auswirken, als vernachlässigbar klein betrachtet werden kann.

In diesem Falle ergibt sich für paarweise verschiedene Quotienten $\frac{n_i}{\gamma_i}$, also falls

$$\frac{n_i}{\gamma_i} \neq \frac{n_j}{\gamma_j} \quad \forall i \neq j \tag{11}$$

eine Hypo-Exponentialverteilung für die Summe $\gamma_i p_i$ der paarweise unabhängigen, exponentialverteilten Zufallsvariablen p_i (s. [Co62, Tr82]):

$$\beta = P\left(\sum_{i=1}^{k} \gamma_i p_i \le \tilde{p}\right) = 1 - \sum_{i=1}^{k} A_i \cdot \exp\left(-\frac{n_i}{\gamma_i} \cdot \tilde{p}\right) \quad \text{mit} \quad A_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{\frac{n_j}{\gamma_j}}{\frac{n_j}{\gamma_j} - \frac{n_i}{\gamma_i}} \tag{12}$$

Der Fall mit paarweise identischen Quotienten $\frac{n_i}{\gamma_i}$ ist grundsätzlich ähnlich behandelbar (s. [AM97]), wird jedoch im Folgenden aus Gründen der damit verbundenen Komplexität nicht weiter betrachtet.

4 Beispiele

In diesem Kapitel wird anhand konkreter Beispiele der Vorteil des oben vorgestellten Ansatzes gegenüber dem in Abschnitt 3.1 dargestellten, bisherigen Vorgehen unter drei unterschiedlichen Gesichtspunkten demonstriert.

Zu diesem Zweck wird im Folgenden die kleinste Aussagesicherheit $\beta_i\ (1 \le i \le k)$ betrachtet und mit β_{kons} bezeichnet:

$$\beta_{kons} := \min_i \beta_i \tag{13}$$

Auf Grund von Ungleichung (9) ergibt diese Größe nur einen unscharfen Schätzwert für die tatsächlich erzielbare Aussagesicherheit.

4.1 Vergleich der nachweisbaren Zuverlässigkeitskenngrößen

Im Folgenden bestehe das betrachtete System aus zwei Komponenten (s. Abbildung 2).

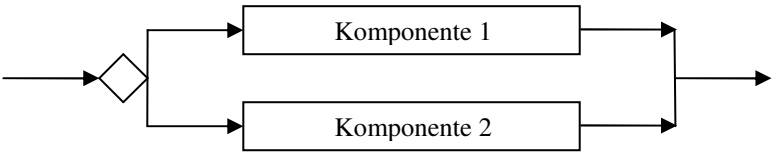

Abbildung 2: Aus zwei alternativen Komponenten bestehendes System

Gemäß Abschnitt 3 wird angenommen, dass die Komponenten funktional unabhängig sind und alternativ genutzt werden. Für Komponente 1 wurden n_1=20000 korrekte, unabhängig ausgewählte und ausgeführte Test- bzw. Betriebsfälle beobachtet, für Komponente 2 entsprechend n_2=50000 Fälle. Tabellen 1 und 2 zeigen die dadurch nachweisbare obere Schranke $\tilde{p}$ für die Versagenswahrscheinlichkeit p des Gesamtsystems zur Aussagesicherheit β=0.99 (bzw. β=0.999) im Falle unterschiedlicher Operationsprofile γ_i (i=1,2). Die relative Abweichung

$$\varepsilon = \left| \frac{\tilde{p}_{kons} - \tilde{p}}{\tilde{p}} \right| \cdot 100\% \qquad (14)$$

zwischen den oberen Schranken $\tilde{p}_{kons}$ und $\tilde{p}$, die jeweils entsprechend Abschnitt 3.1 bzw. Abschnitt 3.2 ermittelt wurden lässt sich ebenfalls aus den Tabellen entnehmen.

β=0.99	$\tilde{p}$	$\tilde{p}_{kons}$	ε
γ_1=0.5, γ_2=0.5	0.0001278	0.0001611	26.03 %
γ_1=0.25, γ_2=0.75	0.0000917	0.0001266	38.05 %
γ_1=0.75, γ_2=0.25	0.0001780	0.0001957	9.92 %

Tabelle 1: Zuverlässigkeitskenngrößen für β=0.99 und verschiedene Betriebsprofile

β=0.999	$\tilde{p}$	$\tilde{p}_{kons}$	ε
γ_1=0.5, γ_2=0.5	0.0001854	0.0002417	30.36 %
γ_1=0.25, γ_2=0.75	0.0001280	0.0001899	48.37 %
γ_1=0.75, γ_2=0.25	0.0002644	0.0002935	11.03 %

Tabelle 2: Zuverlässigkeitskenngrößen für β=0.999 und verschiedene Betriebsprofile

Anhand der Werte wird deutlich, dass der neue Ansatz höhere Zuverlässigkeitskenngrößen zu gleicher Aussagesicherheit nachzuweisen erlaubt. Dies wird auch durch die folgende Graphik (s. Abbildung 3) veranschaulicht:

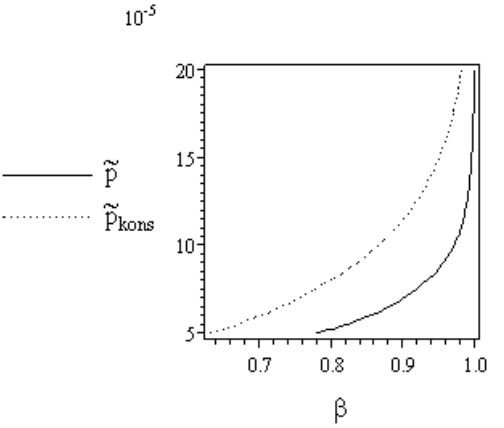

Abbildung 3: Aussagesicherheit β vs. obere Schranke $\tilde{p}$ und $\tilde{p}_{kons}$ für γ_1=0.5, γ_2=0.5

4.2 Vergleich der Aussagesicherheiten

In diesem Abschnitt werden für das gleiche Beispiel zu gegebenen oberen Schranken $\tilde{p}$ =0.0001 bzw. $\tilde{p}$ =0.00005 die Aussagesicherheiten β_{kons} und β verglichen. Die Tabellen 3 und 4 enthalten die entsprechenden Werte, sowie ihre relative Abweichung

$$\delta = \left| \frac{\beta_{kons} - \beta}{\beta} \right| \cdot 100\% \qquad (15)$$

$\tilde{p}$ =0.0001	β	β_{kons}	δ
γ_1=0.5, γ_2=0.5	0.969	0.864	10.82 %
γ_1=0.25, γ_2=0.75	0.994	0.864	13.02 %
γ_1=0.75, γ_2=0.25	0.919	0.864	5.99 %

Tabelle 3: Aussagesicherheiten für $\tilde{p}$ =0.0001 und verschiedene Betriebsprofile

$\tilde{p}$ =0.00005	β	β_{kons}	δ
γ_1=0.5, γ_2=0.5	0.778	0.632	18.85 %
γ_1=0.25, γ_2=0.75	0.877	0.632	27.97 %
γ_1=0.75, γ_2=0.25	0.695	0.632	9.16 %

Tabelle 4: Aussagesicherheiten für $\tilde{p}$ =0.00005 und verschiedene Betriebsprofile

Hier ist erkennbar, dass der neue Ansatz deutlich höhere Aussagesicherheiten erlaubt, was auch in Abbildung 4 veranschaulicht wird.

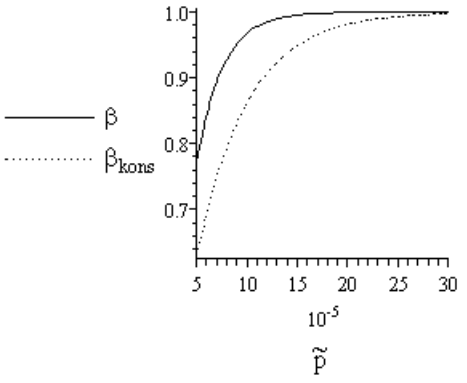

Abbildung 4: Obere Schranke $\tilde{p}$ vs. Aussagesicherheit β und β_{kons} für γ_1=0.5, γ_2=0.5

4.3 Vergleich des erforderlichen Umfangs an Test- bzw. Betriebsfällen

In diesem Abschnitt wird der notwendige Umfang an Test- bzw. Betriebserfahrung verglichen, der notwendig ist, um mit Aussagesicherheit $\beta = 0.99$ nachzuweisen, dass die Versagenswahrscheinlichkeit des Systems durch $\tilde{p} = 0.0001$ nach oben beschränkt ist. Tabellen 5, 6 und 7 enthalten die hierfür erforderliche Anzahl an unabhängigen Test- bzw. Betriebsfällen für Systeme mit 2, 3 bzw. 5 gleichmäßig beanspruchten Komponenten $\gamma_i = 1/k$ ($\forall i=1,\ldots, k$).

n_i (genau)	insgesamt (genau)	n_i (konservativ)	insgesamt (konservativ)	Ersparnis
n_1=33194 n_2=33195	66389	n_1=46052 n_2=46052	92104	27.92 %

Tabelle 5: Erforderliche Test- bzw. Betriebserfahrung bei 2 Komponenten

n_i (genau)	insgesamt (genau)	n_i (konservativ)	insgesamt (konservativ)	Ersparnis
n_1=28023 n_2=28024 n_3=28025	84072	n_1=46052 n_2=46052 n_3=46052	138156	39.15 %

Tabelle 6: Erforderliche Test- bzw. Betriebserfahrung bei 3 Komponenten

n_i (genau)	insgesamt (genau)	n_i (konservativ)	insgesamt (konservativ)	Ersparnis
n_1=23213 n_2=23214 n_3=23215 n_4=23216 n_5=23217	116075	n_1=46052 n_2=46052 n_3=46052 n_4=46052 n_5=46052	230260	49.59 %

Tabelle 7: Erforderliche Test- bzw. Betriebserfahrung bei 5 Komponenten

Die Tabellen zeigen, dass durch den neu entwickelten Ansatz eine erhebliche Ersparnis der notwendigen Test- bzw. Betriebserfahrung möglich wird, was die praktische Anwendbarkeit der hergeleiteten Theorie unterstützt.

Die folgende Graphik zeigt die Gewinnzunahme bei wachsender Komponentenanzahl.

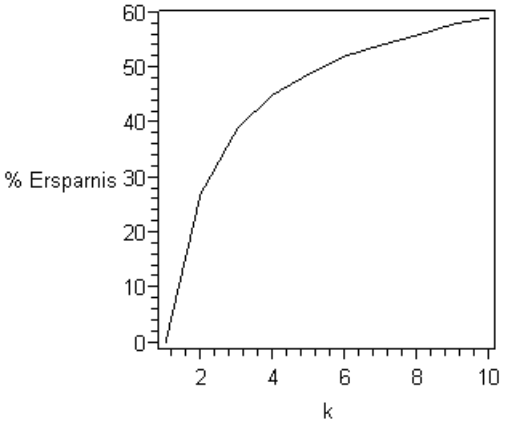

Abbildung 5: Durch neuen Ansatz erzielbare Ersparnis

5 Zusammenfassung

In diesem Artikel wurde ein neuer Ansatz zur Beschränkung der Versagenswahrscheinlichkeit eines komponentenbasierten Systems mit genauer Angabe der zugehörigen Aussagesicherheit beschrieben. Die Vorteile, die sich im Vergleich zum bestehenden Verfahren ergeben, wurden anhand der vorgestellten Beispiele verdeutlicht. Zum einen ermöglicht das Verfahren, zu vorgegebener Aussagesicherheit eine höhere Zuverlässigkeit für das Gesamtsystem nachzuweisen, zum anderen erlaubt es, vorgegebene Zuverlässigkeitsaussagen mit erhöhter Aussagesicherheit zu treffen. Vor allem aber verspricht das vorgestellte Vorgehen eine deutliche Reduktion des bisher zum Nachweis erforderlichen Testaufwands, was gerade im Bereich sicherheitskritischer Anwendungen von größter Bedeutung ist.

Literaturverzeichnis

[AM97] Amari, S.; Misra, R.: Closed-form expressions for distribution of sum of exponential random variables, IEEE Transactions on reliability, 46(4), 1997, S. 519–522.

[BF93] Butler, R; Finelli, G.: The infeasibility of quantifying the reliability of life-critical real-time software, Software Engineering, 19(1), 1993, S. 3–12.

[Co62] Cox, D.: Renewal Theory, Methuen & Co, 1962.

[EL85] Eckhardt, D.E.; Lee, L.D.: A Theoretical Basis for the Analysis of Multiversion Software Subject to Coincident Errors, IEEE Trans. on Software Engineering, Vol. SE-11, No. 12, December 1985, S. 1511-1516.

[Eh02] Ehrenberger, W.: Software-Verifikation, Hanser Verlag, München, Germany, 2002.

[HG72] Heinhold, J.; Gaede K.: Ingenieur-Statistik, Oldenbourg, Germany, 1972.

[Li96] Lions, JL. ARIANE 5 Flight 501 Failure: Report by the Enquiry Board, European Space Agency, Paris, 1996.

[LS93] Littlewood, B.; Strigini L.: Validation of ultra-high dependability for softwarebased systems, Communications of the ACM, 36(11), 1993, S. 69–80.

[LS00] Littlewood, B.; Strigini L.: Software reliability and dependability: A roadmap, The Future of Software Engineering, ACM Press, 2000, S. 177–188.

[PSK90] Parnas, D.; van Schouwen, J.; Kwan, S.: Evaluation of safetycritical software, Communications of the ACM, 33(6), 1990, S. 636–648.

[Qu85] Quirk, W. J.: Verification and validation of real-time software, Springer-Verlag New York, Inc., NY, USA, 1985.

[Sa00] Saglietti F.: Evaluation of pre-developed software for usage in safety critical systems, 26th Euromicro Conference, Software Process and Product Improvement (EUROMICRO 2000), Institute of Electrical and Electronics Engineers (IEEE), 2000.

[St70] Störmer, H.: Mathematische Theorie der Zuverlässigkeit, Oldenburg, 1970.

[Tr82] Trivedi, K.: Probability & Statistics with Reliability, Queuing, and Computer Science Applications, Prentice-Hall, 1982.