

# Automotive 2008

## **Auswertung der Betriebserfahrung zum Zuverlässigkeitsnachweis sicherheitskritischer Softwaresysteme**

**S. Söhnlein, F. Saglietti**

Universität Erlangen-Nürnberg

Lehrstuhl für Software Engineering (Informatik 11)



# Gliederung

- ◆ Motivation
- ◆ Grundlagen des statistischen Testens
- ◆ Zuverlässigkeitsbewertung komponentenbasierter Systeme
- ◆ Leitlinie zur Analyse und Auswertung statistisch relevanter operationaler Daten
- ◆ Beispiele
- ◆ Fazit

# Motivation

## Einsatz von Softwaresystemen in sicherheitskritischen Anwendungsbereichen

- ◆ Rigoroser Nachweis hoher Zuverlässigkeit angebracht und oft auch vorgeschrieben
  - z.B. durch Einhaltung generischer Sicherheitsstandards (IEC 61508), bzw.
  - domänenspezifischer Vorgaben (ISO 26262 *Draft* für die Automobilindustrie)
- ◆ Wiederverwendung von Software-Komponenten:
  - Ökonomische Vorteile
  - Bisherige fehlerfreie Funktionsweise während einer Test- oder Betriebsphase deutet auf ein zuverlässiges Produkt hin

**Notwendigkeit fundierter Methoden zur quantitativen Zuverlässigkeitsbewertung komponentenbasierter Systeme**

## Statistische Stichprobentheorie

- ◆ Ansatz für die quantitative Zuverlässigkeitsbewertung von Softwaresystemen
- ◆ Anwendung der Technik erlaubt Zuverlässigkeitsaussagen zu gegebenen Aussagesicherheiten zu machen

**Kritik: Hoher Aufwand** (bezieht sich vor allem auf neue Systeme für die noch keine Betriebserfahrung vorliegt)

→ Auswertung bereits gewonnener Betriebserfahrung mit Komponenten kann zu einer deutlichen Ersparnis führen

# Motivation

- ◆ Bestimmung der Systemzuverlässigkeit auf Grund der mit einzelnen Komponenten gewonnenen Betriebserfahrung:
  - Statistisch fundierte Kombination komponentenspezifischer Zuverlässigkeitsaussagen notwendig
    - bisher nur konservative Abschätzungen für spezielle Architekturen möglich
  - Analyse und Extraktion statistisch relevanter Informationen aus operationalen Daten
    - Systematische Konzepte notwendig

# Motivation

## ◆ In dieser Arbeit:

- Vorstellung einer Methode zur genauen Berechnung der Zuverlässigkeit eines aus alternativ benutzten Komponenten bestehenden Systems
  - Verbesserung bisheriger Ansätze im Bezug auf die Bestimmung der Zuverlässigkeit, Aussagesicherheit und den erforderlichen Aufwand
- Beschreibung einer Leitlinie zur Extraktion statistisch relevanter Betriebserfahrung
  - Konzept wird im Rahmen eines Forschungsprojektes in Kooperation mit ZF Friedrichshafen erprobt

# Grundlagen des statistischen Testens

## Zuverlässigkeitsbewertung mittels statistischer Stichprobentheorie:

- ◆ Beobachtung von  $n$  korrekt ausgeführten Test- bzw. Betriebsfällen
- ◆ Bestimmung einer oberen Schranke  $p^*$  für die Versagenswahrscheinlichkeit  $p$  zu gegebener Aussagesicherheit  $\beta$ :

$$P(p \leq p^*) = \beta$$

# Grundlagen des statistischen Testens

**Grundannahme:** Invariante Versagenswahrscheinlichkeit  $p$  über dem gesamten Eingaberaum.

## Voraussetzungen für die Stichprobe

- ◆ Unabhängige Auswahl der Testfälle
- ◆ Unabhängige Ausführung der Testfälle
- ◆ Betriebstreue
- ◆ Versagensfreie Test- bzw. Betriebserfahrung  
*(Prinzipiell auch anwendbar für eine geringe Anzahl an Versagen auf Kosten der nachweisbaren Zuverlässigkeitskenngrößen)*

# Grundlagen des statistischen Testens

- ◆ Falls alle Voraussetzungen erfüllt sind lässt sich folgender Zusammenhang zwischen  $n$ ,  $p^*$  und  $\beta$  definieren:

$$(1 - p^*)^n = 1 - \beta$$

- ◆ Damit lässt sich auch die Anzahl notwendiger Test- bzw. Betriebsfälle für  $p^* \ll 1$  bestimmen:

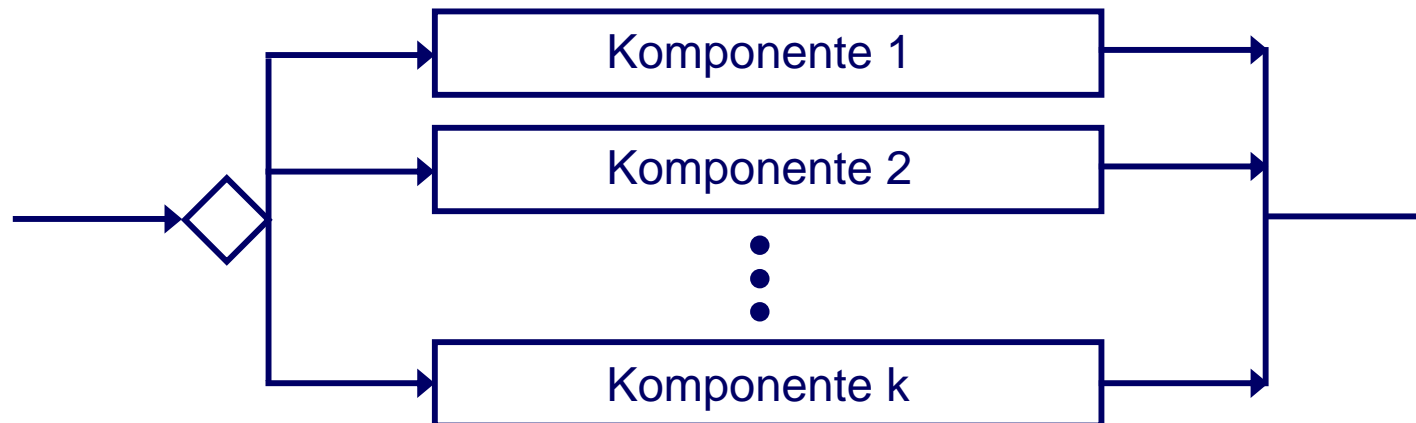
$$n \cong \frac{\ln(1 - \beta)}{-p^*}$$

- ◆ Beispiele:

SIL (IEC 61508)	$p^*$	$\beta$	$n$
2	$10^{-3}$	0.99	4606
3	$10^{-4}$	0.99	46052
4	$10^{-5}$	0.99	460518

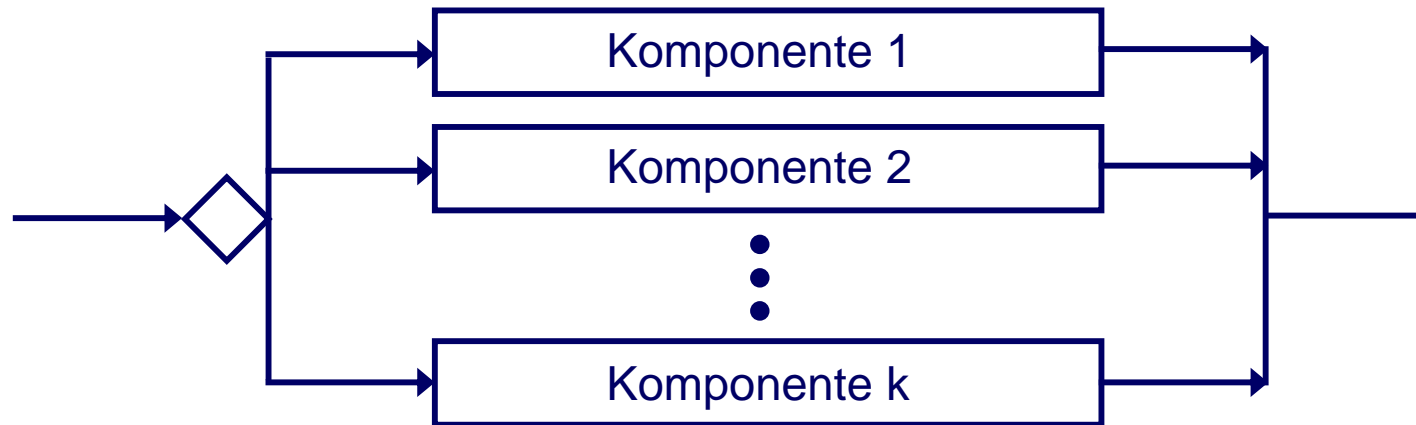
# Komponentenbasierte Systeme

Betrachtet werden Softwaresysteme, bestehend aus  $k$  funktional unabhängigen Komponenten, die alternativ zum Zuge kommen



- ◆ Für jede Komponente  $i$  ( $i=1, \dots, k$ ) ist ein Umfang an  $n_i$  Test- bzw. Betriebsfällen beobachtet worden.
- ◆ Alle Voraussetzungen für die Anwendung der statistischen Stichprobentheorie sind erfüllt

# Komponentenbasierte Systeme



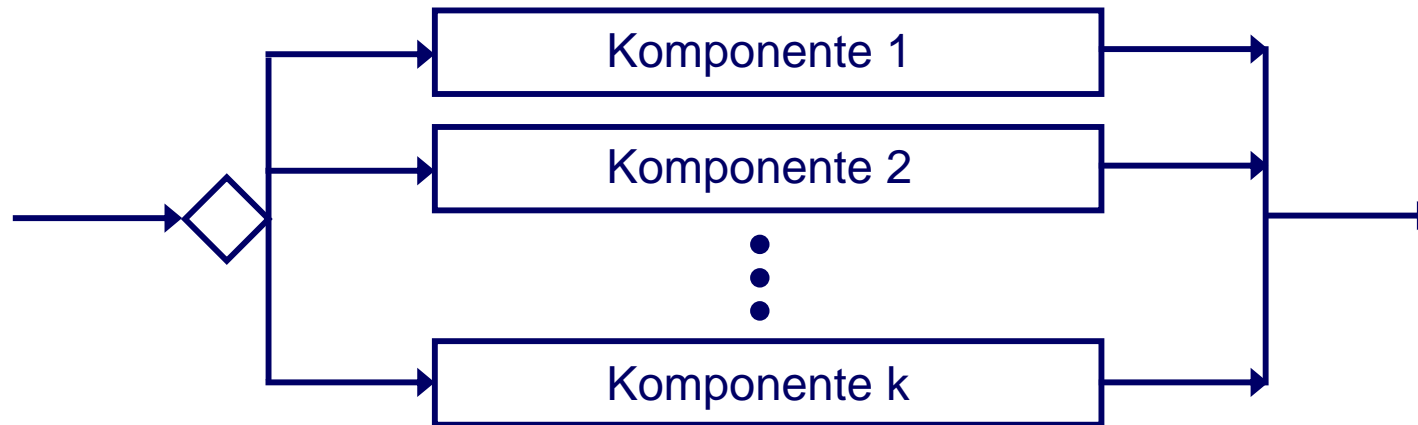
- ◆ Für jede Komponente kann eine obere Schranke  $p_i^*$  für ihre Versagenswahrscheinlichkeit  $p_i$  ( $0 < p_i < 1$ ) mit Aussagesicherheit  $\beta_i$  bestimmt werden:

$$P(p_i \leq p_i^*) = \beta_i$$

- ◆ Falls jede Komponente im Betrieb mit Wahrscheinlichkeit  $\gamma_i$  zum Zuge kommt ( $\sum \gamma_i = 1$ ), ergibt sich die Versagenswahrscheinlichkeit des Gesamtsystems durch:

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

# Komponentenbasierte Systeme



**Gesucht:**

Zusammenhang zwischen  $p^*$  und  $\beta$  auf Systemebene

# Konservativer Ansatz

Bisheriger konservativer Ansatz zur Bestimmung der oberen Schranke  $p^*$  für das Gesamtsystem:

$$p = \sum_{i=1}^k \gamma_i p_i \leq \sum_{i=1}^k \gamma_i p_i^* = p_{\text{kons}}^*$$

Die zugehörige Aussagesicherheit  $\beta$  wird hierbei durch  $\beta_{\text{kons}}$  folgendermaßen abgeschätzt:

$$\beta_{\text{kons}} := \min_i \beta_i < \beta \quad \text{für } i \geq 2$$

## **Nachteile dieses Ansatzes:**

- ◆ Verlust an Aussagenschärfe
- ◆ Verlust an Genauigkeit bei der Zuverlässigkeitsbewertung
- ◆ Unnötig hoher Aufwand für die erforderliche Test- bzw. Betriebserfahrung

# Genauere Berechnung

- ◆ Zur genauen Berechnung des Zusammenhangs zwischen  $p^*$  und  $\beta$  auf Systemebene kann  $\beta_i$  auch als Funktion interpretiert werden:

$$\beta_i = P(p_i \leq p_i^*) = F_{p_i}(p_i^*) = 1 - \exp(-n_i \cdot p_i^*)$$

- Für Exponentialverteilte  $p_i$  und eine Konstante  $\gamma_i$  ( $0 \leq \gamma_i \leq 1$ ) gilt:

$$P(\gamma_i \cdot p_i \leq p_i^*) = P\left(p_i \leq \frac{p_i^*}{\gamma_i}\right) = F_{p_i}\left(\frac{p_i^*}{\gamma_i}\right) = 1 - \exp\left(-\frac{n_i}{\gamma_i} \cdot p_i^*\right)$$

- ◆ Genaue Bestimmung des Zusammenhangs auf Systemebene durch Berechnung der Faltung der komponentenspezifischen Funktionen

# Genauere Berechnung

- ◆ Die Versagenswahrscheinlichkeiten  $p_i$  ( $1 \leq i \leq k$ ) der einzelnen Komponenten sind statistisch unabhängig, denn
  - die Komponenten sind funktional diversitär
  - und haben paarweise disjunkte Eingaberäume
- ◆ In diesem Falle ergibt sich für paarweise verschiedene Quotienten  $n_i/\gamma_i$ , also falls

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

eine **Hypo-Exponentialverteilung**

(Details in Söhnlein S., Saglietti F.: "Nachweis hoher Softwarezuverlässigkeit auf der Basis von Test- und Betriebserfahrung mit wiederverwendbaren Komponenten", Proc. Sicherheit 2008 Lecture Notes in Informatics, Gesellschaft für Informatik (GI) e. V., 2008)

# Genauere Berechnung

## Hypo-Exponentialverteilung

für den Zusammenhang zwischen  $p^*$  und  $\beta$  auf Systemebene:

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

- ◆ Der Fall mit paarweise identischen Quotienten ist grundsätzlich ähnlich behandelbar, wird jedoch aus Gründen der damit verbundenen Komplexität nicht weiter betrachtet.
- ◆ Vorteile durch die genaue Berechnung: siehe Beispiele

# Andere Architekturen

- ◆ Lösungen auch für andere Systemarchitekturen möglich, z.B.
  - Seriensysteme
  - Kombinationen aus parallelen und seriellen Strukturen
- ◆ Auch der Fall des Auftretens einer gewissen Anzahl an Versagens ist für oben genannte Architekturen möglich
  - Lösungen sehr komplex

# Leitlinie

- ◆ Anwendung der Theorie auf die mit Komponenten gewonnene Betriebserfahrung:
  - Analyse und Filterung der operationalen Daten im Hinblick auf die einzuhaltenden Voraussetzungen für die Anwendung der statistischen Stichprobentheorie
- ➔ Leitlinie zur Beschreibung der wesentlichen Schritte zur Extraktion, Auswertung und Ergänzung statistisch relevanter operationaler Daten
  - Gegliedert in 8 Einzelschritte

## **1. Identifikation der zu bewertenden Systemkomponente:**

- Abgrenzung der Komponente / Teilfunktionalität auf die sich die angestrebte Zuverlässigkeitsaussage beziehen soll.

## **2. Identifikation betrieblich unabhängiger Abläufe:**

- Im Hinblick auf Voraussetzung 2 müssen „gedächtnislose“ Ausführungssequenzen bestimmt werden.

## **3. Definition der Struktur eines relevanten Ablaufs:**

- Identifikation aller relevanten Eingabeparameter
- Ausgrenzung irrelevanter Eingabeparameter

## 4. Bestimmung des Betriebsprofils:

- Bestimmung der Auftrittshäufigkeit einzelner funktionaler Anforderungen an die Software im Betrieb

## 5. Filterung der operationalen Daten:

- Extraktion einer unabhängigen Teilmenge aus den operationalen Daten durch Entfernung
  - nicht relevanter Abläufe
  - bzw. statistisch abhängiger Abläufe

## 6. Validierung der gefilterten Daten:

- Sicherstellung des korrekten Verhaltens

## 7. Zuverlässigkeitsbewertung:

- Bestimmung der Zuverlässigkeitsaussage für das Gesamtsystem gemäß vorherigem Abschnitt.

## 8. Ergänzung der Betriebserfahrung:

- Falls die extrahierte Betriebserfahrung nicht ausreicht, um eine vorgegebene Zuverlässigkeitskenngröße nachzuweisen:
  - Generierung zusätzlicher Testfälle
  - Diese müssen ebenfalls den genannten Voraussetzungen entsprechen

➔ Monolithischer Fall: einfach

➔ Kompositionaler Ansatz: Optimierungsproblem

# Sensitivitätsanalyse

- ◆ Sensitivitätsanalyse auf Basis der angegebenen Gleichung für den Zusammenhang zwischen  $p^*$ ,  $\beta$  und  $n_1, \dots, n_k$  auf Systemebene.
- ◆ Auswertung der partiellen Ableitungen

$$\frac{\partial p^*}{\partial n_i} \quad i \in \{1, \dots, k\} \quad \text{bzw.} \quad \frac{\partial \beta}{\partial n_i} \quad i \in \{1, \dots, k\}$$

für die aktuell vorliegenden Testfallanzahlen

- ➔ Ermittlung derjenigen Komponenten, für die sich zusätzlicher Testaufwand am meisten lohnt.
- ◆ Minimierung des zusätzlichen Testaufwands:
  - Numerische Optimierung durch Anwendung des Gradientenverfahrens

# Beispiele

- ◆ Im Folgenden bestehe das betrachtete System aus zwei Komponenten:



- ◆ Funktional unabhängig und alternativ genutzt
- ◆ Anzahl an korrekt ausgeführten Test- bzw. Betriebsfällen:
  - Komponente 1:  $n_1=20000$
  - Komponente 2:  $n_2=50000$

# Beispiele

## Vergleich nachweisbarer Zuverlässigkeitskenngrößen

- ◆ Bestimmung der oberen Schranke mittels des konservativen Ansatzes ( $p^*_{\text{kons}}$ ) und der genauen Berechnung ( $p^*$ )

- ◆ Bestimmung der relativen Abweichung:  $\varepsilon = \left| \frac{p^*_{\text{kons}} - p^*}{p^*} \right| \cdot 100 \%$

$\beta=0.99$	$p^*_{\text{kons}}$	$p^*$	$\varepsilon$
$\gamma_1=0.75, \gamma_2=0.25$	0.0001957	0.0001780	<b>9.92 %</b>
$\gamma_1=0.5, \gamma_2=0.5$	0.0001611	0.0001278	<b>26.03 %</b>
$\gamma_1=0.25, \gamma_2=0.75$	0.0001266	0.0000917	<b>38.05 %</b>

$\beta=0.999$	$p^*_{\text{kons}}$	$p^*$	$\varepsilon$
$\gamma_1=0.75, \gamma_2=0.25$	0.0002935	0.0002644	<b>11.03 %</b>
$\gamma_1=0.5, \gamma_2=0.5$	0.0002417	0.0001854	<b>30.36 %</b>
$\gamma_1=0.25, \gamma_2=0.75$	0.0001899	0.0001280	<b>48.37 %</b>

# Beispiele

## Vergleich der Aussagesicherheiten

- ◆ Bestimmung der Aussagesicherheiten zu gegebenen oberen Schranken mittels des konservativen Ansatzes ( $\beta_{\text{kons}}$ ) und der genauen Berechnung ( $\beta$ )

- ◆ Bestimmung der relativen Abweichung: 
$$\delta = \left| \frac{\beta_{\text{kons}} - \beta}{\beta} \right| \cdot 100 \%$$

<b>p*=0.0001</b>	$\beta_{\text{kons}}$	$\beta$	$\delta$
$\gamma_1=0.75, \gamma_2=0.25$	0.864	0.919	<b>5.99 %</b>
$\gamma_1=0.5, \gamma_2=0.5$	0.864	0.969	<b>10.82 %</b>
$\gamma_1=0.25, \gamma_2=0.75$	0.864	0.994	<b>13.02 %</b>

<b>p*=0.00005</b>	$\beta_{\text{kons}}$	$\beta$	$\delta$
$\gamma_1=0.75, \gamma_2=0.25$	0.632	0.695	<b>9.16 %</b>
$\gamma_1=0.5, \gamma_2=0.5$	0.632	0.778	<b>18.85 %</b>
$\gamma_1=0.25, \gamma_2=0.75$	0.632	0.877	<b>27.97 %</b>

# Beispiele

## Vergleich des erforderlichen Umfangs an Test- bzw. Betriebsfällen

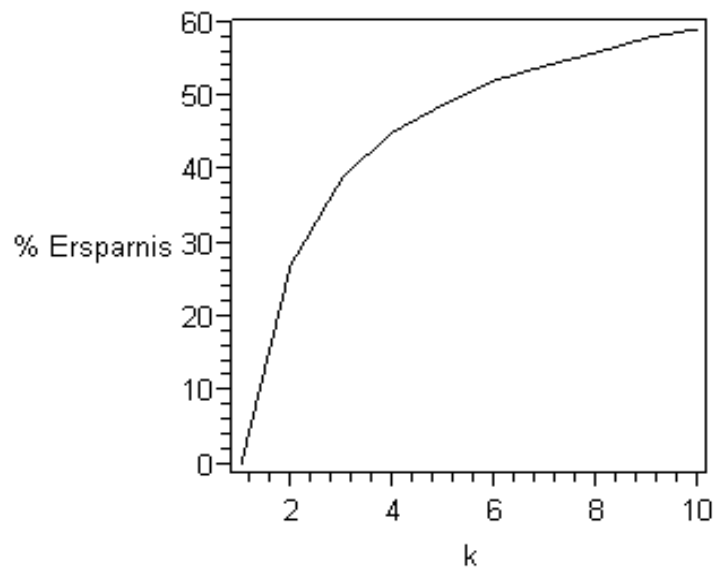
- ◆ Bestimmung der notwendigen Anzahl an Test- bzw. Betriebsfällen für ein System mit 2, 3 und 5 gleichmäßig beanspruchten Komponenten ( $\gamma_i = 1/k \forall i=1, \dots, k$ ) um  $p^*=0.0001$  mit  $\beta=0.99$  nachzuweisen.

	<b>konservativ</b>	<b>genau</b>	<b>Ersparnis</b>
$n_1$	46 052	33 194	---
$n_2$	46 052	33 195	---
$\Sigma$	<b>92 104</b>	<b>66 389</b>	<b>27.92 %</b>

	<b>konservativ</b>	<b>genau</b>	<b>Ersparnis</b>
$n_1$	46 052	28 023	---
$n_2$	46 052	28 024	---
$n_3$	46 052	28 025	---
$\Sigma$	<b>138 156</b>	<b>84 072</b>	<b>39.15 %</b>

# Beispiele

	<b>konservativ</b>	<b>genau</b>	<b>Ersparnis</b>
$n_1$	46 052	23 213	---
$n_2$	46 052	23 214	---
$n_3$	46 052	23 215	---
$n_4$	46 052	23 216	---
$n_5$	46 052	23 217	---
$\Sigma$	<b>230 260</b>	<b>116 075</b>	<b>49.59 %</b>



- ◆ Erhebliche Ersparnis der notwendigen Test- bzw. Betriebserfahrung

# Beispiele

## Optimierung des Nachtestens

- ◆ System bestehend aus zwei Komponenten
- ◆ Ziel ist der Nachweis von  $p^*=0.0001$  zur Aussagesicherheit  $\beta=0.99$
- ◆ Umfang an Betriebserfahrung pro Komponente:
  - $n_1=16000$
  - $n_2=42000$
- ◆ Betriebsprofil:  $\gamma_1=0.25$ ,  $\gamma_2=0.75$
- ◆ Momentan nachweisbare Kenngrößen

$\beta$	$p^*$
<b>0.99</b>	0.0001114443
0.982047991	<b>0.0001</b>

# Beispiele

## Optimierung des Nachtestens

### ◆ Naiver Ansatz:

Verteilung zusätzlicher Testfälle  $m_i$ ,  $i \in \{1,2\}$  gemäß der Häufigkeit der Auswahl der Komponenten im Betrieb ( $m_i \approx \gamma_i \cdot \sum m_i$ ):

$n_1=16000$	$m_1=2094$	$n_1+m_1=18094$
$n_2=42000$	$m_2=12282$	$n_2+m_2=54282$
$n_1+n_2=58000$	$m_1+m_2=14376$	$\Sigma=72376$

### ◆ Optimale Verteilung (durch numerische Optimierung):

$n_1=16000$	$m_1=4331$	$n_1+m_1=20331$
$n_2=42000$	$m_2=1300$	$n_2+m_2=43300$
$n_1+n_2=58000$	$m_1+m_2=5631$	$\Sigma=63631$

# Fazit

- ◆ Neuer Ansatz zur Bestimmung von Zuverlässigkeitskenngrößen auf Basis der gewonnenen Betriebserfahrung beschrieben
- ◆ Statistisch fundierte Kombination komponentenspezifischer Zuverlässigkeitsaussagen
- ◆ Leitlinie zur Beschreibung der wesentlichen Schritte zur Extraktion, Auswertung und Ergänzung statistisch relevanter operationaler Daten
- ◆ Vorteile:
  - Nachweis höherer Zuverlässigkeit zu gegebener Aussagesicherheit
  - Nachweis vorgegebener Zuverlässigkeitsaussagen mit erhöhter Aussagesicherheit
  - **Reduktion des bisher zum Nachweis erforderlichen Aufwands an Test- bzw. Betriebserfahrung**
  - **Unterstützung der praktischen Anwendbarkeit statistischer Verfahren zum Zuverlässigkeitsnachweis**

Vielen Dank für die Aufmerksamkeit!

Fragen?