A Component-based Approach for Assessing Reliability of Compound Software

Monica Kristiansen*, Bent Natvig, Harald Holone

2014-06-23

Introduction

- Before computerized systems can be used in any kind of critical applications, evidence that these systems are dependable is required.

Introduction

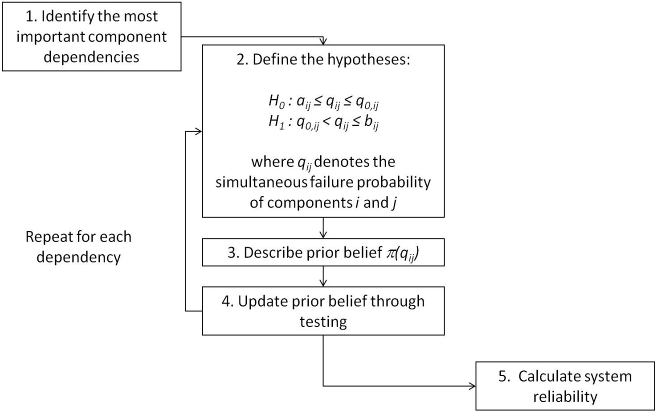
- Most computerized systems are built as a structure consisting of several software components.
- There is therefore a need for methods for assessing reliability of compound software.

Approach

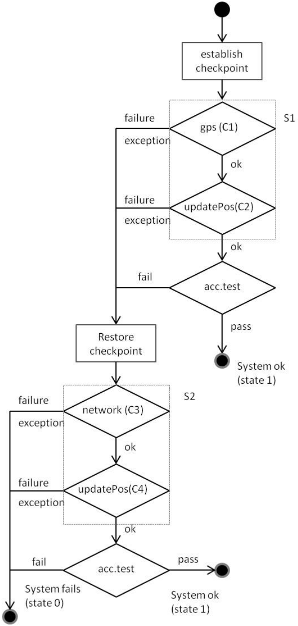
A component-based approach for assessing reliability of compound software in which failure dependencies between software components are explicitly addressed.

- Find accepted upper bounds for probabilities that pairs of software components fail simultaneously.
- Include these upper bounds into the reliability models.

Approach


1. Identify the most important component dependencies
2. Define the hypotheses:
$H_0 : a_{ij} \leq q_{ij} \leq q_{0,ij}$
$H_1 : q_{0,ij} < q_{ij} \leq b_{ij}$
where q_{ij} denotes the simultaneous failure probability of components i and j
3. Describe prior belief $\pi(q_{ij})$
4. Update prior belief through testing
Repeat for each dependency
5. Calculate system reliability

Case - mobile positioning system



Based on the software system's minimal path sets, the reliability of the system is given by:
$P(\phi(\mathbf{x}) = 1) = p_{12} + p_{34} - p_{1234}$.

Restrictions

Marginal reliabilities	Marginal failure probabilities
$p_1 = 0.99$	$q_1 = 0.01$
$p_2 = 0.9999$	$q_2 = 0.0001$
$p_3 = 0.999$	$q_3 = 0.001$
$p_4 = 0.9999$	$q_4 = 0.0001$
Simultaneous reliabilities	**Simultaneous failure probabilities**
$p_{12} \in [0.989901, 0.99]$	$q_{12} \in [10^{-6}, 10^{-4}]$
$p_{13} \in [0.98901, 0.99]$	$q_{13} \in [10^{-5}, 10^{-3}]$
$p_{14} \in [0.989901, 0.99]$	$q_{14} \in [10^{-6}, 10^{-4}]$
$p_{23} \in [0.9989001, 0.999]$	$q_{23} \in [10^{-7}, 10^{-4}]$
$p_{24} \in [0.99980001, 0.9999]$	$q_{24} \in [10^{-8}, 10^{-4}]$
$p_{34} \in [0.9989001, 0.999]$	$q_{34} \in [10^{-7}, 10^{-4}]$
$p_{123} \in [0.988911099, 0.99]$	$q_{123} \in [10^{-9}, 10^{-4}]$
$p_{124} \in [0.98980201, 0.99]$	$q_{124} \in [10^{-10}, 10^{-4}]$
$p_{134} \in [0.988911099, 0.99]$	$q_{134} \in [10^{-9}, 10^{-4}]$
$p_{234} \in [0.99880021, 0.999]$	$q_{234} \in [10^{-11}, 10^{-4}]$
$p_{1234} \in [0.988812208, 0.99]$	$q_{1234} \in [10^{-13}, 10^{-4}]$

Identifying the most important dependencies

- One of the rules for selecting the most important component dependencies, state that including the dependency between the most unreliable data-parallel components gives predictions close to the system's true reliability.
- When only including the dependency between components 1 and 3, the reliability of the complete software system becomes: $P(\phi(\mathbf{x}) = 1) = p_1 p_2 + p_3 p_4 - p_{13} p_2 p_4$.

Defining the hypothesis

- Let's assume that it is required that the reliability of the software system should be at least 0.9999 with confidence level $C_0 = 0.99$.
- Based on this requirement and the addition law of probability, a predefined upper bound $q_{0,13} = 0.00009891$ for the simultaneous failure probability q_{13} can be calculated.
- Based on the upper bound $q_{0,13}$ and the restrictions $[a_{13}, b_{13}]$ on the simultaneous failure probability q_{13}, the following hypotheses can be defined:

$$\begin{aligned} H_0 &: 0.00001 \leq q_{13} \leq 0.00009891 \\ H_1 &: 0.00009891 < q_{13} \leq 0.001. \end{aligned} \tag{1}$$

Describing prior belief regarding the failure probability

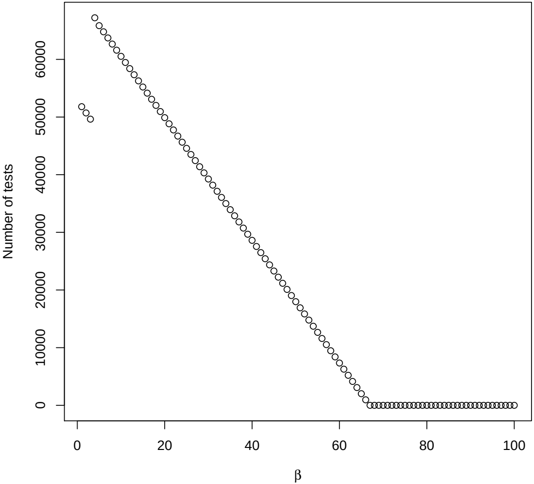
1. Classical statistical testing (assuming a uniform distribution), where no prior information about the simultaneous failure probability q_{13} is included.
2. Bayesian hypothesis testing, where only the restrictions imposed on q_{13} by the marginal failure probabilities are taken into account.
3. Bayesian hypothesis testing, where additional prior information about the simultaneous failure probability q_{13} (assuming a beta distribution with $\alpha = 1$ and $\beta = 66$) is taken into account.

Results

The number of fault free tests, n, required to obtain the upper bound $q_{0,13}$ at the given predefined confidence level $C_{0,13} = 0.99$ is:

1. 46557 using classical statistical testing.
2. 51793 using only the restrictions imposed on q_{13} by the marginal failure probabilities q_1 and q_3.
3. 951 when using additional information about the simultanious failure probability q_{13}.

Number of tests



- $\alpha = 1$
- $0 \leq \beta \leq 100$

Mahalo

Questions?