IT4Innovations national supercomputing center

BRNO UNIVERSITY OF TECHNOLOGY — FACULTY OF INFORMATION TECHNOLOGY

Using Statistical Model Checking to Assess Reliability for Bathtub-Shaped Failure Rates

Josef Strnadel (http://www.fit.vutbr.cz/∼strnadel, strnadel@fit.vutbr.cz)

Key terms and definitions

Features of a system

Functionality | Performance | Cost | **Dependability** | ...

Dependability [1]
- Threats
- **Attributes**
  - Availability
  - **Reliability**
  - Safety
  - Integrity
  - Maintainability
- Means

Reliability can be meant in a **qualitative** or a **quantitative** manner [2]; we concentrate on the latter one.

Phenomena —Action→ **Fault** —Activation→ **Error** —Propagation→ **Failure**

The occurrence times of faults etc. **cannot be specified certainly**, but by means of the probability theory:

- X_{TTF} ... a continuous random variable representing the **time to fault** (**TTF**)
- $f(t)$ ... the **probability density function** (**PDF**) of X_{TTF} representing the probability that a system fails in t
- $F(t)$ ... prob. that a failure occurs before or at t; the **cumulative distribution function** (**CDF**) of X_{TTF}:

$$F(t) \stackrel{def}{=} \int_{-\infty}^{t} f(x)\,dx$$

- $R(t)$ ... **reliability function** (**reliability**): prob. that a failure occurs after t:

$$R(t) \stackrel{def}{=} 1 - F(t) = \int_{t}^{\infty} f(x)\,dx$$

- $h(t)$ ... **failure/hazard** (**rate**) **function**: prob. that a failure occurs in $[t, t+dt]$ given that no has occurred before:

$$h(t) \stackrel{def}{=} \frac{dF(t)}{dt} \times \frac{1}{R(t)} = \frac{f(t)}{R(t)}$$

The quantification gets complicated by many real circumstances (such as fault dynamics/dependencies, multiplicity of faults, state-dependent behavior, repair failures, shared load/repair facilities).

References

[1] J.-C. Geffroy and G. Motet, *Design of Dependable Computing Systems*. Hingham: Kluwer Academic Publishers, 2002.

[2] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004. DOI 10.1109/TDSC.2004.2.

[3] A. David, K. Larsen, A. Legay, M. Mikucionis, and D. Poulsen, "Uppaal SMC Tutorial," *International Journal on Software Tools for Technology Transfer*, vol. 17, no. 4, pp. 397–415, 2015. DOI 10.1007/s10009-014-0361-y.

Cooperation/research plans

- To **search for real problems** to solve.
- Assessment and validation using real-world data – **we search for partner(s)**.
- Reliability assessment in the areas of **repairable** and **reconfigurable** systems.
- Assessment of **maintainability/availability** and assessment under a **mixture of** permanent, transient and intermittent **faults**.
- **Maintainance** planning/optimization.
- **Contact**:

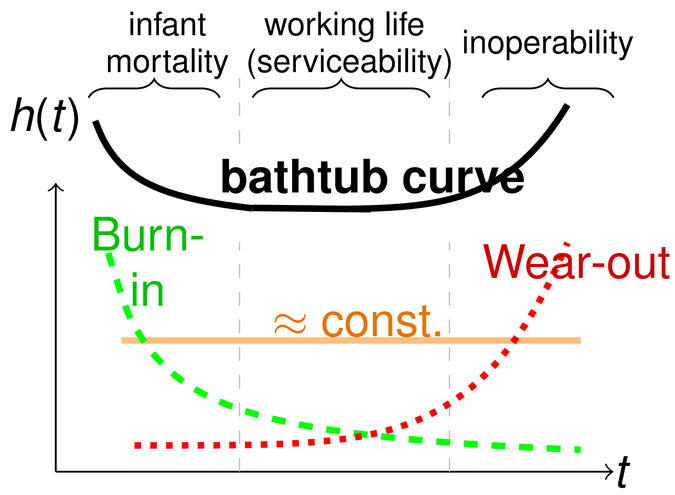
strnadel@fit.vutbr.cz

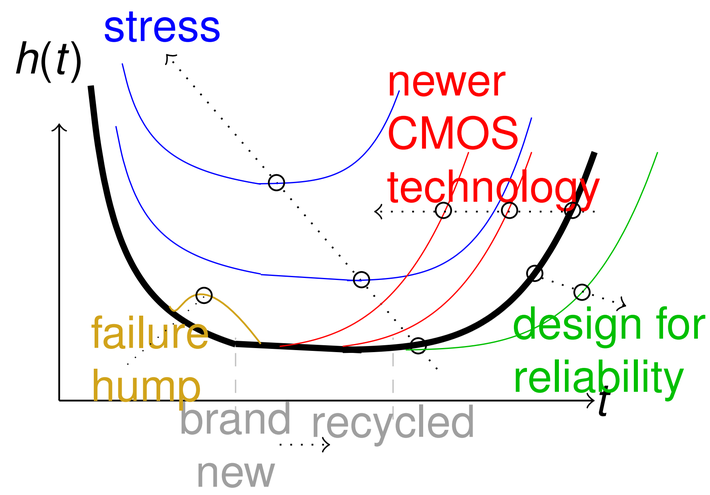
Acknowledgment

This work was supported by

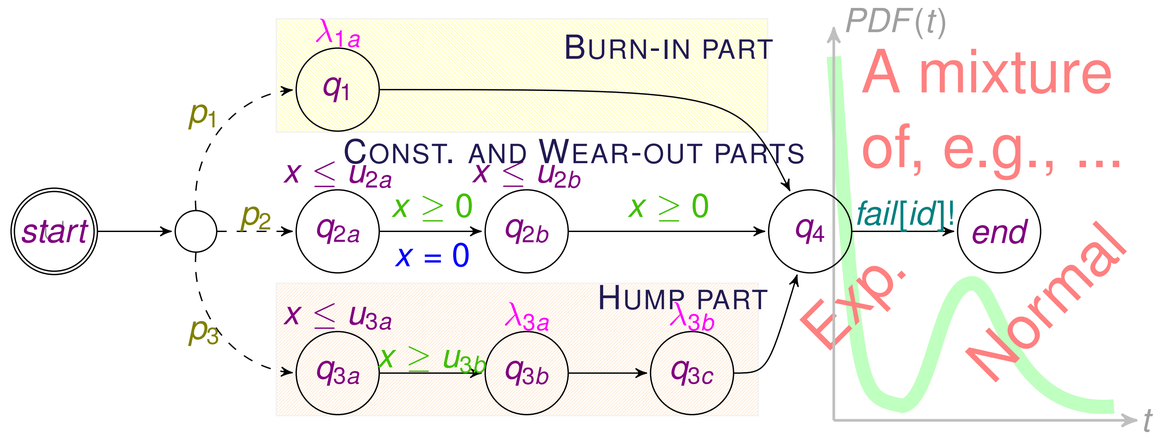
- The Ministry of Education, Youth and Sports from the National Programme of Sustainability (NPU II) **project IT4Innovations excellence in science** – LQ1602,
- the **project Advanced Parallel and Embedded Computer Systems** (FIT-S-17-3994).

What are typical components/shapes of a bathtub-shaped h(t) ?



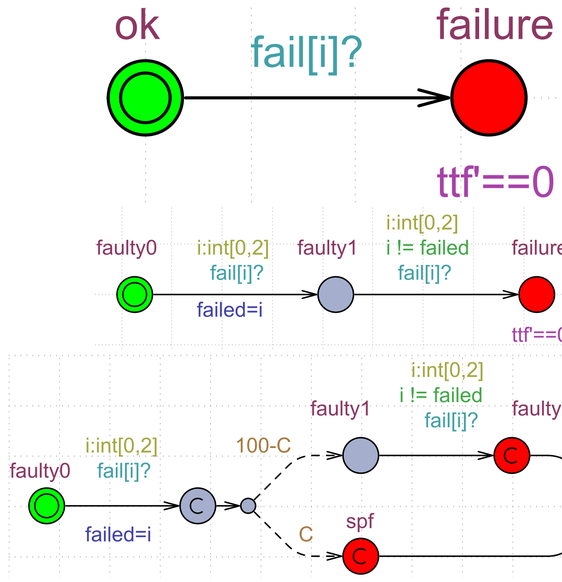


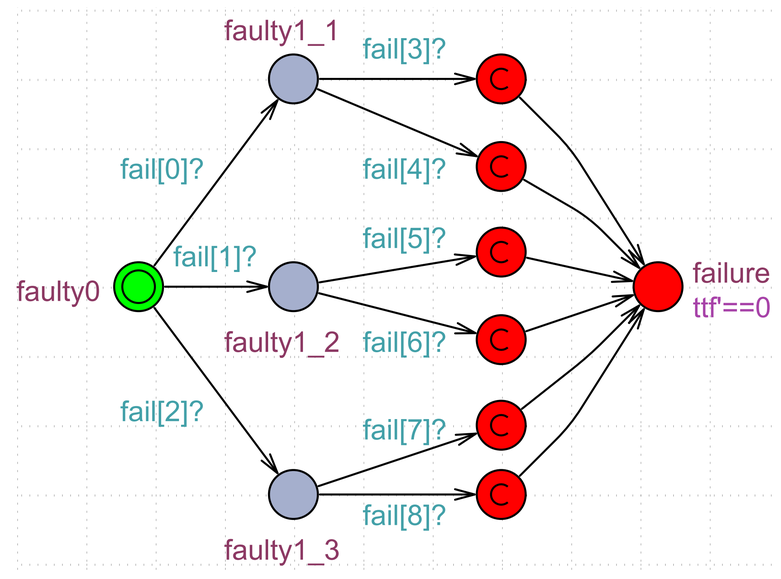
How we model the random variable with a bathtub-shaped h(t) ?



- p_1, p_2, p_3 ... probabilistic choice,
- λ_{1a}, λ_{3a}, λ_{3b} ... exponential probability distributions,
- u_{2a}, u_{2b}, u_{3a}, u_{3b} ... uniform probability distributions,
- *id* ... *identification of the produced fault*

Our reliability models of simple systems. Ask us to know-how.





What is the probability of a failure within the given time ?

```
Pr[<= time_bound] {<> MODEL.failure}
```

Representative results for a simplex system