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

Josef Strnadel
Brno University of Technology, Faculty of Information Technology, Centre of Excellence IT4Innovations
Bozetechova 2, 612 66 Brno, Czech Republic
Email: strnadel@fit.vutbr.cz, Telephone: +420 541141211

***Abstract*—Ideally, the reliability can be assessed analytically, provided that an analytical solution exists and its presumptions are met. Otherwise, alternative approaches to the assessment must apply. This paper proposes a novel, simulation based approach that relies on stochastic timed automata. Based on the automata, our paper explains principles of creating reliability models for various scenarios. Our approach expects that a reliability model is then processed by a statistical model checking method, used to assess the reliability by statistical processing of simulation results over the model. Main goal of this paper is to show that instruments of stochastic timed automata and statistical model checking are capable of facilitating the assessment process even for adverse conditions such as bathtub shaped failure rates.**

***Index Terms*—reliability, assessment, reliability model, fault, failure, stochastic automaton, timed automaton, simulation, statistical model checking**

I. Introduction

Dependability is a complex feature composed of many attributes such as reliability [1], each of them must be quantified separately to form a partial "image" about the dependability. From the reliability viewpoint, this is done through the reliability assessment process, simply "assessment". The assessment must be based on precisely defined concepts. Since supposedly identical systems, operating under similar conditions, fail at different times, any related phenomenon can only be expressed stochastically.

For special cases, such as the exponentially distributed probability density function of a time-to-fault random variable the assessment can be done on the analytical basis [2]. However, for an arbitrary case, an analytical solution may not exist, so an alternative solution must be found instead. In the paper, we show that instruments such as stochastic timed automata and statistical model checking are strong enough to carry out the assessment process even if an analytical solution is unknown. Particularly, we show that for systems with bathtub-shaped failure rates.

The paper is organized as follows. Sect. II presents a short background to the reliability assessment problem. It introduces the problem definition, basic attributes and formulas, bathtub-shaped failure rates and existing approaches to the problem, instruments used in this paper and a motivation of our research. Sect. III presents our approach, shows its applicability for systems with bathtub-shaped failure rates and summarizes representatives of results we have achieved. Sect. IV concludes the paper.

II. Research Background

A. Problem Definition

At this point, we summarize some terms/symbols needed to describe the assessment problem formally. To save the space, we have limited our paper to just non-repairable systems.

1) Basic Attributes of Reliability: Let X_{TTF} be a continuous random variable representing the time to failure (TTF) and let the following notation be introduced: $f_{X_{TTF}}(t)$, $F_{X_{TTF}}(t)$ and $R_{X_{TTF}}(t)$ represent the probability density function (PDF), cumulative distribution function (CDF) and reliability function ("reliability" in brief) of X_{TTF}. Based on $f_{X_{TTF}}(t)$, further attributes can be quantified (see Tab. I). If it is unambiguous, we can omit X_{TTF} to simplify the notation. Formally, the reliability assessment problem is defined as a problem of evaluating attributes of the reliability.

2) Analytical Solutions: Analytical solutions to the assessment problem are known just under special assumptions [2]. For example, such an assumption may expect that X_{TTF} and X_{TTR} follow certain probability distribution. Particularly, for exponentially distributed X_{TTF} (parameterized by λ), the following analytical solution exists (in the simplified notation): $f(t) = \lambda e^{-\lambda t}$, $F(t) = 1 - e^{-\lambda t}$, $R(t) = e^{-\lambda t}$, $h(t) = \lambda$, $MTTF = \frac{1}{\lambda}$. Despite such assumptions comply with a wide range of practical needs, they may be very limiting and not strong enough to cope easily (or, at all) with issues such as assessing the reliability of a system across its life time [3]–[6] or "dynamic reliability" [7], [8]. Lacks of conventional approaches – especially, their complexity, limited applicability/precision and/or long assessment time – have motivated us to cope with the issues using unconventional instruments.

3) Bathtub-Shaped Failure Rates: Special assumptions and limitations from II-A2 cause that the assessment of electronic

TABLE I
Basic symbols and formulas to assess the reliability

Attribute		
Symbol	**Evaluation**	**Meaning**
$f_{X_{TTF}}(t)$	identified empirically	probab. dens. fun. (PDF)
$F_{X_{TTF}}(t)$	$\int_{-\infty}^{t} f_{X_{TTF}}(x)\ dx$	cumul. distrib. fun. (CDF)
$R_{X_{TTF}}(t)$	$1 - F_{X_{TTF}}(t)$	reliability (survival) funct.
$h_{X_{TTF}}(t)$	$f_{X_{TTF}}(t)/R_{X_{TTF}}(t)$	hazard/failure (rate) fun.
$MTTF_{X_{TTF}}$	$\int_0^\infty t \times f_{X_{TTF}}(t)\ dt =$ $= \int_0^\infty 1 - F_{X_{TTF}}(t)\ dt$	mean time to failure (MTTF)

978-3-9819263-2-3/DATE19/©2019 EDAA

systems is only carried out for the working life (constant) region of the so-called bathtub curve (Fig. 1a). As the assessment typically does not reflect the burn-in and wear-out regions, it is very difficult (or even impossible) to study impacts of these regions to the reliability. But, importance of these regions is evident as they affect the bathtub depending on facts such as stress [9], [10], CMOS technology [11], design for reliability means [11], failure hump [12] or recycling [13] – see Fig. 1b.

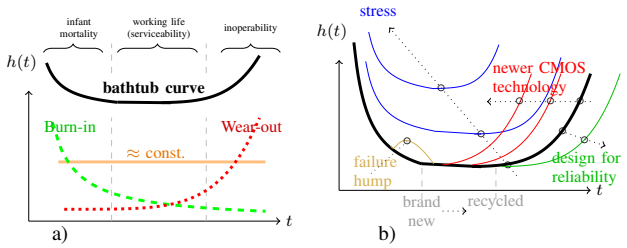

Fig. 1. Bathtub curve: a) its typical shape and components, b) effects of various phenomena to its shape.

To be serious, and for the sake of completeness, let us mention that some papers, such as [14], criticize this (commonly accepted) bathtub model.

B. Existing Non-Analytical Solutions

Many recent alternatives to the analytical solution of the reliability assessment problem rely on the Monte Carlo simulation [15]. However, they suffer from the long running time and a need to solve further problems, such as speeding up the simulation [16], to make the assessment applicable in practice. Authors of [17] substituted the Monte Carlo approach by a more efficient stochastic analysis over a restricted model. Further works, such as [18]–[20], build on Markov models and reward models with stochastic behaviors. They use the "classical" model checking (MC) technique [21] from the PRISM tool [22] to check whether a system surely satisfies a property stated in a specification logic. But, this kind of checking rises two problems. Firstly, it suffers from the state explosion problem for industrial/life-size systems. Secondly, it produces just binary decision (satisfied or violated) about a property. Moreover, recent assessment is typically performed incompletely, i.e., over a fraction of the bathtub curve.

C. Reasoning and Instruments of our Research

To overcome the problems of existing approaches we have based our approach on the so-called statistical model checking (SMC) technique [23]. Simply said, this technique conducts simulations over a stochastic model, monitors them and processes them statistically to infer, with a predefined degree of confidence, whether they provide a statistical evidence for the satisfaction/violation of a property. SMC techniques are advantageous due to the following facts. Firstly, they replace the binarity (regarding the satisfaction) by the ability to quantify the impact of a change in a system [24]. Practically, this allows one to get estimates of the probability measure on the satisfaction of a property, not just producing a simple "Yes"/"No" answer. Secondly, they easily scale to industrial size systems: according to [25], they scale logarithmically in the size of models, are trivially parallelizable and still scale sub-linearly in the time domain.

To assess the reliability of a system across the bathtub-shaped failure rate, we must be able to model such a rate first. But, creating such a model is a problem in itself, being typically approximated analytically, e.g., by adjusting parameters of some distributions [3]–[5]. But, approaches like that are rather academic than practical as they are able to model the effects from Fig. 1b only with great difficulty, or not at all. In this paper, we show that such a model including the effects can be easily created by means of the so-called stochastic timed automata (STA) introduced, e.g., in [26].

III. Our Approach

During our research, we have utilized STA/SMC means being implemented in the publicly available Uppaal SMC tool [27]. Availability of the tool allows anyone to test our approach, evaluate it and check whether it is applicable to desired areas of interest. This section is organized as follows. Firstly, it presents our approach to modeling the bathtub-shaped failure rate by means of STA (III-A). Secondly, it sketches our solution to the reliability assessment problem by means of STA and SMC (III-B). Finally, it summarizes results for representative reliability models and bathtubs (III-D).

A. Modeling the Bathtub Curve

Our model of the bathtub curve is depicted in Fig. 2. It is an STA configurable by parameters summarized in Tab. II. The model starts in "start". From $start$, it moves instantly to q_1, q_{2a} or q_{3a} with the probability given by $\frac{p1}{p1+p2+p3}$, $\frac{p2}{p1+p2+p3}$, $\frac{p3}{p1+p2+p3}$, resp. Time of its staying in q_1 (i.e., the burn-in region) is given by the exponential probability distribution parameterized by λ_{1a}. q_{2a} and q_{2b} model the constant and wear-out regions by composing two uniformly distributions into the Normal probability distribution with its mean set to $u_{2b}-u_{2a}$ and its standard deviation set to $\frac{u_{2b}-u_{2a}}{2}$. The hump region is modeled by q_{3a}, q_{3b} and q_{3c}, composing one uniform (q_{3a}) and two exponential (q_{3b}, q_{3c}) distributions. From q_1, q_{2b} and q_{3c}, the model moves to q_4 and signalizes the occurrence of a fault by sending a signal via the given $fail$ channel. This is our way of modeling X_{TTF} as defined in II-A. Fig. 2 is a template that may be instantiated many times to produce multiple faults, each identified by id and given by the corresponding X_{TTF}.

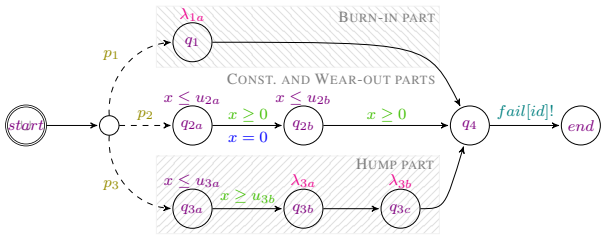

Fig. 2. Our method of modeling arbitrary bathtub-shaped failure/hazard rates according to Fig. 1b: the stochastic timed automata approach (the coloring is in accordance with practices of the Uppaal tool).

TABLE II
PARAMETERS OF OUR BATHTUB MODEL FROM FIG. 2

Parameter	
Symbol	**Used to configure**
p_1, p_2, p_3	probabilistic choice
λ_{1a}, λ_{3a}, λ_{3b}	exponential probability distribution
u_{2a}, u_{2b}, u_{3a}, u_{3b}	uniform probability distribution
id	identification of the produced fault

B. Reliability Assessment

The model of X_{TTF} is a prerequisite for constructing a reliability model of a system. Fig. 3 illustrates two reliability models to explain the main idea of such a construction – one for a simplex (SPX) and second for a triple modular redundant (TMR) system [28]. More complex models may be constructed analogically, using the following principle.

Basically, a reliability model is driven by the occurrence of a fault given by X_{TTF}. In our approach, it means that it is driven by receiving a signal via the corresponding $fail$ channel. Fig. 3a represents the simplest reliability model – the model of a system with a single/common point of a failure. It needs just one X_{TTF} and starts in $fault\text{-}free$. Here it waits until a fault (identified by id) occurs. Then, it moves to $failure$ representing a fault of the only module in the system. Fig. 3b represents the reliability model of a system able to tolerate one fault. The system consists of three independent, functionally equivalent replicas, each of them may fail separately. Here, we need three X_{TTF}s, one per a replica (identified by 0, 1 or 2). In the model, a replica is identified by i and is sensitive to a fault identified by i. The model starts in $fault\text{-}free$. Here it waits until a fault occurs. Then, its identifier is stored into $failed$ and the model moves to $faulty1$ – the system is still operational because it tolerates a faulty replica. If a fault occurs in $faulty1$, two replicas become faulty. As more than one fault cannot be tolerated, the system fails to be fault tolerant. This corresponds to $failure$ in Fig. 3b.

To check properties of reliability models, such as the probability of a failure, we utilize UPPAAL SMC [27]. At its input, it takes our model and a query about a property to be checked in the model. At its output, it produces various data such as PDF, CDF or mean w.r.t. the property. For example, a query may want the SMC engine to evaluate the probability of entering $failure$ (see Fig. 3). Such a query is of the probability estimation type and its form is $Pr[bound](\phi)$, where $bound$ defines how to bound simulation steps/runs and ϕ represents a property to be checked. For a model M to be examined within 10^5 units of time, the query would be $Pr[<= 100000](<> M.failure)$.

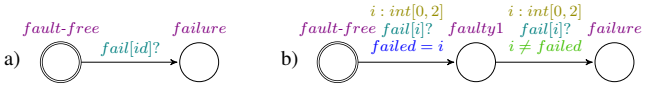

Fig. 3. Our approach to creating reliability models using stochastic timed automata: an illustration for a) SPX and b) TMR systems. The coloring is in accordance with practices of the UPPAAL tool.

C. Assessment Control and Overheads

UPPAAL SMC is driven by parameters such as Probability uncertainty (ε), the values of which strongly affect both the accuracy of SMC results and duration of the assessment process. For example, our results in Fig. 4 show that the values of observed quantities decrease inversely proportionally to ε.

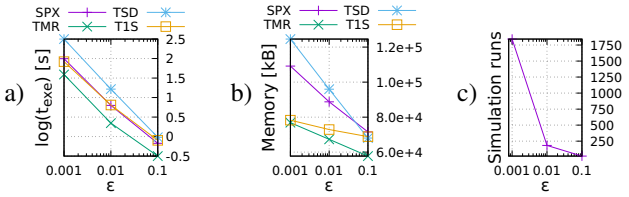

Fig. 4. Impact of ε to the following parameters of the assessment process: a) simulation time, b) memory consumption, c) number of simulation runs (representative cutouts to show key trends). The comparison base (SPX, TMR) was extended by TSD and T1S representing fault tolerant systems not discussed in this paper, but detailed, e.g., in [28] – triplex with successive degradation and triplex with one spare, respectively.

D. Representative Results

Due to a very limited space in this paper, we have decided to present only representative results of experiments over SPX and TMR systems, see Fig. 5 and Fig. 6, resp. In the experiments, we have utilized four variants of the bathtub to assess the reliability of SPX and TMR. The results show that i) our approach is able to model and parameterize phenomena from Fig. 1 as well as to evaluate quantities such as $R(t)$ or $h(t)$ and ii) effects such as newer CMOS technology or higher stress affect the reliability very negatively, comparing to a hump. As expected, the reliability of TMR is worse comparing to SPX because TMR consists of three replicas which may fail independently. This increases the probability of a failure, but allows TMR to to i) detect a fault and ii) be operational despite of a faulty replica.

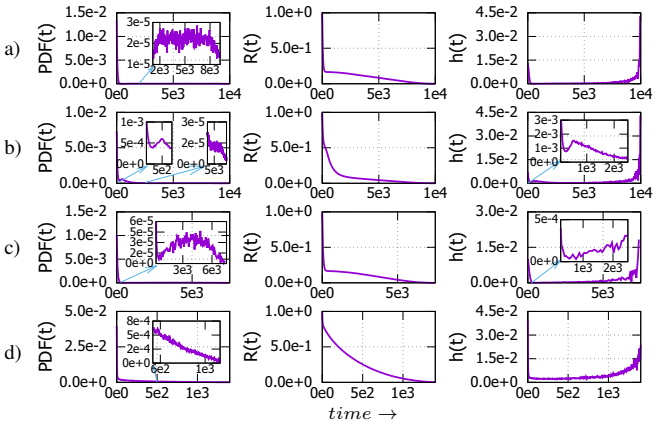

Fig. 5. SPX results for bathtubs given by the following 10-tuples (p_1, p_2, p_3 λ_{1a}, λ_{3a}, λ_{3b} u_{2a}, u_{2b}, u_{3a}, u_{3b}) of parameters from Tab. II: a) implicit (500, 100, 0, $\frac{1}{50}$, $\frac{1}{500}$, $\frac{10}{50}$, 2500, 7500, 500, 25), b) with a hump ($p_3 = 500$), c) newer CMOS technology ($u_{2b} = 5000$), d) higher stress ($p_1 = 750$, $\lambda_{1a} = \frac{1}{10}$, $u_{2a} = 5000$). MTTF values corresponding to the bathtub representatives and SPX are a) 865, b) 830, c) 654, d) 314.

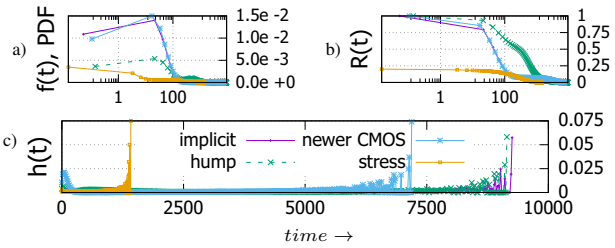

Fig. 6. TMR results for bathtubs specified in Fig. 5 – i) implicit, ii) with a hump, iii) newer CMOS and iv) stress. MTTF values corresponding to the bathtub representatives and TMR are i) 330, ii) 317, iii) 265, iv) 259.

IV. Conclusion

This paper presents a simulation based method able to assess reliability of systems in various bathtub scenarios reflecting phenomena such as failure hump, newer CMOS technology or stress. Actually, this is beyond the scope of existing approaches. The novelty of our method relies on unconventional instruments – stochastic timed automata, used to describe bathtub and reliability models, and statistical model checking, used to perform the assessment over the models. The efficiency and accuracy of the assessment are controllable by a set of parameters such as probability uncertainty.

Acknowledgment

This work was supported by The Ministry of Education, Youth and Sports of the Czech Republic from the National Programme of Sustainability (NPU II); project IT4Innovations excellence in science – LQ1602. Next, it was supported by the project Advanced parallel and embedded computer systems – FIT-S-17-3994.

References

[1] 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.

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

[3] T. Zhang, R. Dwight, and K. El-Akruti, "On a Weibull Related Distribution Model with Decreasing, Increasing and Upside-Down Bathtub-Shaped Failure Rate," in *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, Jan 2013, pp. 1–6, DOI 10.1109/RAMS.2013.6517749.

[4] Y. Lu, A. A. Miller, R. Hoffmann, and C. W. Johnson, *Towards the Automated Verification of Weibull Distributions for System Failure Rates*. Cham: Springer International Publishing, 2016, pp. 81–96, DOI 10.1007/978-3-319-45943-1_6.

[5] V. Nekoukhou and H. Bidram, "A New Generalization of the Weibull-Geometric Distribution with Bathtub Failure Rate," *Communications in Statistics - Theory and Methods*, vol. 46, no. 9, pp. 4296–4310, 2017, DOI 10.1080/03610926.2015.1081949.

[6] J. B. Bowles, "Commentary - caution: constant failure-rate models may be hazardous to your design," *IEEE Transactions on Reliability*, vol. 51, no. 3, pp. 375–377, Sept 2002, DOI 10.1109/TR.2002.801850.

[7] J. Devooght, "Dynamic Reliability," *Advances in Nuclear Science and Technology*, vol. 25, pp. 215–278, 1997, DOI 10.1007/0-306-47812-9_7.

[8] P. Zhu, J. Han, L. Liu, and M. Zuo, "A stochastic approach for the analysis of fault trees with priority and gates," *IEEE Transactions on Reliability*, vol. 63, no. 2, pp. 480–494, 2014, DOI 10.1109/TR.2014.2313796.

[9] A. Dasgupta, K. Sinha, and J. Herzberger, *Reliability Engineering for Driver Electronics in Solid-State Lighting Products*. New York: Springer, 2013, pp. 243–284, DOI 10.1007/978-1-4614-3067-4_8.

[10] P. Maris Ferreira, H. Cai, and N. Lirida, "Reliability Aware AMS / RF Performance Optimization," in *Performance Optimization Techniques in Analog, Mixed-Signal, and Radio-Frequency Circuit Design*, M. H. F. Mourad Fakhfakh, Esteban Tlelo-Cuautle, Ed., Oct. 2014, DOI 10.4018/978-1-4666-6627-6.ch002.

[11] V. Huard, S. Mhira, F. Cacho, and A. Bravaix, "Enabling robust automotive electronic components in advanced cmos nodes," *Microelectronics Reliability*, vol. 76-77, pp. 13 – 24, 2017, DOI 10.1016/j.microrel.2017.07.064.

[12] W. K. L., "The roller-coaster curve is in," *Quality and Reliability Engineering International*, vol. 5, no. 1, pp. 29–36, 1989, DOI doi:10.1002/qre.4680050108.

[13] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled ic detection based on statistical methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 947–960, June 2015, DOI 10.1109/TCAD.2015.2409267.

[14] G. A. Klutke, P. C. Kiessler, and M. A. Wortman, "A critical look at the bathtub curve," *IEEE Transactions on Reliability*, vol. 52, no. 1, pp. 125–129, March 2003, DOI 10.1109/TR.2002.804492.

[15] K. Durga Rao, V. Gopika, V. Sanyasi Rao, H. Kushwaha, A. Verma, and A. Srividya, "Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment," *Reliability Engineering and System Safety*, vol. 94, no. 4, pp. 872–883, 2009, DOI 10.1016/j.ress.2008.09.007.

[16] Y. Liu, Y. Ren, L. Liu, and Z. Li, "A spark-based parallel simulation approach for repairable system," vol. 2016-April, 2016, DOI 10.1109/RAMS.2016.7447965.

[17] P. Zhu, J. Han, L. Liu, and F. Lombardi, "Reliability evaluation of phased-mission systems using stochastic computation," *IEEE Transactions on Reliability*, vol. 65, no. 3, pp. 1612–1623, 2016, DOI 10.1109/TR.2016.2570565.

[18] Z. Peng, Y. Lu, A. Miller, C. Johnson, and T. Zhao, "A Probabilistic Model Checking Approach to Analysing Reliability, Availability, and Maintainability of a Single Satellite System," in *Modelling Symposium (EMS), 2013 European*, Nov 2013, pp. 611–616, DOI 10.1109/EMS.2013.102.

[19] Y. Lu, Z. Peng, A. A. Miller, T. Zhao, and C. W. Johnson, "How Reliable is Satellite Navigation for Aviation? Checking Availability Properties with Probabilistic Verification," *Reliability Engineering & System Safety*, vol. 144, pp. 95 – 116, 2015, DOI 10.1016/j.ress.2015.07.020.

[20] R. Calinescu, C. Ghezzi, K. Johnson, M. Pezz, Y. Rafiq, and G. Tamburrelli, "Formal Verification With Confidence Intervals to Establish Quality of Service Properties of Software Systems," *IEEE Transactions on Reliability*, vol. 65, no. 1, pp. 107–125, March 2016, DOI 10.1109/TR.2015.2452931.

[21] C. Baier and J.-P. Katoen, *Principles of Model Checking*, ser. Representation and Mind. MIT Press, 2008.

[22] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: Probabilistic Model Checking for Performance and Reliability Analysis," *SIGMETRICS Perform. Eval. Rev.*, vol. 36, no. 4, pp. 40–45, Mar. 2009, DOI 10.1145/1530873.1530882.

[23] G. Agha and K. Palmskog, "A Survey of Statistical Model Checking," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 28, no. 1, pp. 6:1–6:39, Jan. 2018, DOI 10.1145/3158668.

[24] K. G. Larsen and A. Legay, "Statistical model checking past, present, and future," in *Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications*, T. Margaria and B. Steffen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 135–142, DOI 10.1007/978-3-662-45231-8_10.

[25] J. H. Kim, A. Boudjadar, U. Nyman, M. Mikucionis, K. G. Larsen, and I. Lee, "Quantitative Schedulability Analysis of Continuous Probability Tasks in a Hierarchical Context," in *2015 18th International ACM SIGSOFT Symposium on Component-Based Software Engineering (CBSE)*, May 2015, pp. 91–100, DOI 10.1145/2737166.2737170.

[26] N. Bertrand, P. Bouyer, T. Brihaye, Q. Menet, C. Baier, M. Größer, and M. Jurdzinski, "Stochastic Timed Automata," *Logical Methods in Computer Science*, vol. 10, no. 4, 2014, DOI 10.2168/LMCS-10(4:6)2014.

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

[28] B. Ricky W. and J. Sally C., "Techniques for modeling the reliability of fault-tolerant systems with the markov state-space approach," Tech. Rep., 1995. [Online]. Available: http://shemesh.larc.nasa.gov/fm/papers/Butler-RP-1348-Techniques-Model_Rel-FT.pdf