On Dependability Assessment of Fault Tolerant Systems by Means of Statistical Model Checking

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*—The problem of dependability assessment can be solved analytically just under predefined conditions. If they do not hold, alternative approaches must apply. Widely, they rely on the Monte Carlo simulation, suffering by the high computational complexity. Some rest on further instruments such as probabilistic timed automata that have been shown to be efficient to solve problems in various areas. However, more general as well as precise and faster instruments such as stochastic timed automata (STA) and statistical model checking (SMC) are available for the same purpose the moment. In the paper, basic terms and principles behind the construction of reliability models and dependability assessment on the STA/SMC basis are summarized, followed by a demonstration of their practical applicability in the area of non-repairable systems. Our main goal is to show that, instruments of STA/SMC can facilitate the dependability assessment process even in adverse conditions such as presence of multiple faults of various parameters.**

***Index Terms*—fault tolerant system; dependability; assessment; reliability model; simulation; fault; failure; rate; fault tolerant; stochastic timed automaton; statistical model checking; triple modular redundancy; UPPAAL SMC**

I. Introduction

The ability of a system to provide a required service and to perform it for a specified period of time within specified tolerances and other conditions is denoted as *dependability*. It can be meant in a qualitative or a quantitative manner [1]. Qualitatively, it can be seen as "the ability to deliver a service that can be justifiably trusted" [1] or, as a property such that "reliance can be justifiably placed on the services delivered by the system" [2]. Since dependability is a complex feature composed of many attributes, the (overall) dependability cannot be simply quantified by a single value. Instead, the attributes are quantified to form a complex image about dependability. As the time of occurrence of a fault, error or failure cannot be specified certainly, the attributes are typically described by means of the probability theory based on which attributes such as reliability, maintainability or availability can be quantified.

For the quantification purposes, let X_{TTF} be a continuous random variable representing the *time to failure* (*TTF*) and $f(t)$ be its *probability density function* (*PDF*), representing the probability that a system fails in t. Next, let $F(t)$ be the probability that a failure occurs before or at t. Formally, $F(t)$ is the *cumulative distribution function* (*CDF*) of the X_{TTF} defined by $F(t) = \int_{-\infty}^{t} f(x)\ dx$. Next, let $R(t)$ be the *reliability function* (or, simply *reliability*) defined as the probability that a failure occurs after t; formally, $R(t) \stackrel{def}{=} 1 - F(t) = \int_{t}^{\infty} f(x)\ dx$. Since $R(t)$ represents the probability of surviving by t, it is called a *survival function* too.

Based on the above mentioned definitions, further functions can be constructed and further attributes can be quantified based on various measures [3]. Out of those, let us limit our illustration herein just to $h(t)$ and *MTTF* (*Mean Time To Failure*), details to which follow. $h(t)$ is the *hazard* (*rate*) *function* that represents the probability that a failure occurs in $[t,\ t + dt]$ given that no failure has occurred prior to t. Formally, $h(t) \stackrel{def}{=} \frac{dF(t)}{dt} \times \frac{1}{R(t)} = \frac{f(t)}{R(t)}$. For a *non-repairable* system, *MTTF* is the measure utilized to quantify the mean time to the first (and only) failure in the system; formally, $MTTF = \int_0^{\infty} t \times f(t)\ dt = \int_0^{\infty} R(t)\ dt$.

To facilitate the quantification process, so-called *reliability models* [2] are widely utilized. Without any loss of generality, we have decided to limit this paper just to representatives of reliability models and dependability assessment techniques w.r.t. non-repairable systems (e.g., Fig. 1 or [4]). This paper is organized as follows. Sect. II introduces the (dependability assessment) problem, Sect. III presents key aspect of our approach based on the instruments, completed by demonstrative case studies and results. Sect. IV concludes the paper.

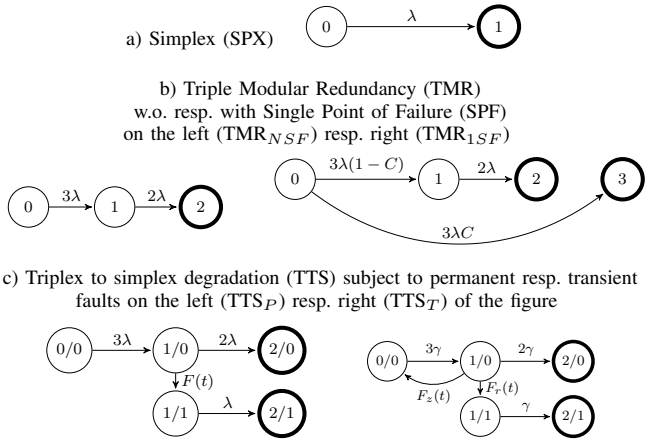

Fig. 1. (Semi-)Markov models of selected fault tolerant (FT) systems: simplex w.o. FT (a), FT based on the static redundancy (b). λ resp. γ are the permanent resp. transient failure rates, $F(t)$ is CDF used to model the isolation of a permanently faulty module, $F_r(t)$ resp. F_z(t) model isolation of a module due a transient fault resp. disappearance of a transient fault, C is the ratio of SPF faults

978-1-5386-2146-2/17 $31.00 © 2017 IEEE
DOI 10.1109/DSD.2017.12

II. Towards the Assessment Problem

For special cases of X_{TTF}, expressed using the well-known types of probability distribution (*exponential*, *normal*, *Weibull*, *gamma*, *lognormal* etc.), the quantification can be done on the analytical basis [2]. Particularly, for the exponentially distributed X_{TTF}, parameterized by λ, it holds $f(t) = \lambda e^{-\lambda t}$, $F(t) = 1 - e^{-\lambda t}$, $R(t) = e^{-\lambda t}$, $h(t) = \lambda$, $MTTF = \frac{1}{\lambda}$.

However, for an arbitrary X_{TTF}, such an analytical solution may not exist, so an alternative one must apply. Those alternatives are typically based on the *Monte Carlo* simulation [5] the long running time of which needs to be softened somehow – e.g. by speeding up the simulation [6]. Works such as [7] show that the analysis based on the stochastic models and techniques is more efficient than the Monte Carlo simulation at the same execution complexity in the number of runs; however, that approach is limited just to non-repairable systems.

It should be emphasized that the long simulation time is not the only problem w.r.t. alternative approaches. For example, to model the hazard rate of the bathtub shape is a problem in itself, being typically approximated analytically by adjusting parameters of the Weibull distribution [8]. Moreover, the analysis is complicated by facts such as dependencies among faults, dynamic behavior of faults, state-dependent behavior, faults being introduced before the recovery process is completed or complexity of the recovery mechanisms. To cope problems like that, techniques such as dynamic fault-tree models are available [9]. But, methods able to analyze dynamic fault-trees lead to similar disadvantages mentioned above, i.e. they require complex analytical procedures and/or long simulation time for the accurate analysis [10].

To cope with the problems, many works based on the PRISM [11] tool exist. Those works are based on Markov chains and reward models with stochastic behaviors; properties of a system can be checked by the PRISM's *model checking* (*MC*) engine. Although PRISM itself is able to cover a wide range of quantitative properties for various probabilistic, discrete time models including (*Priced*) *Probabilistic Timed Automata*, it does not support the analysis of reward-based metrics like throughput and buffer occupancy. Furthermore, it lacks features such as the concept of urgency (utilized e.g. in UPPAAL [12], [13]) to ease controlling resolution of non-determinism. Actually, further instruments such as *Stochastic Timed Automata* (*STA*s) exist that do not suffer by the above-mentioned lacks. Moreover, [14] shows that the approach utilized in [13] is not only more general, but also much faster comparing to PRISM. Alike, it has been shown w.r.t. MATLAB [15]. The advantages of the UPPAAL's instruments – especially, its ability to model continuous-time systems in a fully stochastic way and to analyze their parameters efficiently – has motivated us to rely our approach on them. Moreover, their applicability has not been explored enough w.r.t. the dependability assessment.

TABLE I
Illustration to Faults and Their Attributes

Fault Attributes			
Id	**Type** P: permanent T: transient	**Random Variable Details**	
		X_{TTF} **(Arrival times)**	X_{TTD} **(Departure times)**
0	T	Uni(0, 100)	Uni(0, 200)
1	P	Uni(0, 500)	–
2	T	Exp($\frac{1}{80}$)	Uni(0, 10)
3	T	Exp($\frac{1}{4}$)	Exp(1)
4	P	Exp($\frac{1}{5000}$)	–

It can be summarized that widely utilized reliability models are able to cover a wide range of practical needs. However, there are scenarios that make the dependability assessment process more difficult. Those scenarios include e.g. assessment i) for an arbitrary X_{TTF}, ii) across the entire bathtub curve, iii) under dependent faults, iv) under various fault scenarios such as multiplicity of faults, combination of permanent, transient and/or intermittent faults, faults with dynamically varying parameters, v) for dynamic, evolvable/reconfigurable systems capable to add, remove their components and/or change their parameters at run-time, vi) in the context of further features such as liveness, safety, security and/or timing, power and other constraints.

The difficulties give us a motivation for our research. Actually, we concentrate our efforts to the assessment under selected fault scenarios, principles and results of which we present in this paper. Although our approach can be easily extended to cope with remaining difficulties as well, we have decided to publish the related facts separately.

III. Our Approach

To demonstrate practical applicability of our ideas, we have utilized the publicly available UPPAAL SMC tool [13]. It is a toolbox designed for the modeling and analysis of *real-time* systems using (a network of) STAs It allows one to create a model of a discrete, continuous or hybrid (discrete/continuous) system and to check properties of (a deterministic or stochastic model of) the system in the given stochastic environment or conditions such as faults due to radiation. A property, such as MTTF, may be checked by the so-called *statistical model checking* (SMC) technique available within the toolbox. For the purpose, a property is expressed in the form of so-called *query*, which may be of various types (e.g., *probability estimation*, *hypothesis testing*, *probability comparison*).

In our previous work [16], we have utilized the STA/SMC means to construct and analyze a stochastic model allowing us to specify the behavior and dynamics of faults that may affect a system during the simulation time. Also, we have dealt with the modeling of faults characterized by the hazard function of the bathtub shape. In this paper, we focus to principles of creating reliability models and dependability assessment on the STA/SMC basis. To be beneficial for its readers, the consecutive text tends to give an illustrative overview of key (representative) ideas and instruments rather than to be exhaustive. Basic skeleton of our method can be summarized as follows:

- Based on the type and parameters of expected faults, utilize the STA means to create the models of i) fault

generators/sources and ii) staying of faults in a system, *fault behavior models* in short.

- Using the STA means, create the *reliability model* of a system being examined. Let the reliability model be driven by the fault behavior models resulting from the the previous step.
- Construct and utilize appropriate *SMC queries* to check all desired properties (such as the probability of a failure) w.r.t. system being modeled.
- *Process* (i.e. gather, analyze, visualize and interpret) *data* produced on basis of the SMC queries from the dependability assessment viewpoint.

A. Remarks to Dependability Assessment

Before moving forward, let us present the principle behind dependability assessment on the STA/SMC basis. Then, let us compare the results of such an assessment to the results of an existing, well established assessment. Instead of being exhaustive, let us limit herein just to the principle/comparison that relates to the exponentially distributed X_{TTF} and the SPX model (Fig. 1a). For such a model, the analytical solution to the assessment problem exists (start of Sect. II), so it can be utilized for the validation purposes. Based on the STA instruments, the SPX can be modeled by an STA from Fig. 2. This can be done either using UPPAAL's native instruments (Fig. 2a) or using the instruments of our fault behavior framework (Fig. 2b) introduced in [16]. Comparing to the first one, the latter (our) approach is open to arbitrary distributions of probability, without a need to change the model. In our approach, the occurence of a fault is given by its parameterizable, potentially time-varying, fault behavior model able to signalize a fault via a dedicated channel (*fail[i]!*). Properties (such as the probability of a failure) of a network of STAs can be checked by the SMC engine. It may produce various data and/or functions such as PDF, CDF or mean w.r.t. the properties. A property may be checked by the so-called *query*.

Particularly (Fig. 2), the engine may be asked to evaluate the probability of entering (the state) *failure*. This can be expressed using a query of the probability estimation type. Such a query is in the form $Pr[bound](\phi)$ where *bound* defines how to bound, e.g. the number of, simulation steps (runs) and ϕ represents a property to be checked. Let us suppose that the probability is going to be examined for four, exponentially distributed, random variables X_{TTF} (Fig. 3) within 10^5, i.e. 1e+5, units of time. Then, the particular query would be $Pr[<= 100000](<> STA.failure)$ for each of the variables. The result of the query can be stored e.g. in the PDF, i.e. $f(t)$, form (Fig. 3a) or CDF, i.e. $F(t)$, form (Fig. 3b) and directly exported from UPPAAL to be processed later.

Apparently, $f(t)$, $F(t)$ of X_{TTF} suffice to assess further dependability attributes such as *MTTF* or *R(t)* by their definitions. Knowing $f(t)$ and $R(t)$, $h(t)$ may be constructed

Fig. 2. An idea to the STA representation of the SPX model (Fig. 1a)

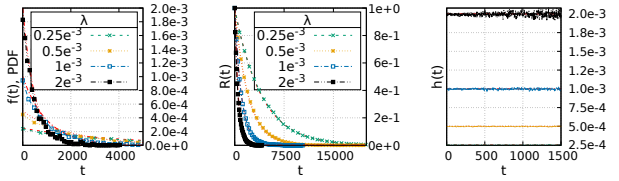

Fig. 3. Comparison of the analytical results to the results of the SMC query $Pr[<= 100000](<> STA.failure)$ for uncertainty (ε) set to 1‰

by its definition as well. For the results based on the above-mentioned query see Fig. 3, please. It can be seen there that the curve produced by the analytical solution (dashed red) practically overlaps with the curves produced by the SMC engine (green, orange, cyan and black).

B. Representative Case Studies

This section presents several case studies, main goal of which is to demonstrate the practical applicability of our approach to the dependability assessment problem. The demonstration relies on our STA-based variants of the models from Fig. 1 and our SMC-based dependability assessment (III-A). To make our models more understandable, let their form be unified in the following way (e.g., see Fig. 4). A model starts in the (green-colored) state *faulty0*, representing the correct operation of all components in a system; alike, any state representing a failure is colored in red and a state after reconfiguration is colored in yellow. A model declares its local variable (*ttf*) of the clock type to measure the time to failure using the invariant *ttf'*$== 0$.

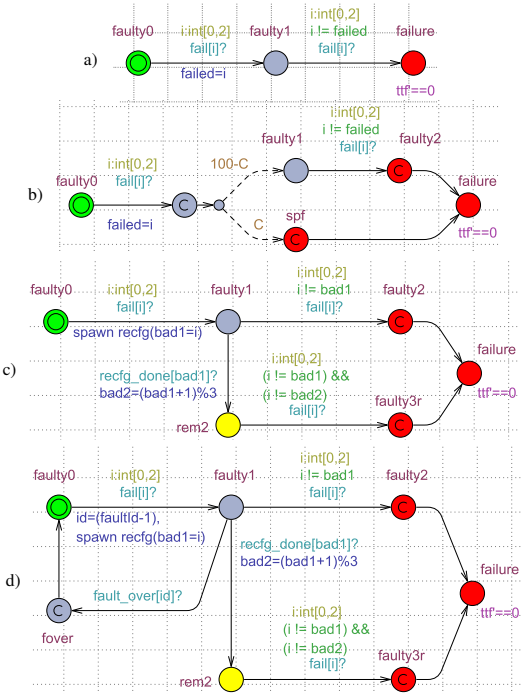

Fig. 4. STA variants of a) TMR_{NSF}, b) TMR_{1SF}, c) TTS_P, d) TTS_T

Let the illustration start for *TMR*$_{NSF}$ (Fig. 1b). The associated STA (Fig. 4a) starts in *faulty0* where it waits for

the reception of a signal via one of 3 channels (`fail[`i`]`, $i = 0, 1, 2$), each belonging to a replica in the TMR system. If one of the replicas fails then the corresponding value of i is stored in (the local variable) $failed$ to identify the replica and the STA transits to *faulty1*. It stays here until one of the remaining two replicas fails; then, it transits to *failure*. TMR_{1SF} (Fig. 4b), waits in *faulty0* until one of the replicas fails. With probability given by C [%], such a replica results into SPF (entering *spf*, then *failure*). Otherwise, with prob. given 100-C, it behaves as TMR_{NSF}. Fig. 4c, d represent the models of TTS_P, TTS_T from Fig. 1c, details to which follow. If a replica fails in *faulty0* then the reconfiguration process, based on isolation/removal of the faulty replica (identified by *bad1*), is initiated for the replica and the STA transits to *faulty1*. Here, it waits until the reconfiguration completes (the channel *recfg_done[bad1]* on the transition to *rem1*) or one of the non-faulty replicas fails (*faulty2*). The reconfiguration is driven by a separate STA, an instance of which can be dynamically i) introduced into the simulation process using the *spawn* keyword resp. ii) removed from the simulation process using *exit()*. In Fig. 4c, d, a fault-free module (*bad2*) have to be removed along with the faulty one (*bad1*) while transiting from *faulty1* to *rem2*; the value of *bad2* is selected as the next one after *bad1* based on the modulo ($\%$) operation. Comparing to Fig. 4c, Fig. 4d has extra feedback transitions from *faulty1*, having the three successors: *fover*, *rem2* and *faulty2*. If the (transient) fault disappears then it transits to *fover*, followed by *faulty0*. Else, the process of isolating the faulty component and removing a non-faulty one may complete before the fault disappears; then, the STA enters *rem2*. Else, one of the two non-faulty modules may fail before entering *fover* or *rem2* and the system fails (*faulty2* followed by *failure*).

IV. Conclusion

In this paper, a novel, simulation-based approach to the construction of reliability models and their dependability assessment by the STA/SMC means have been introduced, summary of which follows in the next. The novelty of the approach can be seen in its i) openness to modifications – it is highly extendable by further concepts, some of which are mentioned below, ii) intuitiveness – it has been shown using a series of case studies, iii) expressive power – means of (a network of) STAs are general enough to cope with arbitrary, timed stochastic behaviors over continuous time, dynamically manageable objects within the simulation process etc., iv) efficiency and accuracy – properties of the SMC process are controllable by a set of parameters such as ε. Our further research plans relate to parameterizable models of random variables with the bathtub-shaped hazard rate functions, repairable systems with a special attention paid to shared load and/or repair facilities, multiple failure modes, and assessment of maintainability and availability by the STA/SMC means.

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" and 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] I. Koren and C. M. Krishna, *Fault-Tolerant Systems*, 1st ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.

[4] R. W. Butler and S. C. Johnson, "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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems," *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 363–377, Sep 1992. DOI 10.1109/24.159800.

[10] 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.

[11] 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.

[12] G. Behrmann, A. David, and K. Larsen, "A Tutorial on UPPAAL," in *Formal Methods for the Design of Real-Time Systems*, ser. Lecture Notes in Computer Science, M. Bernardo and F. Corradini, Eds. Springer Berlin Heidelberg, 2004, vol. 3185, pp. 200–236, DOI 10.1007/978-3-540-30080-9_7.

[13] 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.

[14] A. David, K. G. Larsen, A. Legay, M. Mikucionis, D. B. Poulsen, J. van Vliet, and Z. Wang, "Stochastic Semantics and Statistical Model Checking for Networks of Priced Timed Automata," *CoRR*, vol. abs/1106.3961, 2011. [Online]. Available: http://arxiv.org/abs/1106.3961

[15] A. Boudjadar, J. H. Kim, A. David, K. G. L. M. Mikucionis, U. Nyman, A. Skou, I. Lee, and L. T. X. Phan, "Flexible Framework for Statistical Schedulability Analysis of Probabilistic Sporadic Tasks," in *Proceedings of the 2015 IEEE 18th International Symposium on Real-Time Distributed Computing*, ser. ISORC '15. Washington, DC, USA: IEEE Computer Society, 2015, pp. 74–83, DOI 10.1109/ISORC.2015.21.

[16] J. Strnadel, *On Creation and Analysis of Reliability Models by Means of Stochastic Timed Automata and Statistical Model Checking: Principle*. In: Proceedings of 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques (ISoLA), Part I. Cham: Springer International Publishing, 2016, pp. 166–181. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-47166-2_11