16th Industrial Simulation Conference (ISC 2018), Ponta Delgada, Portugal, June 2018 (Tutorial), pp. 1-6.

RELIABILITY MODELLING AND SIMULATION OF COMPLEX DYNAMIC DISCRETE-EVENT SYSTEMS

Armin Zimmermann
Technische Universität Ilmenau
Computer Science and Automation Department
Systems and Software Engineering Group
Helmholtzplatz 5, D-98693 Ilmenau, Germany
Email: armin.zimmermann@tu-ilmenau.de

KEYWORDS

Reliability, modelling, simulation, rare-event simulation, Markov chains, stochastic Petri nets, software tools

ABSTRACT

This tutorial covers motivation, use, and advantages of stochastic Petri nets as a tool for reliability evaluation of complex systems. Rare-event simulation techniques are demonstrated, which are applicable to a wide class of reliability problems. While this approach is known in the academic world, it has not yet been adopted much in industrial applications despite its apparent benefits. Additional triggers for this tutorial are advances in rare-event simulation for this model class as well as the recent standard IEC62551 for dependability evaluation with Petri nets. New results in performability evaluation using an integration of simulation and numerical analysis are presented. Example case studies and tool support are demonstrated.

INTRODUCTION AND MOTIVATION

Reliability is an important non-functional requirement of many man-made systems, especially when failures may lead to catastrophic events. When such systems are too complex to be understood and designed by one person, the resulting effect of local design decisions on overall system properties are not obvious. Mathematical models can help to describe such systems and to compute their reliability [29, 2, 15, 23, 20] with the help of appropriate software tools.

Unavoidable faults may be masked or tolerated by static or dynamic redundancy measures, all at a considerably increasing cost. The main task is to design a system such that its reliability and safety requirements are achieved with the least amount of resources. Classic models and tools for static analysis are not able to cover systems in which the complex behaviour influences failures, or if dynamic reconfigurations are applied (possibly because of a better resource / reliability trade-off).

Depending on the complexity of the system behaviour and the corresponding size of the state space, Markov chains and stochastic Petri nets are applied to reliability problems [29, 18]. They are attractive models as long as the underlying assumption of a Markov behaviour is realistic (Phase-type distributions can emulate others up to a certain accuracy, but this is paid for with an even larger state space). Petri nets have been adopted as a suggested tool for reliability engineering of complex systems in an international standard recently [5].

However, non-Markovian delay distributions (necessary, for instance, in the case of deterministic deadlines or maintenance cycles) are characteristic of technical systems. Stochastic Petri net classes allowing them exist, and they can be used for reliability evaluation [19]. However, their numerical analysis is restricted, only allowing the application to special cases [8]. An alternative evaluation technique is simulation [6], but the problem here is that the computational effort to generate enough failure states to achieve statistical confidence in the estimated results is usually intractable [11].

This problem is well-known as *rare-event simulation* [12], and there are two main approaches used: *importance sampling* [10] and *splitting* [9]. They have the common goal to increase the frequency of the rare event in order to gain more significant samples out of the same number of generated events. For methods that can be automated and implemented in a software tool for industrial applications, the latter technique has the advantage of requiring less insight into the model details, and with the RESTART algorithm [33] there are efficient and robust implementations available [7, 31, 36, 37].

The tutorial will present motivation, introduction of background material, sample Petri net models of reliability issues, as well as ideas and algorithms towards simulation speedup for reliability evaluation. This will be done along the points mentioned so far in the introduction; some more details of planned contents are given in the subsequent sections. To avoid a purely theoretical lecture, the tutorial will be accompanied by practical application examples (c.f. Section) demonstrated with the software tool TimeNET [37, 38].

Finally, recent results towards automated splitting simulations for stochastic Petri nets [25, 45] as well as

advancements in integrating simulation with numerical analysis techniques [42] are pointed out as first results of future research directions in this area.

INTRODUCTORY MATERIAL

Depending on the background of the audience and available time, the tutorial will start with a brief coverage of necessary background. Reliability terms and measures are introduced as the application domain of the later modelling problems. Static and dynamic redundancy setups and basic assumptions about the behaviour of single components are discussed [29, 15, 23].
Classic models in the area of reliability engineering will be touched briefly to explain what can be done with them and where they fail, as a motivation of using stochastic Petri nets for reliability design depending on complex system behaviour. Fault trees and reliability block diagrams are common examples. Industrial acceptance issues in the conservative domain of safety-critical systems is mentioned; for instance, even for the space shuttle design, no dynamic model was used [24].
Basic dynamic models comprise stochastic automata and Markov chains, which are useful for dynamic system reliability analysis as long as the state space is still manageable and the Markov assumption can be accepted [19, 17]. Their application to reliability design is suggested by an industry standard [4]. Queueing network models can be applied to reliability evaluations as well; their advantages and drawbacks compared to Petri nets in reliability will be pointed out.

RELIABILITY EVALUATION WITH STOCHASTIC PETRI NETS

For listeners without background knowledge in stochastic Petri nets, a short intro will be given, using examples rather than formal definitions to underline the tutorial style of the presentation. As they allow modular specification of systems, basic building blocks for reliability setups will be presented. Suggestions from the recent IEC standard [5] are covered.
For the performance and reliability evaluation of such models, the standard methods numerical analysis and simulation can be applied. The advantages and shortcomings of numerical analysis [16, 8] will be given as well as their effect on reliability analysis [19].
As a way around these problems, rare-event simulation techniques are introduced to the audience covering problem, solution strategies and algorithms. The RESTART method [33] will be covered in more detail because of its broad applicability. Its open problems — manual specification of importance function and levels as well as restrictions in some reliability problems — will be shown. Recent developments towards improvements in this area are pointed out, and open research questions are mentioned [39]. Specifically, recent advances towards an integration of simulation and numerical analysis techniques [42] are covered, which have a high potential for future innovative solutions in efficient reliability engineering.

Software Tool Support

Complex system modelling and evaluation would not be practical without the support of software tools. The tutorial will include demonstrations based on the software tool TimeNET [38], which supports graphical modelling and performability evaluation of several Petri net classes [37]. Among its main characteristics are the evaluation of models with non-exponentially distributed firing delays, the ability to model and evaluate complex coloured stochastic Petri nets [35], and efficient rare-event simulation methods for stochastic Petri nets.

Severl of the techniques covered by the tutorial have been implemented in TimeNET, and the tool will be used to show their application and necessary configuration parameters with application examples. It also supports rare-event simulation of high-level Petri net models for complex systems; a sample screen shot is shown in Figure 1. The tool can be downloaded by the tutorial participants from its home page at `http://timenet.tu-ilmenau.de`.

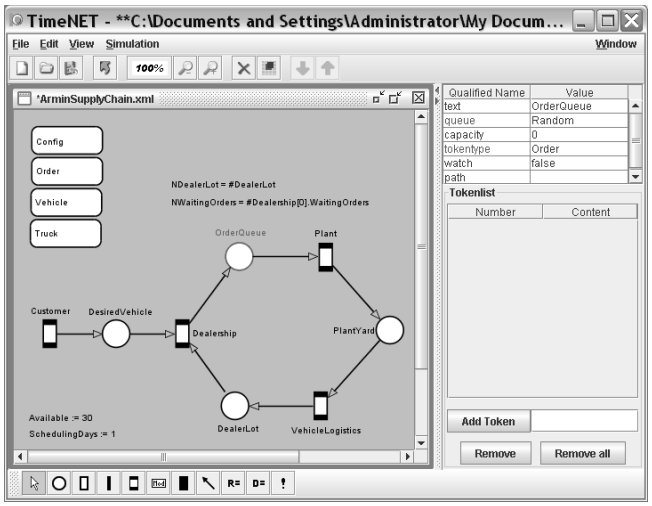

Figure 1: Sample screen shot of TimeNET

The tutorial will also point out other available software tools applicable to the reliability evaluation with stochastic Petri nets, such as SHARPE [26, 13], OpenSESAME [34], GreatSPN [1], Möbius [3], and SIMTHESys [14]. Other implementations of the RESTART technique include SPNP [31] for stochastic Petri nets and ASTRO [32]. Importance sampling techniques are e.g. included in UltraSAN [22, 21] for stochastic activity networks.

Example Case Studies

Besides small explanatory examples, which are used during the tutorial to explain models and methodology, some examples of complex systems from different application domains will be presented. We will select examples from literature and previous projects to give a motivating overview and show the benefits of the shown methodology:

Hybrid electric vehicles are a growing field of application for model-based systems engineering. Among other issues, battery management is important to balance battery life span, energy efficiency, and road safety. An example application scenario has been introduced in [40], Figure 2 shows the proposed model.

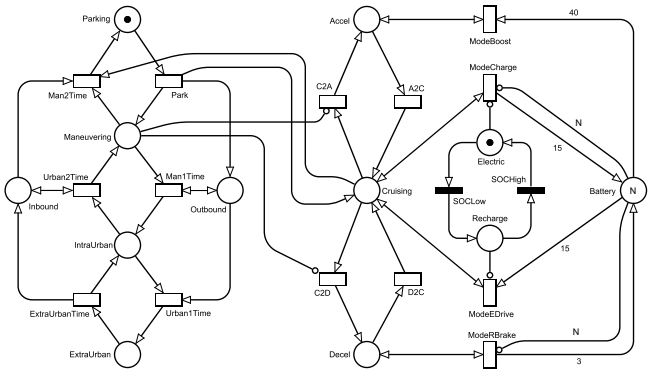

Figure 2: Hybrid electric vehicle model of driver behavior and battery management

Train control is obviously a highly safety-relevant application, where model-based engineering can help to achieve the necessary reliability with efficient resources. The currently introduced European Train Control System ETCS is a major shift in train control. The dependency of real-time deadline misses and failure-prone wireless communication in a highly safety-relevant environment can be evaluated based on stochastic Petri nets [30, 41]. Figure 3 presents a sample model from this example.

Just-in-time delivery and fine-grained production planning allows to save warehouse costs. However, it makes production dependable on a reliable and timely delivery of parts. Logistics has become more important to avoid costly plant downtimes. Reliable supply chain operations can be designed based on coloured stochastic Petri nets [44, 36].

Other possible application areas to present examples include avionic communication networks [27, 43, 46] and distributed fault-tolerant cloud computing architectures [28]. A stochastic Petri net model for reliability evaluation of the latter is depicted in Figure 4.

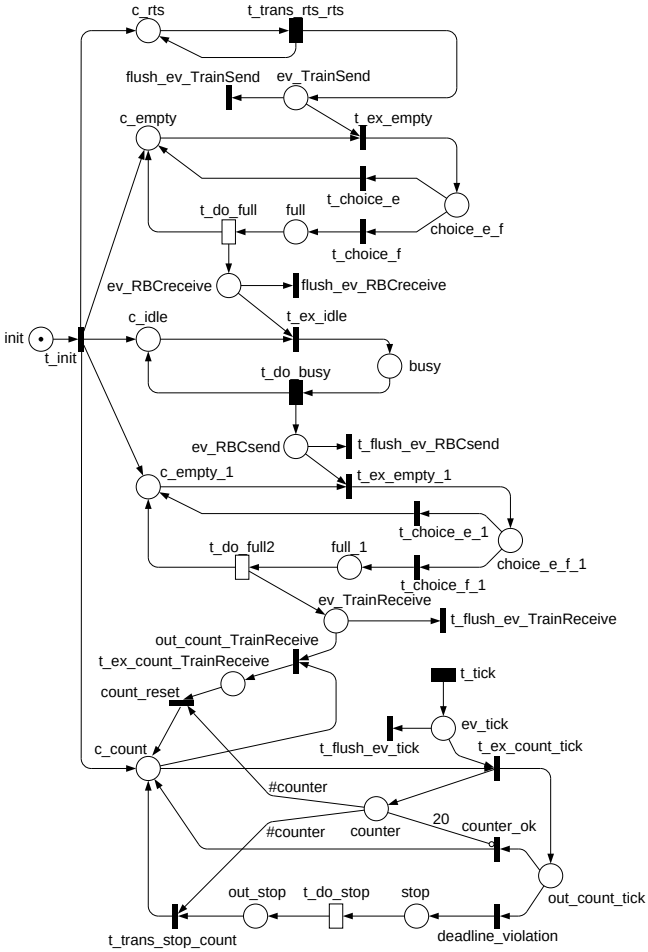

Figure 3: Stochastic Petri net of ETCS communication and control message timeouts

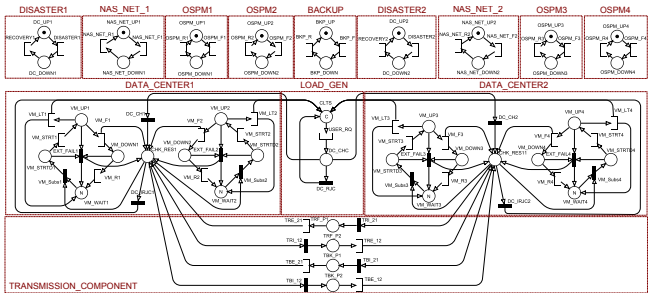

Figure 4: Reliability model of a cloud architecture

CONCLUSION

The tutorial will offer participants an overview of stochastic Petri nets as a valuable tool for modelling and evaluating reliability measures of complex systems, comparing them with classic reliability models. It highlights recent developments in rare-event simulation as well as the new IEC standard on reliability evaluation with Petri nets. The presentation will cover models and methods to understand advantages and restrictions; an-

other central point are application examples from actual projects and a tool demonstration.

ACKNOWLEDGMENTS

The author would like to thank all colleagues and former students who contributed to the software tool TimeNET, and the colleagues with whom many of the projects referenced in this tutorial have been carried out.

REFERENCES

[1] S. Baarir, M. Beccuti, D. Cerotti, M. De Pierro, S. Donatelli, and G. Franceschinis. The GreatSPN tool: recent enhancements. *SIGMETRICS Perform. Eval. Rev.*, 36(4):4–9, March 2009.

[2] W. R. Blischke and D. N. Prabhakar Murthy. *Reliability: Modeling, Prediction, and Optimization*. Wiley Series in Probability and Statistics. Wiley, 2000.

[3] T. Courtney, S. Gaonkar, K. Keefe, E. Rozier, and W. Sanders. Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models. In *IEEE/IFIP Int. Conf. on Dependable Systems Networks*, pages 353–358, 2009.

[4] Application of Markov techniques. IEC 61165:2006 Ed. 2.0, May 2006.

[5] Analysis techniques for dependability — Petri net techniques. IEC 62551:2012, Sept. 2013.

[6] J. Faulin, A. A. Juan, S. Martorell, and J.-E. Ramírez-Márquez, editors. *Simulation methods for reliability and availability of complex systems*. Springer, 2010.

[7] M. J. Garvels and D. P. Kroese. A comparison of RESTART implementations. In *Proc. 1998 Winter Simulation Conference*, 1998.

[8] R. German. *Performance Analysis of Communication Systems, Modeling with Non-Markovian Stochastic Petri Nets*. John Wiley and Sons, 2000.

[9] P. Glasserman, P. Heidelberger, P. Shahabuddin, and T. Zajic. Multilevel splitting for estimating rare event probabilities. *Operations Research*, 47:585–600, 1999.

[10] P. W. Glynn and D. L. Iglehart. Importance sampling for stochastic simulations. *Management Science*, 35(11):1367–1392, Nov. 1989.

[11] P. E. Heegaard. Speedup simulation techniques. In *Proc. Workshop on Rare Event Simulation*, pages 28–29, Aachen, Germany, 1997.

[12] P. Heidelberger. Fast simulation of rare events in queueing and reliability models. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 5(1):43–85, 1995.

[13] C. Hirel, R. A. Sahner, X. Zang, and K. S. Trivedi. Reliability and performability modeling using SHARPE 2000. In B. R. Haverkort, H. C. Bohnenkamp, and C. U. Smith, editors, *11th Int. Conf. Computer Performance Evaluation: Modelling Techniques and Tools (TOOLS 2000)*, volume 1786 of *Lecture Notes in Computer Science*, pages 345–349, Schaumburg, IL, USA, 2000. Springer.

[14] M. Iacono, E. Barbierato, and M. Gribaudo. The SIMTHESys multiformalism modeling framework. *Computers & Mathematics with Applications*, 64(12):3828 – 3839, 2012. Theory and Practice of Stochastic Modeling.

[15] K. Kolowrocki and J. Soszynska-Budny. *Reliability and Safety of Complex Technical Systems and Processes: Modeling - Identification - Prediction - Optimization*. Springer Series in Reliability Engineering. Springer, 2013.

[16] C. Lindemann. *Performance Modelling with Deterministic and Stochastic Petri Nets*. Wiley, 1998.

[17] C. Lindemann, M. Malhotra, and K. Trivedi. Numerical methods for reliability evaluation of Markov closed fault-tolerant systems. *IEEE Trans. on Reliability*, 44(4):694–704, 1995.

[18] M. Malhotra and K. Trivedi. Dependability modeling using Petri-net based models. *IEEE Trans. on Reliability*, 44(3):428–440, 1995.

[19] I. Mura, A. Bondavalli, X. Zang, and K. Trivedi. Dependability modeling and evaluation of phased mission systems: a DSPN approach. In *Dependable Computing for Critical Applications 7, 1999*, pages 319–337, 1999.

[20] D. Nicol, W. Sanders, and K. Trivedi. Model-based evaluation: from dependability to security. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):48–65, 2004.

[21] W. Obal and W. Sanders. Importance sampling simulation in UltraSAN. *Simulation*, 62(2):98–111, 1994.

[22] W. D. Obal and W. H. Sanders. An environment for importance sampling based on stochastic activity networks. In *Proc. 13th Symp. on Reliable Distributed Systems*, pages 64–73, Dana Point, CA, October 1994.

[23] P. P. O'Connor and A. Kleyner. *Practical Reliability Engineering*. Wiley, 2012.

[24] M. E. Paté-Cornell and R. L. Dillon. Probabilistic risk analysis for the NASA space shuttle: a brief history and current work. *Reliability Engineering & System Safety*, 74(3):345–352, 2001.

[25] D. Reijsbergen, P.-T. Boer, W. Scheinhardt, and B. Haverkort. Automated rare event simulation for stochastic Petri nets. In K. Joshi, M. Siegle, M. Stoelinga, and P. R. D'Argenio, editors, *Quantitative Evaluation of Systems*, volume 8054 of *Lecture Notes in Computer Science*, pages 372–388. Springer Berlin Heidelberg, 2013.

[26] R. A. Sahner, K. S. Trivedi, and A. Puliafito. *Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package*. Kluwer Academic Publishers, 1995.

[27] K. Schulze, M. Caldeira, J. a. F. Baptista, and A. Zimmermann. Model-based design and evaluation of fault-tolerant fibre-optical networks for avionics. In *Proc. 11th Int. Probabilistic Safety Assessment & Management Conference / European Safety & Reliability Conference (PSAM11 & ESREL 2012)*, pages 1–10, Helsinki, Finland, June 2012.

[28] B. Silva, P. Maciel, E. Tavares, and A. Zimmermann. Dependability models for designing disaster tolerant cloud computing systems. In *Proc. 3rd Int. Workshop on Dependability of Clouds, Data Centers and Virtual Machine Technology (DCDV-2013) at the 43rd IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN 2013)*, pages 1–6, Budapest, Hungary, June 2013.

[29] K. S. Trivedi. *Probability and Statistics with Reliability, Queuing and Computer Science Applications*. Wiley, 2nd edition, 2002.

[30] J. Trowitzsch and A. Zimmermann. Using UML state machines and Petri nets for the quantitative investigation of ETCS. In *Proc. Int. Conf. on Performance Evaluation Methodologies and Tools (VALUETOOLS 2006)*, Pisa, Italy, 2006.

[31] B. Tuffin and K. S. Trivedi. Implementation of importance splitting techniques in stochastic Petri net package. In B. R. Haverkort, H. C. Bohnenkamp, and C. U. Smith, editors, *Computer Performance Evaluation, Modelling Techniques and Tools — 11th Int. Conf., TOOLS 2000*, volume 1786 of *Lecture Notes in Computer Science*, pages 216–229, Schaumburg, IL, USA, 2000. Springer Verlag.

[32] M. Villén-Altamirano and J. Villén-Altamirano. RESTART: A straightforward method for fast simulation of rare events. In *Proc. Winter Simulation Conference*, pages 282–289, 1994.

[33] M. Villén-Altamirano and J. Villén-Altamirano. Optimality and robustness of RESTART simulation. In *Proc. 4th Workshop on Rare Event Simulation and Related Combinatorial Optimisation Problems*, Madrid, Spain, Apr. 2002.

[34] M. Walter, M. Siegle, and A. Bode. OpenSESAME — the simple but extensive, structured availability modeling environment. *Reliability Engineering and System Safety*, 93(6):857–873, 2008.

[35] A. Zimmermann. *Stochastic Discrete Event Systems*. Springer, Berlin Heidelberg New York, 2007.

[36] A. Zimmermann. RESTART simulation of colored stochastic Petri nets. In *Proc. 7th Int. Workshop on Rare Event Simulation (RESIM 2008)*, pages 143–152, Rennes, France, Sept. 2008.

[37] A. Zimmermann. Dependability evaluation of complex systems with TimeNET. In *Proc. Int. Workshop on Dynamic Aspects in Dependability Models for Fault-Tolerant Systems (DYADEM-FTS 2010)*, Valencia, Spain, Apr. 2010.

[38] A. Zimmermann. Modelling and performance evaluation with TimeNET 4.4. In *Quantitative Evaluation of Systems - 14th Int. Conf., QEST 2017*, pages 300–303, Berlin, Germany, sep 2017.

[39] A. Zimmermann, A. Canabal Lavista, and R. J. Rodríguez. Some notes on rare-event simulation challenges. In *Proc. 11th Int. Conf. on Performance Evaluation Methodologies and Tools (Valuetools 2017)*, Venice, Italy, dec 2017.

[40] A. Zimmermann, T. Dietrich, P. Maciel, and A. Hildebrandt. Model-based dynamic reliability engineering for hybrid electric vehicle design. In *IEEE Int. Systems Conference (SysCon 2017)*, Montreal, Canada, Apr. 2017.

[41] A. Zimmermann and G. Hommel. Towards modeling and evaluation of ETCS real-time communication and operation. *Journal of Systems and Software*, 77:47–54, 2005.

[42] A. Zimmermann, T. Hotz, and A. Canabal Lavista. A hybrid multi-trajectory simulation algorithm for the performance evaluation of stochastic Petri nets. In N. Bertrand and L. Bortolussi, editors, *Quantitative Evaluation of Systems (QEST 2017)*, volume 10503 of *Lecture Notes in Computer Science*, pages 107–122, Berlin, Germany, Sept. 2017. Springer.

[43] A. Zimmermann, S. Jäger, and F. Geyer. Towards reliability evaluation of AFDX avionic communication systems with rare-event simulation. In *Proc. Probabilistic Safety Assessment & Management Conference 2014 (PSAM 12)*, pages 1–12, Honolulu, Hawaii, USA, June 2014.

[44] A. Zimmermann, M. Knoke, S.-T. Yee, and J. D. Tew. Model-based performance engineering of General Motors' vehicle supply chain. In *IEEE Int. Conf. on Systems, Man and Cybernetics (SMC 2007)*, pages 1415–1420, Montreal, Canada, Oct. 2007.

[45] A. Zimmermann and P. Maciel. Importance function derivation for RESTART simulations of Petri nets. In *9th Int. Workshop on Rare Event Simulation (RESIM 2012)*, pages 8–15, Trondheim, Norway, June 2012.

[46] A. Zimmermann and P. Maciel. Dependability evaluation of AFDX real-time avionic communication networks. In *Proc. 22nd IEEE Pacific Rim Int. Symposium on Dependable Computing (PRDC 2017)*, Christchurch, New Zealand, Jan. 2017.