22nd IEEE Pacific Rim Int. Symposium on Dependable Computing (PRDC 2017), Christchurch, New Zealand, January 22-25, 2017.

Dependability Evaluation of AFDX Real-Time Avionic Communication Networks

Armin Zimmermann
Systems and Software Eng., TU Ilmenau
Helmholtzplatz 5, 98684 Ilmenau, Germany
Email: armin.zimmermann@tu-ilmenau.de

Paulo Maciel
Modeling of Distributed and Concurrent Systems
Federal University of Pernambuco, Recife, Brazil
Email: prmm@cin.ufpe.br

***Abstract*—This short paper presents ongoing work towards the model-based evaluation of AFDX avionic networks. The required reliability of this type of network depends on timely packet delivery, which must be analyzed during design. We extend previous work by colored stochastic Petri net models of AFDX modules, which reduces several restrictions of the earlier Petri net models. Rare-event simulation for such models allows to efficiently compute small probabilities of long (potentially safety-critical) transmission delays. This has been implemented in the software tool TimeNET previously, and the simulation results validate the proposed model.**

***Index Terms*—AFDX, Avionic Communication Network Dependability, Colored Stochastic Petri Net, Rare-Event Simulation**

I. Introduction

Distributed embedded systems are increasingly important for the monitoring, control and operation of complex technical systems. Their reliability is crucial if they are part of a safety-critical system or function (such as in automotive, train control, and avionics). Model-based systems engineering is a necessary help in the design of such systems to understand the mutual dependencies of design parameters and local decisions. There is a large body of work including models, analysis techniques and software tools supporting model-based reliability design [1].

This paper aims at a reliability evaluation of AFDX (avionics full-duplex Ethernet [2]), a network architecture for modern aircraft that has been developed for and is used now in the Airbus A380. One aspect of its reliable function are guaranteed packet delivery times, to allow real-time control tasks on the higher software application level. There are several methods for worst-case end-to-end delay analysis (network calculus, simulation, and model checking [3], [4], [5]), all with their individual advantages and drawbacks. However, an upcoming question for network and buffer sizing are probabilistic end-to-end measures such as quantiles of the distribution [6]. For instance, the conservative settings of guaranteed bounds may lead to system designs in which observed delays are only about 5% of the computed bound.

While classic models (fault trees, reliability block diagrams etc.) are well understood for static reliability questions, reliability of complex dynamic systems is not supported equally well. In avionic system design, for instance, fly-by-wire systems, flight control and management, maintenance processes, as well as modern communication architectures are examples in which dynamic reliability models are necessary. Stochastic automata, Markov chains, and Petri nets are possible models. Petri nets have been suggested for reliability engineering of complex systems including concurrency, stochastic aspects, and time in an international standard recently [7]. As non-memoryless distributions (such as deterministic clocks or deadlines) are typical for embedded systems, analysis methods based on the Markov assumption are not well suited.

A natural alternative is a stochastic discrete-event simulation, 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. This problem is well-known as rare-event simulation, and there are efficient speed-up methods including *importance sampling* and *splitting*. A variant is the RESTART algorithm [8], which has been shown to work robustly and efficiently for many applications and which has been adapted and implemented for variants of stochastic Petri nets (e.g., [9]).

This paper extends earlier work that presented (uncolored) stochastic Petri net models of the main AFDX building blocks [10], and showed that small probabilities of rare higher levels in packet buffers (which are the main influence on delay jitter) can be simulated efficiently with rare-event simulation techniques. However, because of the use of simple Petri nets, some details of AFDX networks such as multicast traffic and individual packet lengths had to be ignored, restricting the applications to rather simplistic setups.

This paper proposes how colored stochastic Petri nets can be used to capture such additional information for a more detailed system description, leading to more realistic results while retaining the same simple mapping from network structure to Petri net model setup. The paper introduces colored Petri net models of AFDX end systems, links, and switches, and extends the previous work by allowing crossing / overlapping network link architectures, multicast traffic, as well as transmission delays based on individual packet lengths.

Another main advantage is an extension of the possible performance results: our previous proposal mainly allowed to analyze buffer levels and mean end-to-end packet transmission delays [10] (although there is a workaround for deadline violations), while the model introduced here also supports the computation of quantiles and empirical distributions of the packet delay.

II. Colored Petri Net Models for AFDX

An AFDX network contains source and destination *end systems*, *switches* that collect and forward packets and are thus responsible for routing, traffic policing and multicast packet duplication, and *links* between the elements. Sources may send data either in a periodic or sporadic fashion, however restricted in their bandwidth to avoid overload. Links are dedicated one-to-one Ethernet connections without packet collisions. *Virtual link*s (VL) form logical connections from source to end systems and similar to rate-constrained network tunnels.

The main difference of colored over normal Petri nets is that tokens are individual entities having attributes with values, similar to a type in a programming language. Details of this and the consequences for transition definition and net semantics can be found in [11]. One user-defined token type for messages (packets) is needed in our AFDX proposal, where the virtual link (VL) identifier as well as time stamps for message creation and sending are kept (the latter for evaluation purposes only).

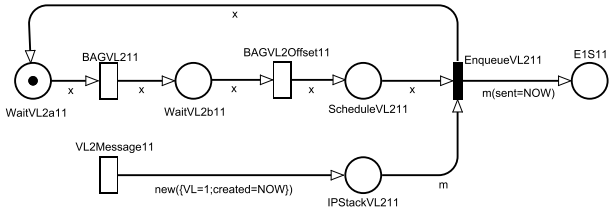

Fig. 1. AFDX source end-system with sporadic traffic and packet regulation

The model structure of these AFDX building blocks is structurally very similar to the ones proposed earlier [10]. Figure 1 shows a source end-system generating sporadic packets (transition `VL2Message..` fires) and sending them to the output port under a bandwidth-restricted policy which is governed by the upper model part. The left transition fires deterministically after the bandwidth allocation gap (BAG) time, the one in the middle introduces some stochastic jitter to model the unsynchronized local clocks in the system which will lead to every possible interleaving of packet generation between end systems.

III. An AFDX Application Setup

Figure 2 shows an application example of an AFDX network architecture with a more complex structure than what could have been modeled with our earlier method. There are several virtual links (including multicast destinations) which cross and influence each other.

Its evaluation is done with the use of our software tool TimeNET [12], which allows the efficient rare-event simulation of colored stochastic Petri nets. Numerical results show the effect of such issues on jitter and probability distribution of packet arrival delays. Our first validating simulations show the expected behavior, with 81% of all packets arriving at the minimum possible delay of $282\mu s$ (i.e., without any blocking in the network), while the rest has a maximum delay of $369\mu s$.

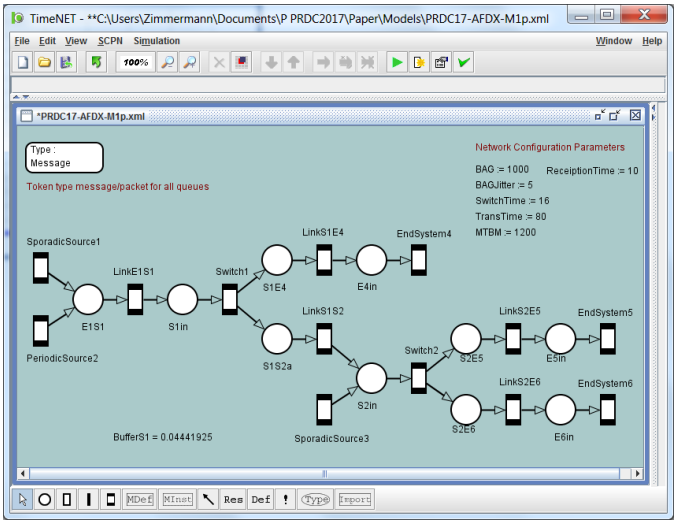

Fig. 2. Petri net model of an example AFDX setup in TimeNET

IV. Conclusion

The paper presented *colored* stochastic Petri net patterns for the systematic modeling of AFDX avionic networks, allowing additional details including multicast and overlapping traffic routes, per-link individual packet lengths, as well as more complex performance measures w.r.t. previous work.

References

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

[2] "Arinc 664, aircraft data network, part 7: Avionics full duplex switched Ethernet (AFDX) network," Jun. 2005.

[3] J.-L. Scharbarg and C. Fraboul, "Methods and tools for the temporal analysis of avionic networks," in *New Trends in Technologies: Control, Management, Computational Intelligence and Network Systems*, M. J. Er, Ed. Sciyo, 2010.

[4] H. Charara, J.-L. Scharbarg, J. Ermont, and C. Fraboul, "Methods for bounding end-to-end delays on an AFDX network," in *Proc. 18th Euromicro Conf. on Real-Time Systems (ECRTS06)*, 2006.

[5] H. Bauer, J.-L. Scharbarg, and C. Fraboul, "Improving the worst-case delay analysis of an AFDX network using an optimized trajectory approach," *IEEE Trans. Industrial Informatics*, vol. 6, no. 4, pp. 521–533, Nov. 2010.

[6] C. Fraboul and J.-L. Scharbarg, "Trends in avionics switched Ethernet networks," in *Proc. 1st Workshop on Real-Time Ethernet (RATE) at the IEEE Real-Time Systems Symposium*, Vancouver, Canada, 2013.

[7] *Analysis techniques for dependability — Petri net techniques*, IEC 62551:2012, IEC Norm DIN EN 00 338, Sep. 2013.

[8] M. Villén-Altamirano and J. Villén-Altamirano, "Analysis of RESTART simulation: Theoretical basis and sensitivity study," *European Transactions on Telecommunications*, vol. 13, no. 4, pp. 373–385, 2002.

[9] A. Zimmermann, D. Reijsbergen, A. Wichmann, and A. Canabal Lavista, "Numerical results for the automated rare event simulation of stochastic Petri nets," in *11th Int. Workshop on Rare Event Simulation (RESIM 2016)*, Eindhoven, Netherlands, 2016, pp. 1–10.

[10] 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)*, Honolulu, Hawaii, USA, Jun. 2014, p. 12.

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

[12] ——, "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.