

# Modelling and Analysing of Stochastic Failures in Complex Component-Based Systems

LARS GRUNSKÉ

*University of Queensland, School of ITEE (Boeing Postdoctoral Research Fellow), 4072 Brisbane (St.Lucia), Australia [grunsk@itee.uq.edu.au ]*

Complex computer-based systems used in mission- or safety-critical domains, including defence applications, air traffic control, railway signalling and medical applications play an important role in our modern society. One important task in the development of these systems is the construction of safe cases and safety models that are used to determine quantitative measures for failure or hazard probabilities. These safety models should be intuitive, compositional and have the expressive power to model both software and hardware behaviour.

In industrial projects, currently event-based models such as Fault Trees or state-based models such as Markov-chains are used. Each of these models has its limitations [3]. A model that combines elements from Fault Trees and Markov Models could improve expressive power of safety cases. In [2], we (Bernhard Kaiser, Yiannis Papadopoulos, and Lars Grunské) have introduced State Event Fault Trees (SEFTs), a new model for safety analysis with a combined state-event semantic. SEFTs are a hierarchical and visual model that integrates elements from stochastic state-based models (Markov-chains) with FTs. The quantitative probabilistic analysis is performed by translation of the safety models into Deterministic and Stochastic Petri Nets (DSPNs) [1], a class of Petri Nets for which analysis tools exist (e.g. the tool TimeNET [4]).

In the proposed talk I want to explore the problems and benefits of State Event Fault Trees in the construction of safety cases for complex computer-based systems. Furthermore, I will address the usefulness of strongly encapsulated and hierarchical evaluation models, such as SEFT, to analyse the stochastic behaviour of complex component-based systems.

1. CIARDO, G., LINDEMANN, C. 1993. Analysis of deterministic and stochastic Petri nets. In Proc. of the Fifth Int. Workshop on Petri Nets and Performance Models (PNPM93), Toulouse, France, Oct.
2. GRUNSKÉ L., KAISER B., PAPADOPOULOS Y. 2005. Model-Driven Safety Evaluation with State-Event-Based Component Failure Annotations, accepted (10.02.2005) *Eighth International SIGSOFT Symposium on Component-based Software Engineering (CBSE 2005) Co-Located with ICSE-2005*, St Luis, Missouri, May 14-15
3. VILLEMEUR A. 2000. *Reliability, Availability, Maintainability, and Safety Assessment*, John Wiley and Sons, ISBN: 0-47193-048-2 (2000).
4. ZIMMERMANN, A., GERMAN, R., FREIHEIT, J., HOMMEL, G. 1999. TimeNET 3.0 Tool Description. *Int. Conf. on Petri Nets and Performance Models (PNPM'99)*, Zaragoza, Spain