HALF-DAY TUTORIAL: TOOL SUPPORTED MODEL-BASED SAFETY ANALYSIS

TOPICS

Model Based Safety Analysis, Safety-Critical Systems, Failure Modeling, Quantitative Analysis, Qualitative Analysis, Reliability, Dependability, Optimization

OVERVIEW

The complexity of modern systems and the risk failure of these systems have resulted in a great need for reliable safety assessments. Therefore a big variety of different safety analysis methods have been developed over the last years. Some of the most well-known are fault tree analysis (FTA) and failure modes and effects analysis (FMEA). Both techniques exist in a broad variety of notions and domain-specific extensions. Common to all the traditional safety analysis methods is, that they are mostly informal and rely highly on skill and experience of the safety engineer. At the same time, the steadily growing complexity of safety critical systems is making it harder and harder for humans to foresee all possible effects.

As a consequence a lot of work has been put into developing model-based safety analysis methods during the last one or two decades. The big advantage is that the results of a model-based method do not solely rely on the skill of the engineer and his understanding of the system, but rather on a (formal) model of the system. The rigorousity of formal methods allow for a very high level of quality of a safety analysis method, which cannot be reached with traditional (only informal) methods alone. Big advances in computing power and the effectiveness of model checkers allow applying such methods to medium-sized systems almost automatically.

In this tutorial, we will present how qualitative as well as quantitative safety properties may be derived in a model based way. The tutorial will cover the whole process of model-based analysis. This includes systematic modeling of failure modes, automatic derivation of minimal cut sets, model-based computation of hazard probabilities as well as optimization of safety goals on system level. The tutorial will start by explaining the basic underlying theory briefly and then show an interactive application to a small case study.

For the modeling part we will present an Eclipse-based system developed by our working group. No detailed background is needed; interest in the topic of safety analysis, verification and any knowledge about model-based development (Tools like Scade, SimuLink, NuSMV) will be welcome, but not demanded. After presenting the traditional way of model-based safety analysis and the new approach, there will be space for discussion and comparison of model-based safety analysis methods in the context of different safety relevant questions. During the tutorial, the example will be interactively presented and possible benefits and limitations will be discussed. Also the benefit resulting out of the tool-support will be discussed and possible extensions of the tools will be presented and discussed to develop the tool further.

Structure (half-day)

- Brief introduction
- Background information (15 min)
    - safety analysis methods
    - formal methods
- Modeling safety-critical systems (60 min)
    - adequate system models
    - abstracting real-world systems to state-spaces
    - differences between software, hardware and environmental parts
    - formal failure mode models

================ Break (15min) ================

- Model-based safety analysis (90 min)
    - Qualitative methods
    - Quantitative methods
    - Multi-criteria optimization
- Summary/Outlook (15 min)

Proposed supporting materials

Whiteboard and/or Flipchart would be nice. A beamer will be needed.

Frank Ortmeier, Otto-von-Guericke University Magdeburg

frank.ortmeier@ovgu.de

Presenter

Frank Ortmeier is a professor for "Computer Systems in Engineering" at the Otto-von-Guericke-University of Magdeburg. His current research is mainly focused on making cyber-physical and software-intensive systems smarter and more dependable. This includes a priori model-based design methods known from software engineering as well as a posteriori analysis techniques known from safety analysis or program verification. Main domains of application include robotics, transportation, rail and avionics.

He has lead a number of different research project in the domain of critical systems. He is active in several (pre-)standardization committees and program chair of the “31st International Conference on Computer Safety, Reliability and Security”.