Model-based Formal Safety Analysis of an Airport Surveillance Radar System

Adrian Beer\textsuperscript{1}, Uwe Kühne\textsuperscript{2}, Florian Leitner-Fischer\textsuperscript{1}, Stefan Leue\textsuperscript{1}, Rüdiger Prem\textsuperscript{2}

2 pages
Model-based Formal Safety Analysis of an Airport Surveillance Radar System

Adrian Beer¹, Uwe Kühne², Florian Leitner-Fischer¹, Stefan Leue¹, Rüdiger Prem²

¹University of Konstanz
²EADS Deutschland GmbH – Cassidian

Abstract. The development of safety-critical systems is commonly governed by development standards such as, for instance, ESAAR 4 [2]. It is applicable to the Airport Surveillance Radar (ASR) system, under development at Cassidian, that we consider here. A common feature of these standards is that they recommend methods and processes, including semi-formal and formal analysis methods, for highly safety-critical components. We report on a case study which demonstrates that the formal analysis technique of probabilistic model checking can be applied to the ASR System and that this formal analysis activity can be fully automated and seamlessly integrated into existing industrial software development processes and tools.

QuantUM. In precursory work we have proposed the QuantUM [4] approach that enables the automatic quantitative safety analysis of models given in the Unified Modeling Language (UML). To accommodate the fact that system architectures in industrial design processes are increasingly often modeled using an extension of the UML called the Systems Modeling Language (SysML), we have adopted QuantUM to SysML. The QuantUM tool chain that we have implemented can directly interface with standard industrial-strength CASE tools supporting UML or SysML, such as Rational Rhapsody or Enterprise Architect. QuantUM automatically translates a given UML or SysML model and its properties directly into the input language of the probabilistic model checker PRISM [3], which QuantUM uses as a verification back-end. QuantUM automatically computes probabilistic counterexamples for the translated models and presents them as fault trees or UML sequence diagrams, which are notations frequently used in engineering practice.

Verification of the ASR. The ASR System is used for monitoring the airspace in the vicinity of an airport and to guide aircraft according to their flight plan. We consider the hazard of an unintended loss of information concerning some aircraft, which is also referred to as a “coasted track”. We are interested in the total occurrence probability for this hazard over a mission time of one hour. The QuantUM/SysML model of the ASR consists of 5 components, each of which contains a state machine with between 15 and 40 states representing both the normal and the failure behavior. For an increased system availability the ASR is built with redundancy. The first, naïve approach to model the redundancies led to a state space explosion during the analysis of the system. In order to contain the size of the state space of the PRISM model we applied adequate forms of abstraction to the QuantUM/SysML model, akin to counter abstraction.
Model-based Formal Safety Analysis of an Airport Surveillance Radar System

Figure 1: The fault tree for getting a coasted track.

The generated PRISM model consists of appr. 46 million states and appr. 326 transitions. Model checking the total probability of reaching the hazard using PRISM required 509 sec. analysis time on common hardware. Due to the size of the PRISM model a complete fault tree, requiring a complete state space exploration, could not be generated by QuantUM. However, the probability accumulated over all paths represented by the fault tree converges towards the value of the probability of reaching the hazard state computed during the preceding model checking run. We can hence draw conclusions even from an incomplete fault tree. In Figure 1 a partial fault tree with the probability for the hazard occurring within one hour is shown. The depicted fault tree was computed with QuantUM in appr. 10 min. and the probability mass difference for reaching the hazard state was in the order of $10^{-14}$. This means that the inaccuracy of the result was at most $10^{-14}$ which is sufficiently small to consider the result as valid. Notice that all values given here are dummy values since the real values are confidential and cannot be published. For more information on the analysis refer to [1].

Conclusion. We show that the QuantUM approach is applicable to industrial size case studies. The calculation of the probabilities for different properties of the ASR system was efficiently possible in a reasonable amount of time. We currently work on an improvement for the fault tree generation based on a combination with functional model checking to enable a full construction of the fault tree even for large systems.

References


