Risk Management for High Tech Systems

Marielle Stoelinga

University Twente, the Netherlands
Radboud University Nijmegen, the Netherlands

ABSTRACT

How do we ensure that self-driving cars, nuclear power plants and Internet-of-things devices are safe and reliable? That is the topic of risk management. Fault tree analysis is a very popular technique here, deployed by many institutions like NASA, ESA, Honeywell, Ford, Airbus, the FDA, Toyota, Shell etc.

In this presentation, I will elaborate how the deployment of stochastic model checking can improve the capabilities of fault tree analysis, making them more powerful, flexible and efficient, allowing one to analyze a richer variety of questions faster, and thereby increasing their practical relevance and deployment in practical risk assessments.

I will report on our experience with the application and validation of these techniques in industrial practice. In particular, I will show how compositionally, model-driven engineering, graph rewriting all helped to crunch industrial cases. Finally, I will present some new directions on the deployment of big data analytics within fault tree analysis.