



Master's  
Thesis

Risk-Aware Software  
Architecture for  
Cyber-Physical  
Production Systems

Background

Life is full of risks and so are the systems surrounding us. Sensors can be unreliable, components can fail, communication may get lost, actuators may be imprecise. Nowadays, software and system models rarely make the risks related to their parts explicit, which prevents analyzing and addressing them. Where risks are known, countermeasures can be planned. To enable this, means to express software and system architectures and risk modeling means need to be integrated in a way that the analysis of inherent risks can be automated.

Challenge

MontiArc is an architecture description language based on the focus calculus that enables formal analyses of system properties and has been applied to a variety of domains including automotive, digital twins, manufacturing, and robotics. In this thesis, it shall be extended with risk modeling means based on OpenPRA to support risk analysis as well. Therefore, suitable means to modular risk modeling shall be analyzed and integrated into MontiArc's language and model checking framework such that risks based on individual architecture components but also on their integration can be identified and estimated. OpenPRA is an open-source framework, which aims to integrate multiple Probabilistic Risk Assessment (PRA) methods into an easy-to-use and highly customizable environment. OpenPRA includes a Fault Tree Analysis module, a Discrete-Time Markov Chain module, an Event Tree Analysis module, an integrated analysis module and Model-to-Model transformation methods.

Task

- Identify sources of risks for MontiArc architectures
- Devise a method for modular risk analysis based on OpenPRA
- Integrate OpenPRA into MontiArc
- Generate risk models in the OpenPRA format from MontiArc
- Systematically evaluate risk modeling with OpenPRA and MontiArc

Requirements

- Curiosity for modeling languages
- Experience in object-oriented programming
- Motivation to learn and perform challenging tasks
- Ability to work independently
- Creativity and problem solving skills

Knowledge gained

- Model-Driven Software Development
- Architecture modeling with MontiArc
- Risk modeling with OpenPRA
- Independent scientific work

