SysRO

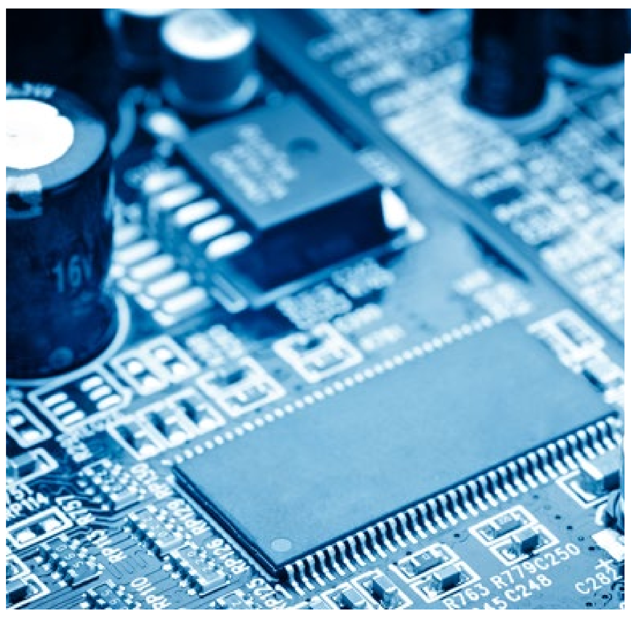
Requirement-driven Optimization of System Concept with Integrated Model Based Safety Analysis

Context

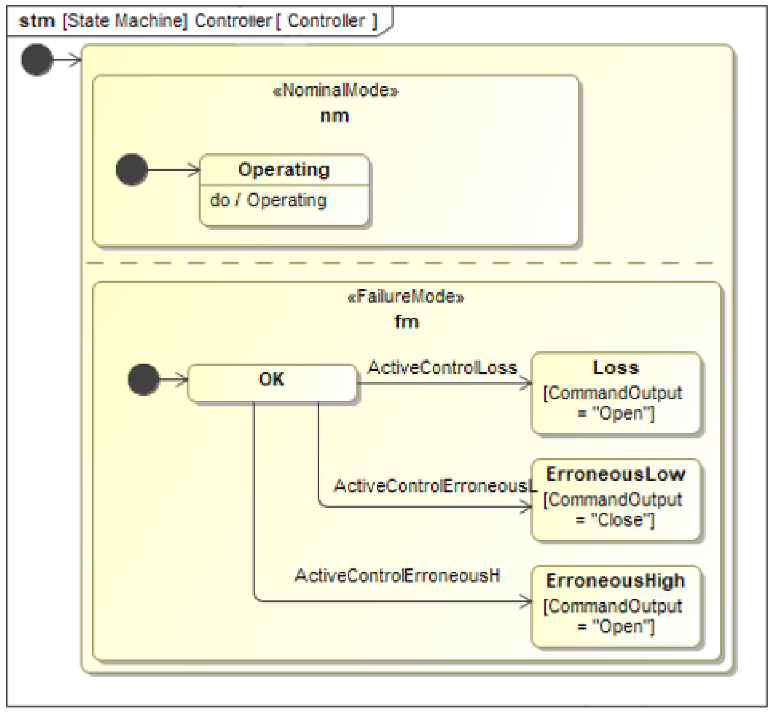
Today's technical systems are getting more and more complex associated with the rapid increase of new technologies in a number of industrial domains. These systems have one feature in common: the increasing amount and complexity of software. And they have to be safe against humans and the environment. Ascertaining the safe behavior of technical systems is key. Therefore, a number of safety regulations and standards have emerged just over the last decade. Consequently, there is a significant growth of the scope and the intensity of safety assessments of technical systems required to being compliant with these safety regulations and standards. However, this has also an impact on today's approach of performing safety assessments which are predominantly carried out "manually", i.e. today's commercially available and cross-industry used safety analysis tools, that are no longer up to date to cope with the complexity of technical systems. In order to compete with the increasing complexity of technical systems in combination with the faster time-to-market demands guaranteeing the required level of safety, a framework for a requirements-driven optimization of the system concepts in conjunction with a Model-Based Safety Analysis (MBSA) respectively Model-Based Systems Engineering (MBSE) is proposed for this research. By integrating MBSA into the MBSE based development of the system concepts, an automated procedure was developed respecting the relevant safety regulations/standards.

Results

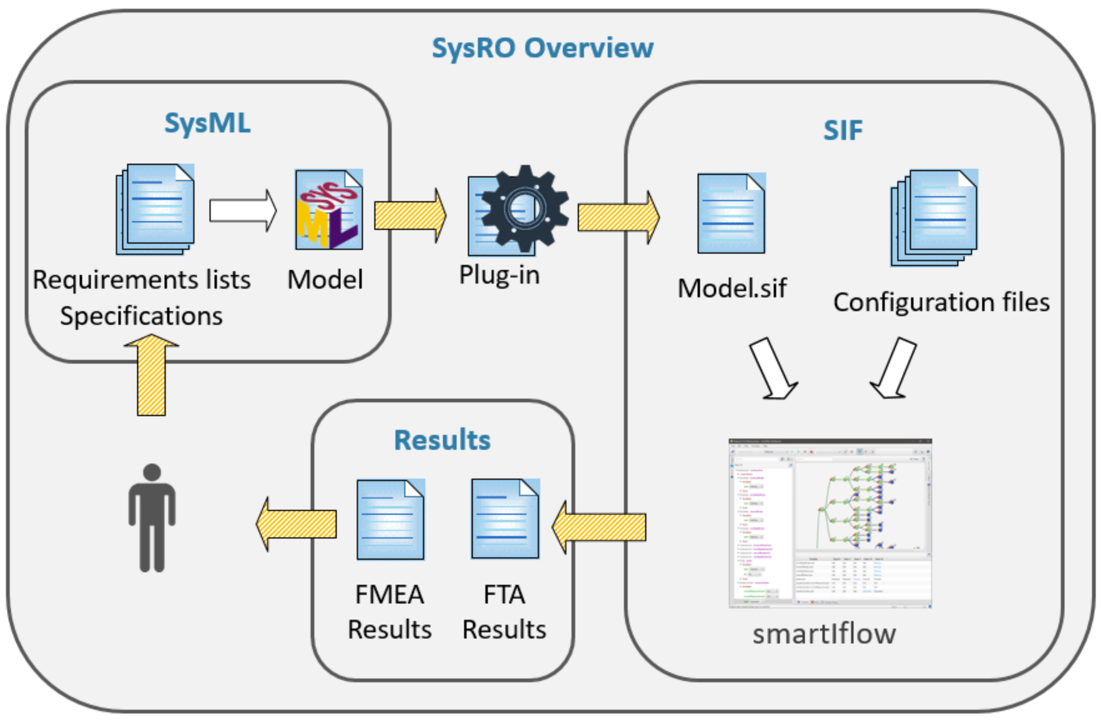
Automated MBSE-MBSA procedure is available for the industrial partners after being tested for several use cases. This procedure makes the automatic generation of FTA and FMEA from a common qualitative technical system model described with the SysML language. The SysML modeling includes both the description of the nominal system behavior and of the failure system behavior. This way of system modeling ensures a full MBSE-MBSA integration enabling the industrial partners to identify earlier in the preliminary concept phase the critical and in many cases safety-related design aspects. The automated procedure combines the modeling method of the nominal and failure system behavior using SysML and the coupled safety analysis using smartIflow Workbench developed by Ulm University of Applied Sciences with the automatic generation of the safety analysis artifacts.



Technical System



Failure modelling approach in SysML



Integrated MBSE-MBSA Procedure

Result Valorisation

The four industrial partners use the results in different ways:

- Through the network of expertise constituted by the SysRO research, the MBSE-MBSA know-how of the industrial partner companies acquired were directly valorized in their industrial practices
- The automatic creation of the safety artifacts helps to avoid human errors of omission or misunderstanding of the technical system. The automatically generated FTA and FMEA are well-suited for system concepts
- Suitable solutions to model high-level system, to control the size of the transition system and to compute the potential failure modes require further research and development (limitations with the complexity of industrial cases). The potential of the automated procedure is demonstrated.

Partners

Industrial Partners: Brusa Elektronik – Johnson Electric - Liebherr Machines Bulle - Meggitt System
Academic Partners: School of engineering and architecture Fribourg, ROSAS Center Fribourg, Institute of Smart and Secured Systems, Sustainable Engineering Systems Institute - Ulm University of Applied Sciences, Department of Computer Science
Research Funding Body: New Regional Policy of the canton Fribourg

npr Nouvelle politique régionale

Hochschule Ulm

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

ROSAS
Center Fribourg