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

Collaborative Project funded by npr Nouvelle politique régionale

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 technical systems have to be safe against humans and the environment.

Scope

Therefore, a number a 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. Nowadays, to perform safety assessments, Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) typically applied to support evaluation and verification of a system design are done manually.

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 in this study. By integrating MBSA into the development of system concepts referring to MBSE, an automated procedure was developed respecting the relevant safety regulations and standards.

Methodology

The chosen 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 v0.3.9 with the automatic generation of the safety analysis artifacts. The tooled-procedure for MBSE-MBSA integration consists of enhanced system modeling structure, using the SysML language, which includes the nominal and failure modes in a single model. The interface between SysML and smartIflow is bridged by a specific developed Plug-in (see Fig. 1, SysML Plug-In). Once to export/translate the data in smartIflow, where the analysis of failure modes is conducted and post-processed. The automated generation of fault tree analysis (FTA) and failure mode and effect analysis (FMEA) is performed by two Plug-ins into smartIflow Workbench as shown in Fig.1.

Results

The automated MBSE-MBSA procedure is available for the industrial partners after being tested for simple technical 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.
For simple technical systems analyzed, the automatically generated FTA and FMEA are similar to the manual FTA and FMEA, except additional detected failure modes for automated FTA and FMEA.

The automatic creation of the safety artifacts helps to avoid human errors of omission or misunderstanding of the system. For technical systems of industrial partners, the automated procedure has limitations and is not yet sufficiently developed.

The model checking algorithm of smartIflow transforms the generic model representation into a transition system. Ideally, the graph contains paths for every possible sequence of input event, so that every possible evolution of the system is covered. Since the complexity can be enormous, 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.

Facts et Figures

Project Acronym	SysRO
Number of partners	6
Research Area	Safety Engineering
Project Dates	Nv.2018 – Febr.2020
Project Cost	CHF 256'000
Project Funding	New Regional Policy
Information	pascal.bovet@hefr.ch

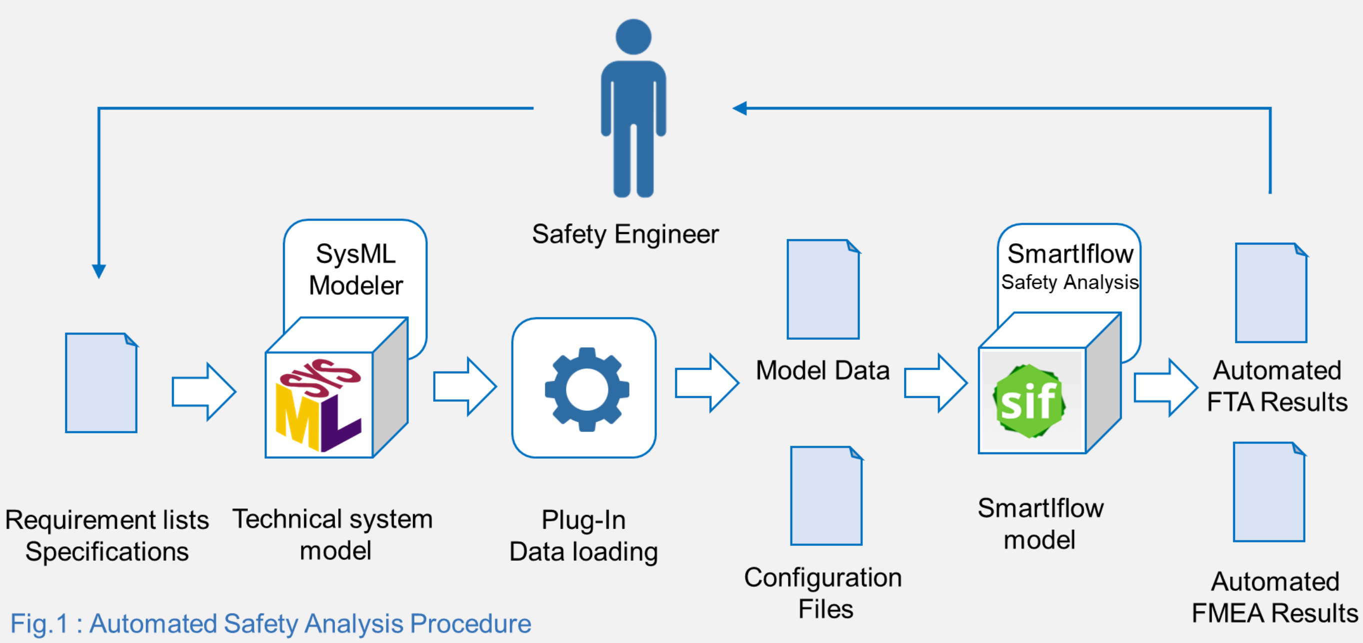

Fig.1 : Automated Safety Analysis Procedure

Project Partners

BRUSA, JOHNSON ELECTRIC, LIEBHERR, MEGGiTT, Hochschule Ulm, ROSAS Center Fribourg, Haute école d'ingénierie et d'architecture Fribourg / Hochschule für Technik und Architektur Freiburg