The SAFE Technology Platform - An Open Source Tool Platform for Safety Modeling and Analysis

The ISO26262 standard (ISO, 2011) defines process requirements for functional safety-aware development in the automotive domain. It has high demands on process documentation and analysis. It is currently not clear how the development view and models necessary for safety documentation and analysis can and should be integrated in order to minimize modeling effort, to keep consistency between artifacts and enable effective reusability. These challenges can only be tackled effectively in a joint initiative that includes the complete automotive supply chain (OEMs, Tier 1's, Silicon vendors and tool suppliers) as well as academia.

The project SAFE

The ITEA2 project SAFE (Safe Automotive software architecture) is a European funded project. It provides methods for integrated safety modeling and safety analysis. The results ensure and speed up the efficient development of safety features in cars.

The three main objectives of SAFE are:

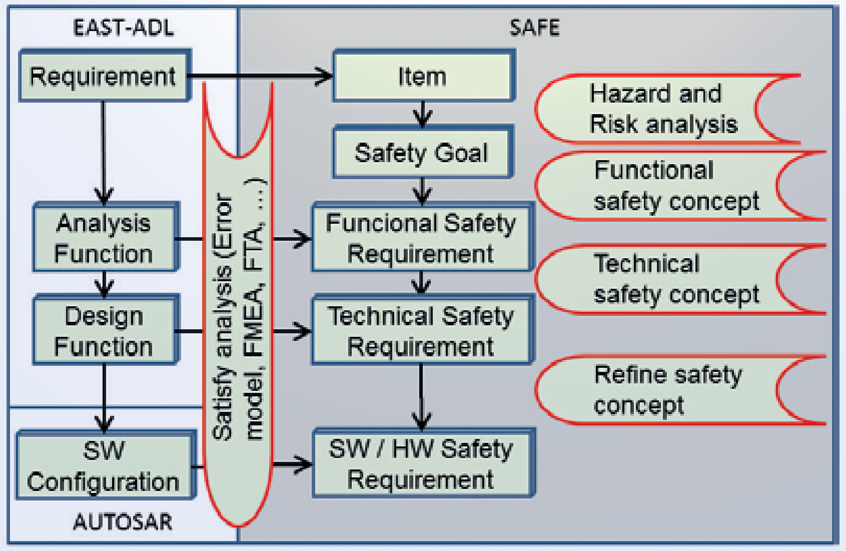
- Extension of EAST-ADL and AUTOSAR, to enable effective integration of artifacts associated with the application of ISO26262. The extended model is implemented in a reference technology platform (SAFE RTP).
- Methods, e.g. for efficient capturing of safety goals and requirements as well as for safety evaluation, are enhanced in order to benefit from the integrated model. The SAFE RTP is extended with a set of appropriate plug-Ins.
- An ISO26262 compliant process is defined on top of model-based development and evaluated with realistic and measurable industrial case studies.

The extensions to EAST-ADL and AUTOSAR are defined in an own meta-model. This meta-model covers the safety related elements and relationships necessary to ensure the safety requirements. This meta-model refers to the architecture models in EAST-ADL and AUTOSAR. Therefore, the meta-model is not a stand-alone architecture description language. This has an important implication for the SAFE RTP: It has close relationships to the platform implementations from EAST-ADL and AUTOSAR. EAST-ADL has an Eclipse platform implementation called "EATOP" (www.eclipse.org/proposals/modeling.eatop/). For AUTOSAR a user group "ARTOP" providing an Eclipse based implementation already exists. The SAFE RTP integrates EATOP and ARTOP.

EATOP: An Eclipse tool platform for EAST-ADL

EATOP supports the work of the EAST-ADL association by providing an Eclipse-based tool platform implementation for the EAST-ADL standard. In the past there have been multiple initiatives to create Eclipse-based implementations of EAST-ADL which led to a quite cluttered and redundant tool landscape. The goal of EATOP is to reconcile these initiatives, consolidate the different implementations and shape like a reference implementation of EAST-ADL under one umbrella. It focus on providing the following main features:

- Implementation of important versions and revisions of the EAST-ADL meta-model in EMF
- Serialization/de-serialization of EAST-ADL models/files conforming to the EAST-ADL XSD schema
- A tool platform and an exemplary basic IDE experience for creating, managing, editing, validating, transforming or otherwise processing EAST-ADL models in the Eclipse workspace.



Scope of the SAFE meta-model. The red bordered actions are supported by the SAFE RTP.

ARTOP: An Eclipse tool platform for AUTOSAR

ARTOP is an Eclipse-based implementation of the AUTOSAR metamodel. From features point of view it is similar to the features implemented in EATOP. ARTOP is organized by the ARTOP user group, a cooperation of several companies from the automotive industry. The availability of ARTOP is restricted to AUTOSAR members only.

SAFE RTP: An Eclipse tool platform for the SAFE metamodel

SAFE RTP is an EMF-based Java implementation of the SAFE metamodel that integrates with the AUTOSAR meta-model from ARTOP and the EAST-ADL meta-model from EATOP.

It offers a basic authoring experience, i.e., an Eclipse perspective with a tree-based model explorer view for navigating through SAFE model files and their contents as well as some exemplary form and tree-based editors enabling safety-related extensions for EAST-ADL, and AUTOSAR models to be edited.

An important aspect of the SAFE RTP is interoperability. On the one hand, it supports the integration and exchange of safety-enriched architecture, dynamic behaviour, execution environment and hardware descriptions with existing non-Eclipse based engineering tools by making an appropriate XSD schema-based exchange format and corresponding serialize/de-serialize components available. On the other hand, the SAFE meta-model platform enables the integration with other Eclipse-based tools and plugins. To make this possible, the SAFE meta-model platform is based on Sphinx (www.eclipse.org/sphinx). Using Sphinx simplifies the integration of the SAFE meta-model with EATOP and ARTOP.

Outlook

Compliance with the Cooperation RTP developed in the CESAR project and maintained by EICOSE will be ensured. An integration will be discussed (more information about the CRTP in SafeTRANS News 1/2013, page 14 and 15).

The research project SAFE started in July 2011 and will end June 2014. Initial concepts are already published in February 2013, an integrated meta-model and the technology platform since June 2013. The process model will follow end of 2013.

By Stefan Voget, Continental

More information:
www.safe-project.eu
www.artop.org
www.autosar.org
www.east-adl.info
www.cesar-project.eu

Acknowledgement:
Many thanks to the project partners from the SAFE project.

This document is based on the SAFE and SAFE-E projects. SAFE is in the framework of ITEA2, EUREKA cluster program Σ! 3674. The work has been funded by the German Ministry for Education and Research (BMBF) under the funding ID 01IS11019, and by the French Ministry of the Economy and Finance (DGCIS). SAFE-E is part of the Eurostars program, which is powered by EUREKA and the European Community (ID 01|S1101). The work has been funded by the German Ministry of Education and Research (BMBF) and the Austrian research association (FFG) under the funding ID E!6095. The responsibility for the content rests with the authors.