ITEA 3

Project Results

SAFE

The integrated modelling of function and safety in automotive processes

Executive summary

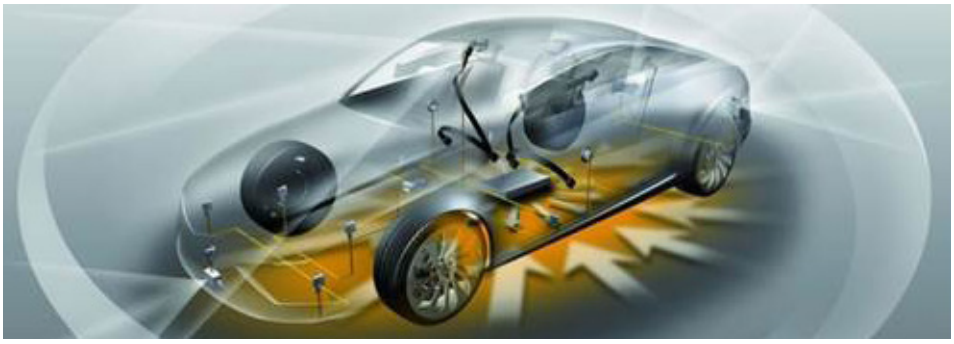
The goal of the SAFE project was to enable effective and compliant application of ISO26262 in the automotive industry processes by providing model-based development processes that integrate functional and safety development based on existing development lifecycle processes. The most concrete impact realised by the SAFE project is the enhancement of tools that not only support the users in safety modelling and analysis but also directly influence further change in the market towards the integrated modelling of both functional and safety aspects.

Project origins

In 2011 a new standard, ISO26262, an adaptation of the generic IEC 61508 functional safety base standard, was published for the functional safety-related aspects during the safety lifecycle of systems related to electrical, electronic and software elements that provide safety critical functions. Innovations were needed, and generated, on three levels: concept, tools and process. In addition, developers and safety engineers had to be brought together to overcome the diversity in language and mind set of two, until now, separated disciplines. In fact, a key breakthrough in the project came through a common understanding of the requirements listed in the standard; at tool level this is the basis for improving the interoperability between the tools.

Technology applied

Firstly, new concepts were developed to model safety and architecture as well as methods for safety analysis, variant management and safety code generation based on the existing modelling languages EAST-ADL and AUTOSAR. Next, SAFE developed an exchange format compliant with the existing standards, enriched with the SAFE meta-model formats, make a major step in



direction of integrated, model based design in the tool market of the automotive industry; the tools provide functionality for integrated development and safety analysis on each of the abstraction levels – requirements, architecture, HW design, SW modelling and coding. The initial fast exploitation results of these tools show that the market is increasingly harmonising the processes implemented in the tools. Finally, a guideline developed by the SAFE project, formalised in a process model and enclosing an assessment model, provided an interpretation to help the industry to come to a unique, common agreed interpretation.

The evaluations during the project were made with the help of real industrial developments, including existing products such as a powertrain e-gas concept and electronic steering column lock system as well as developments of new, innovative products like an electrical brake system, a mixed criticality HW/SW platform, new microcontroller abstraction software and an active torque distribution system. Since the evaluators are not demonstrators, their development processes have been improved with SAFE concepts based on the evaluation results in a process where no borders exist between research and series development.

Making the difference

The impact is evident in both commercial and research tools. For instance, Dassault Systèmes introduced requirements in Safety Designer as a temporary solution, adding innovative architectural metric plug-ins and achieving major breakthroughs in the performance of algorithms for safety analysis, a key issue in large-scale industrial models. Vector Informatik implemented FMEA, a model-based qualitative

safety analysis method, and added malfunction modelling capabilities in its PREEvision tool while pure::systems managed to seamlessly integrate pure::variants into the SAFE platform, thereby enabling the variant management capabilities of pure::variants for contexts with safety related assets. On the research tool side, FZI added prototype implementations for hardware modelling and evaluation in PREEvision tailored to the demands of ISO 26262 and including an extension for failure data annotation. Itemis was active in the implementation, publication and distribution of a tool platform via internet that realises the SAFE meta-model. Finally, OFFIS enhanced the safety analysis platform, originally developed during the ESACS and ISAAC projects, by implementing a novel approach for model-based safety analysis (MBSA).

The early publication of concept documents along with the publication of two books on functional safety (for didactic purposes and for specialists) helped the standardisation activities of the SAFE partners to reach another level. From the beginning partners were involved in the standardisation activities in EAST-ADL association and AUTOSAR consortium, and then in discussions with SafeTrans and OMG, with the contribution made to the ISO 26262 standard a major achievement. In fact, SAFE realised the first incorporation of ISO26262 in a standardised ADL while the SAFE guidelines provide an interpretation of the ISO26262 standard to the market. Besides the standardisation activities, the Eclipse-based tool platform activities led to visibility and interest in the market, with several downloads, especially from OEMs and suppliers, already registered. Since the tools implemented in the SAFE project were developed by both commercial tool vendors and research institutes, and are part of already existing bigger tool-sets, fast exploitation was facilitated by delivering new versions of the commercial tools as well as by publishing new features in the research tools.

Future prospects

SAFE has set the foundation to enable EAST-ADL, AUTOSAR, OMG and other standards to evolve as well as helped to identify limitations of the ISO26262 such that also the basis standard itself can be improved in a subsequent iteration. The concepts now need to be applied in the company processes and product projects so that SAFE can influence other upcoming research projects as well as industrial series projects.

Major project outcomes

Dissemination

- 9 articles in magazines, 2 books and 5 thesis
- 67 presentations/demos at conferences and fairs – mainly functional safety related conferences in France and Germany

Exploitation (so far)

- Enhancements of commercial tools:
  - Dassault Systèmes added new functionality in Aralia Fault Tree Analyser and Safety Designer
  - Vector Informatik introduced functional and technical safety concept in the architecture tool PREEVision
  - pure::systems enabled integrated variant handling with safety related items in pure::variants
- Concept implementations in research tools:
  - FZI realized an architectural benchmarking plugin in the PREEVision tool
  - Fortiss implemented safety case analysis and reporting in autoFOCUS3 and CHROMOSOME
  - Itemis created an open source Eclipse tool platform
  - OFFIS enhanced the tool HeRaClear with safety analysis methods

Standardisation

- Participation in the EAST-ADL association with 11 change requests
- Continous, active participation in the AUTOSAR consortium to enhance the safety parts
- Feedback to the ISO26262 consortium to enhance future releases
- Coordination and hand over of results to OMG to create a future ADL standard for the automotive industry
- Coordination and hand over of results to Eicose to create a tool reference implementation

ITEA is the EUREKA Cluster programme supporting innovative, industry-driven, pre-competitive R&D projects in the area of Software-intensive Systems & Services (SiSS). ITEA stimulates projects in an open community of large industry, SMEs, universities, research institutes and user organisations. As ITEA is a EUREKA Cluster, the community is founded in Europe based on the EUREKA principles and is open to participants worldwide.

https://itea3.org

SAFE

10039

Partners

Austria

TTTech Computertechnik AG

France

Continental Automotive France SAS
Dassault Systèmes
itemis France
Laboratoire Bordelais de Recherche en Informatique
Valeo

Germany

AVL GmbH
BMW Car IT GmbH
Continental Automotive
Continental Teves AG & Co. oHG
Forschungszentrum Informatik (FZI)
Fortiss
Infineon Technologies AG
OFFIS
Pure Systems GmbH
TÜV NORD Mobilität GmbH & Co KG
Vector Informatik GmbH
ZF Friedrichshafen AG

Project start
July 2011
Project end
December 2014

Project leader
Stefan Voget,
Continental Automotive GmbH

Project email
stefan.voget@continental-corporation.com

Project website
www.safe-project.eu