SAFE

Sustaining automotive safety standards and standardisation

Published December 2017

Driving on the road is a way of life. Being able to get safely from A to B is something we take for granted. And today driving is safer than it was ten years ago, and ten years before that, and in ten years time it will be even safer. In 2011, a new standard, ISO26262, 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. The goal of the SAFE project was to enable the automotive industry to comply effectively with this ISO26262 by providing model-based development processes that integrate functional and safety development based on existing development lifecycle processes.

Impact highlights

- SAFE was an essential part of the jigsaw in establishing ISO26262, a worldwide standard and one of the most important in the automotive industry.
- SAFE enabled the automotive industry to comply effectively with ISO26262, which is mandatory for all OEMs and suppliers. SAFE realised the first incorporation of ISO26262 in a standardised Architecture Description Language (ADL) while the SAFE guidelines provide an interpretation of the ISO26262 standard to the market.
- 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 the basic standard itself can also be improved in subsequent iteration.
- Thanks to the SAFE project, Continental established the ISO26262 compliance in two major domains, namely the safety critical domains of powertrains and chassis brake systems. These domains represent 40% of Continental's product share and thanks to the SAFE project, Continental was able to keep its leading role in these domains.

Project results

SAFE developed new concepts to model safety and architecture as well as methods for safety analysis, variant management and safety code generation based on the modelling languages EAST-ADL and AUTOSAR. In addition, an exchange format was created that is compliant with the existing standards, enriched with the SAFE meta-model formats. This represents a major step in direction of integrated, model-based design in the tool market of the automotive industry. The resulting tools provide functionality for integrated development and safety analysis on each abstraction level – requirements, architecture, hardware design, software modelling and coding. Finally, a guideline developed by SAFE, formalised in a process model and containing an assessment model, provided an interpretation to help the industry to come to a unique, commonly agreed interpretation. The evaluations during the project were made with the help of real industrial developments. These included 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 and a mixed criticality HW/SW platform.

Exploitation

As a result of the SAFE project, Dassault Systèmes developed a Smart, Safe & Connected Car solution, offering customers the 3DExperience platform© designed to give automotive developers a very specific way to manage the kind of embedded systems that have become a growing challenge in the automotive industry. This new solution also helps customers ensure they are compliant with the ISO26262 and Automotive Open System Architecture (AUTOSAR) safety standards.

Vector Informatik implemented FMEA, a model-based qualitative safety analysis method, and added malfunction modelling capabilities in its PREEvision tool, a software application that supports architects, network designers, development engineers and test engineers through the entire development process.

pure::systems has seamlessly integrated pure::variants into the SAFE platform, enabling the variant management capabilities of pure::variants for contexts with safety related assets whereby the development process becomes up to 20% more efficient, faster and more reliable.

OFFIS extended the model-based safety analyses towards security aspects in such a way that the occurrence of hazardous events can be investigated not only with respect to relevant faults (of the system) but also with respect to relevant threats. In the future all results will be embedded as part of a contract-based design theory allowing the construction of compositional safety cases.

TTTech developed a safety layer software package enabling designers to use AUTOSAR QM basic software within safety relevant applications up to automotive safety integrity level D, and developed a safety issue hardware, satisfying particular safety requirements. This enables TTTech to provide a means whereby application developers can reuse existing non-safety relevant software building blocks in highly safety relevant applications, reducing development time and cost and mitigating the risk of the reuse of proven software elements.

SAFE

07006

PROJECT LEADER

Stefan Voget, Continental Automotive GmbH

PROJECT START

July 2011

PROJECT END

December 2014

PROJECT WEBSITE

https://itea4.org/project/safe.html

PARTNERS

Austria

- AIT ○
- TTTech Computertechnik AG ⊙

France

- Continental Automotive France SAS ◉
- Dassault Systèmes ◉
- itemis France ⊙
- Laboratoire Bordelais de Recherche enInformatique ○
- 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 ◉

◉ (Large) Industry ○ Research institute ⊙ SME ◉ University ● Government