Contract number: ITEA2 – 10039

Safe Automotive soFtware architEcture (SAFE)

ITEA Roadmap application domains:

Major: Services, Systems & Software Creation

Minor: Society

ITEA Roadmap technology categories:

Major: Systems Engineering & Software Engineering

Minor 1: Engineering Process Support

WP7
Deliverable 7.2
Training Material

Due date of deliverable: 30/05/2014

Actual submission date: 30/05/2014

Start date of the project: 01/07/2011 **Duration:** 36 months

Project coordinator name: Stefan Voget

Organization name of lead contractor for this deliverable: Vector Informatik GmbH

Editor: Eduard Metzker

Contributors: Eduard Metzker (Vector Informatik GmbH), Nico Adler, Stefan Otten (Forschungszentrum Informatik Karlsruhe), Stefan Voget (Continental AG), Maged Khalil (fortiss), Michael Schulze (pure-systems GmbH)

Revision chart and history log

Version	Date	Reason
0.1	15.05.2013	Initial draft version
0.5	05.08.2013	Overview of contributors and contributions
0.7	01.01.2013	Update of contributors and contributions
0.8	22.03.2014	Short descriptions of contributions
0.9	23.05.2014	Review version
1.0	30.05.2014	Released version

1 Table of contents

2 Executive Summary

The purpose of deliverable D7.2 is to give a reference to and summary of the training material which was contributed by the SAFE project partners. The goal of the training material is to illustrate the application, usability and utility of the concepts and tools which have been developed in the SAFE project. The contributions have been made in different formats such as presentations, webinar video recordings and professional training workshops.

3 Introduction and Overview of the Document

The SAFE project developed a meta model and tools for designing and analyzing safe automotive software architectures based on the requirements of ISO 26262 [1]. The results are evaluated in SAFEV WP5 by the industrial project partners. To support further dissemination and adoption of the SAFE concepts, methods and tools the project partners developed training material which illustrates the practical application of the SAFE results. It is explicitly not meant as training material to teach the basics of the ISO 26262. In section 4 we give an overview and classification of the SAFE training material and explain the classification criteria. In section 5 a brief summary of the training material is given.

4 Overview and Classification of Training Material

Figure 1 gives an overview and classification of the SAFE training material. The column “Free Access” indicates if the training material is accessible via the SAFE website. If training material is not accessible via the SAFE website an alternative link can be found together with the abstract of the training material in section 5. The type of material indicates the format of the training material. Currently training material is available as presentations, video and audio recordings of webinars and full training workshops. The “Summary” column very briefly summarizes the scope of the training. More detailed summaries can be found in section 5. The column “Contributors” shows the authors of the training material which can be contacted for more detailed information. The remaining columns classify the content of the training material with respect to prominent concepts of the ISO 26262 [1]. It indicates which content can be found in the training material.

.

#	Training Material	Access	Type of Material	Summary	Contributor(s)	Item Definition	Hazard and Risk Analysis	Safety Goals	Safety Requirements Traceability	Safety Requirements Allocation	ASIL decomposition	Functional Safety Concept	Technical Safety Concept	Technical Safety Concept (HW)	Technical Safety Concept (SW)	HW/SW Interface (HSI)	Malfunction Analysis	FMEA	Qualitative FTA	Quantitative FTA	Fault Tree Synthesis	HW Failure Data Table	HW Architectural Metrics	FRC Method	Safety & AUTOSAR	Code Generation	Safety Case	Variability
1	ISO 26262 Compliant Development of Automotive EE Systems with PREEvision	Free	Slides	Illustrates the design and analysis of safety relevant systems with PREEvision from item definition to the safety case.	Vector Informatik gmbH, FZI	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
2	ISO 26262 Compliant Development of Automotive EE Systems with PREEvision	Free	Webinar	see 1)	Vector Informatik gmbH	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
3	Break Example	Free	Slides	EAST-ADL dependability package illustrated by a brake example	Continental AG	X		X	X	X		X	X															
4	Safety Goals Modeling, Safety Cases and Patterns in Safety-critical Development	Free	Slides	Introdution to safety goals modelling and reusable patterns in safety critical model-based development	Fortiss			X																			X	
5	Integrated Safety Workshop	Commercial	Training	Methods of embedded sofware development based on requirements of ISO 26262 and application in the tools DaVinci and PREEvision.	Vector Informatik GmbH	X	X	X	X	X	X	X		X			X								X	X		X
6	Functional Safety and Variability - Can they be brought together?	Free	Webinar	Variability in functional safety related assets like hazard analysis, FTA, FMEA.	pure-systems GmbH		X										X	X	X									X

Figure 1: Overview of SAFE Training Material

5 Summary of Training Material

5.1 #1 ISO 26262 Compliant Development of Automotive EE Systems with PREEvision

The presentation covers the design and analysis of safety relevant systems with the system engineering tool PREEvision [2]. As a consistent example for the training a lane keeping assistance example (LKA) is used. The basic goal of the LKA system is to serve „as a mechanism designed to warn a driver when the vehicle begins to move out of its lane (unless a turn signal is on in that direction) and to perform correcting measures if necessary. The LKA example does not claim to be complete in any sense. Its main purpose is to illustrate the model based system engineering approach for functional safety which is provided in PREEvision.

First an item definition is performed which serves as a foundation for the hazard and risk analysis. In the hazard and risk analysis the hazardous events are classified based on a catalogue of operational situations and operating modes. Functions and malfunctions can be allocated to each hazardous event. Safety goals and safe states are formulated to prevent or mitigate the hazardous events.

In the next step the safety goals are refined to functional safety requirements and a functional safety concept is developed. The functional safety requirements are allocated to elements of the preliminary architecture. The concept of ASIL decomposition is illustrated.

The functional safety requirements are further refined into technical safety requirements and a technical safety concept is developed. The technical safety concept includes the hardware architecture, software architecture and safety mechanisms. The technical safety requirements are allocated to the architecture elements and the HW/SW interface is specified.

Analysis techniques such as FMEA, FTA and hardware architectural metrics are applied to the developed safety concepts. The results of the analysis are used to introduce new requirements and safety mechanisms to improve the safety concept.

All developed work products are fully traceable. The implementation in PREEvision supports dedicated trace tables for all work products. All developed work products are continuously and automatically checked for consistency. Safety engineers can quickly identify and fix formal issues in their concepts.

A safety case report can be generated based on the developed work products. A safety case structure which was developed in the SAFE project is used to generate the safety case report from the work products.

The training material can be downloaded from the SAFE website or form the Vector website (www.vector.com).

5.2 #2 ISO 26262 Compliant Development of Automotive EE Systems with PREEvision (Webinar Recording)

This is a webinar video & audio recording of the material described in #1 including a presentation of the PREEvision tool.

The training material can be downloaded from the SAFE website or form the Vector website (www.vector.com).

5.3 #3 Break Example

The training material describes the EAST-ADL dependability package illustrated by a brake example. The brake system has been modeled in several versions before. In this training we take a version including service brake and parking brake. It is not the intention of this presentation to model the brake system complete and correct. Intention is to illustrate the EAST-ADL principles for safety modeling with a realistic system. Therefore, some extensions in the safety modeling and analysis part are done compared to previous publications.

The training material can be downloaded from the SAFE website.

5.4 #4 Safety Goals Modeling, Safety Cases and Patterns in Safety-critical Development

Failure Modes and Effects Analysis – FMEA – is a methodology for analyzing potential reliability problems early in the development cycle where it is easier to take actions to overcome these issues, thereby enhancing reliability through design. FMEA is used to identify potential failure modes, determine their effect on the operation of the product, and identify actions to mitigate the failures. A crucial step is anticipating the potential failure modes of a product.

The training material can be downloaded from the SAFE website.

5.5 #5 Integrated Safety Workshop

The ISO 26262 Standard demands a set of specific engineering methods for the development of safety critical ECUs in the automobile industry. This workshop introduces the necessary fundamental safety methods, e.g. technical safety concept, safety analysis and ASIL software components. The main focus during the training lies on the topics system and software development. Practical exercises with an example ECU from the automobile industry will help understanding the theoretical aspects. The exercises include the use of typical engineering tools, such as PREEvision and DaVinci.

The training material is available at https://vector.com/vi_class_integrated_safety_en.html

5.6 #6 Functional Safety and Variability - Can they be brought together?

The webinar answers questions like: Can variability in functional safety related assets like hazard analysis, FTA, FMEA be treated in the same way as other artifacts (Requirements, models and source code)? Furthermore, challenges with respect to variable safety analyses, regulations, and reuse of certifications are discussed.

The training material can be downloaded from the SAFE website or accessed via https://in2soft.webex.com/in2soft/ldr.php?RCID=5824fed9e13dc6c2254b778782441a5c

6 References

[1] International Standards Organization, ISO 26262 Standard, “Road Vehicles - Functional Safety,” http://www.iso.org/, 2011.

[2] Vector Informatik GmbH, PREEvision, https://vector.com/vi_preevision_en.html

7 Acknowledgments

This document is based on the SAFE and SAFE-E projects. SAFE is in the framework of the 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. 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.