ARTEMIS Call 2011 Project
295311

VeTeSS

Verification and Testing to Support Functional Safety Standards

EXECUTIVE *summary*

VeTeSS is developing standardised tools and methods to verify the safety of automotive embedded systems. By providing objective data for safety qualification and certification, reliance on manual processes and expert opinion will be reduced as will development costs and time to market, even with the increasing complexity of embedded systems and software.

CONTRIBUTION *to SRA*

The VeTeSS project is an international collaboration between industry and academia. It is undertaking significant new research and innovation in tools and methods to generate quantitative data for safety verification and certification in the strategically important automotive market.

The end result will be a tool platform developed by European tool vendors and users to support an integrated approach to the verification of safety features throughout the supply chain. This will reduce the time taken to design, verify and certify the safety of these systems. Just as importantly, it will enable a platform-based approach that will ease revalidation and recertification.

The goal is to make complex embedded systems more cost-effective, hence improving safety, supporting greener transport and strengthening the European automotive position.

MARKET INNOVATION *& impact*

VeTeSS will have benefits for companies in all parts of the automotive supply chain, the European automotive industry as a whole, and other safety-related industries. It will provide opportunities for companies, especially SMEs and start-ups, to develop new products and services, including tools, training and consultancy for implementing safety standards.

The outputs from the project will have both commercial and practical benefits. The ability to succinctly and accurately communicate the safety properties and related value proposition of components and platforms will result in:

- Improved vehicle safety, quality and reliability.
- More predictable safety qualification and certification processes.
- Reduced time to market, despite new functions and the increasing complexity of embedded systems.
- Effective implementation of ISO 26262 and other safety standards.
- Greater supply chain flexibility.
- Faster development of electric and hybrid vehicles.

RELEVANCE & CONTRIBUTIONS *to Call Objectives*

VeTeSS is focused on the ARTEMIS sub-programme "System Design Methods and Tools" and the industrial priority "Methods and Processes For Safety-Relevant Embedded Systems". It will address the challenges of safety verification and certification caused by

increasingly complex embedded systems and software, combined in new and unexpected ways. The project will research methods for meeting the requirements of safety standards, such as ISO 26262 for automotive, leading to the development of a suitable tool platform. Thus enabling an integrated approach to the verification of safety features throughout the supply chain.

The project will develop tools and standard formats for communicating safety properties between all levels of the supply chain, and for the verification of these properties in systems constructed from heterogeneous components. This will include tools for simulation and modelling the embedded systems wich combine analogue and digital, hardware and software components.

The project will contribute to the ARTEMIS objectives by:

- Developing an integrated and standardised toolchain for safety verification and qualification allowing the interchange of data between all levels of the supply chain.
- Reducing the cost of system and component design because safety aspects can be verified more rapidly and earlier within the design process.
- Providing an objective, integrated and largely automated approach to the verification of safety-related functions to improve safety verification and system integration.
- Making the certification process more objective will speed revalidation and recertification by moving beyond the current ad-hoc and manual methods. This should also aid market acceptance of new technologies.

R&D INNOVATION *and technical excellence*

The VeTeSS project is investigating the verification methods and coverage metrics used to test the response of safety-relevant embedded systems to errors. This will include physical testing simulation and formal methods. We will also investigate the correlation of fault coverage in hardware against different levels of simulation , using data from physical testing and experience in the field. One of the key areas of research is the verification of the mechanisms commonly used to ensure robustness against common-cause failures. Where appropriate, new mechanisms or design guidelines will be defined.

The project will define a seamless, automated design flow from requirements to validation, integrating formal analysis, simulation and physical test. Based on this, a set of consistent tools and methods for safety analysis and testing across hardware and software, and analogue and digital domains will be provided. This will include methods and tools to automatically derive test procedures and test vectors to validate an architecture against the safety goals.

The development of quantitative methods and the use of objective data will support verification, certification and qualification. It will enable the communication and integration of the safety case at every level of the supply chain.

Characterising and isolating the effect of faults in each part of the system will lead to improved predictability and reusability. This should result in both enhanced safety and increased availability thereby improving the user's perception of the reliability and quality of the system.

PROJECT *partners*

Infineon, Volvo, AVL, TU Wien, exida, TWT, Barcelona Supercomputing Center, Synopsys, ikv++ technologies ag, idneo, virtual vehicle research and test center, QRTECH, Rapita Systems Ltd, Infineon, Politecnico di Torino, University of Oxford, Infineon, SP, NXP, Dizain PLM - EDA DESIGN - TRAINING Services, CRF Centro Ricerche Fiat, Fraunhofer IIS

ARTEMIS

www.artemis.eu

VeTeSS

PROJECT COORDINATOR
Steve Neill

INSTITUTION
Infineon Technologies UK Ltd

EMAIL
steve.neill@infineon.com

WEBSITE
http://vetess.eu

START
May 2012

DURATION
36 months

TOTAL INVESTMENT
€18.34 M

PARTICIPATING ORGANISATIONS
22

NUMBER OF COUNTRIES
8