ARTEMIS Call 2011 Project
295373

nSafeCer

Safety Certification of Software-Intensive Systems with Reusable Components

EXECUTIVE *summary*

European industry has a great potential to achieve a leading position in the growing global market of safety-relevant embedded systems, provided it can devise efficient and industrial-strength methods and processes for their development and certification. The three-year nSafeCer project targets increased efficiency and reduced time-to-market by composable safety certification of safety-relevant embedded systems.

CONTRIBUTION *to SRA*

nSafeCer builds on the ARTEMIS pilot project pSafeCer. Sharing the same overall goals, the concepts developed in pSafeCer are advanced into tangible industrial implementations of "project-ready", unified and seamlessly integrated solutions, and demonstrators of the proof of concepts. nSafeCer aims to support arguments for the reuse of safety certification and pre-qualified components within and across industrial domains. This addresses the overarching goal of the ARTEMIS JU strategy to overcome fragmentation in the embedded systems markets so as to increase the efficiency of technological development. Furthermore, it facilitates the establishment of a competitive market in the supply of embedded systems technologies and market access for SMEs as suppliers of reliable (pre-qualified) components, qualified tools and software (meeting the specific SME related target of ARTEMIS Innovation Environment). nSafeCer adds scientific objectives, including support for product lines and cross-domain certification and reuse.

MARKET INNOVATION *& impact*

nSafeCer brings about market innovation and impact in several respects, including:

- Innovation for process, component models, safety arguments and verification/validation, applicable to multiple domains, targeting cost-efficient reuse which leads to lighter, cheaper and faster certification of safety-related, software-intensive embedded real-time systems.
- Instantiation of methods and tools for automotive, avionics, aerospace, construction equipment and rail domains. Creation of integrated certification and development framework. Market impact through the development, verification and certification of tools, providing direction for methodology, reference architecture and prototype tool environment.
- Research aimed at extending to an open framework for new (other) domains and for certification for cross-domain use of components.
- Contribution to standards and regulations. Focus on software components qualified for certification. Impact on European industry, especially SMEs and technology providers, substantially opening up markets for niche components and increasing cost-effectiveness by allowing product lines/variants across multiple domains.
- Indirect effects, via adoption and dissemination of nSafeCer results in other projects and activities, including more attention in academic education and research.

RELEVANCE & CONTRIBUTIONS *to Call Objectives*

nSafeCer addresses the ARTEMIS industrial priorities, design, development and deployment of safe and secure electronics and software systems (i.e. software-intensive systems) with focus on reliable, composable systems:

- Design Methods and Tools by (1) providing methods and processes that support qualification and certification, (2) helping to establish integrated chains of European-sourced tool platforms, and (3) integrating/developing test, validation and verification tools to support compositional design.

- Reference Design and Architectures by (1) supporting composability of reliable systems (via constructive composition of large systems from pre-certified or qualified components and sub-systems), and (2) proving design for safety by means of architectures instantiated from generic platforms with an emphasis on support for modular and incremental qualification and certification, and the establishment of composable safety cases.

For ASP1 methods and processes for safety-relevant embedded systems, nSafeCer covers the following ARTEMIS objectives:

- Contribution to a European Reference Technology Platform (meta-models, methods, and tools for development of safety-relevant embedded systems) from the modular viewpoint, supported by European tool vendors, and complementing the CESAR Reference Technology Platform.
- A model-driven process for the compositional development of safety-relevant embedded systems (model-based compositional development, certification and qualification, safety argumentation, qualification, certification of compositionally designed systems and re-qualification after change)
- The establishment of analysis methodologies to support safety arguments and decision-making in an industrial context with a safety focus.

There is strong interaction with ASP5, computing environments for embedded systems, especially certifiable computing environments and how to enable the transition from vertically structured application markets to a horizontally structured embedded system market that supports cross-domain reuse.

R&D INNOVATION *and technical excellence*

In nSafeCer there is an extra focus to evaluate the suitability and effectiveness of the processes, methods and tools developed. To demonstrate the applicability of these outcomes for particular domains and across multiple domains, use cases have been chosen that cover automotive and construction equipment, avionics and aerospace, rail as well as cross-domain aspects. These use cases are representative of the challenges industry currently faces. Each of the selected use cases has facets concerning qualification, certification or verification. Work comprises the implementation of demonstrators as well as the demonstration and assessment of the ambition with respect to:.

- 15% reduction in development cycles requiring certification,
- 15% less effort and time needed for revalidation and recertification,
- cross-domain reusability,
- efficiency and effectiveness in development and certification by reducing system design costs by 15% while handling 25% more complexity.

It has been stated* that 20% of the components in a system tend to be reusable generic components, such as de-facto standard libraries functioning as extensions to the programming language. An additional 65% containing commonly recurring functionality presents potential for reuse. Assuming that efficient processes are in place to define, develop and maintain the reusable components, this represents an amazing potential of up to 85% savings on component development activities in a system development project. While SafeCer overall goals are therefore realistic, the suitability and effectiveness of the processes, methods and tools developed must be carefully evaluated and assessed.

* *H. Mili, F. Mili, A. Mili, Reusing Software: Issues and Research Directions, IEEE Transactions on Software Engineering, Vol. 21, No. 6, pp. 528 – 562, 1995.*

PROJECT *partners*

THALES · VOLVO · intecs · ResilTech · VITROCISET · akhela · CAF Power & Automation · AVL · VOLVO · ThalesAlenia Space · AdaCore · cr·ssc·ntr·l · magillem · ULMA Embedded Solutins · TTTech · gmv · Algorego · Bexen cardio · QuviQ · FBK Fondazione Bruno Kessler · virtual vehicle · SP · cea · Mälardalen University Sweden · Politécnica · Rīgas Tehniskā Universitāte · Mondragon Unibertsitatea · AIT Austrian Institute of Technology

ARTEMIS

www.artemis.eu

SafeCer

PROJECT COORDINATOR
Volvo

INSTITUTION
Advanced Technology & Research

EMAIL
safecer-coordinator@safecer.eu

WEBSITE
www.safecer.eu

START
April 2012

DURATION
36 months

TOTAL INVESTMENT
€15.3 M

PARTICIPATING ORGANISATIONS
29

NUMBER OF COUNTRIES
6