ARTEMIS Call 2010 Project
269265

pSafeCer

(pilot)Safety Certification of Software-Intensive Systems with Reusable Components

PROJECT *description*

SafeCer is an international research collaboration targeting increased efficiency and reduced time-to-market by composable certification of safety-relevant embedded systems. The two and a half-year pSafeCer (pilot SafeCer) project was started in 2011 and is funded partly by the ARTEMIS JU and partly by national funding.

RELEVANCE *to call*

Design Methods and Tools

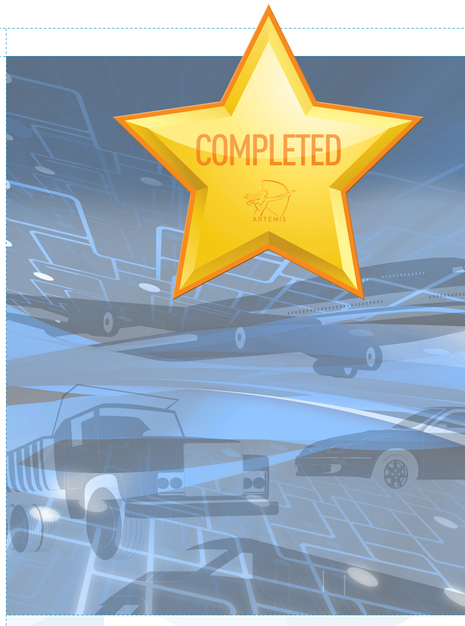
- Methods and processes supporting qualification and certification
- Contributing to the establishment of integrated chains of European-sourced tool platforms
- Integrating/developing test, validation and verification tools to support compositional design Reference Designs and Architectures
- Supporting composability of trustworthy systems
- Proving design for safety by means of architectures instantiated from generic platforms with emphasis put on support for modular and incremental qualification and certification, and the establishment of composable safety cases.

MARKET *innovation*

- Innovations 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.
- Instantiation of methods and tools for automotive, avionics, construction equipment, and rail domains. Creation of integrated certification and development framework. Impacts the development, verification, and certification tools, providing direction for methodology, reference architecture, and prototype tool environment.
- Research in the direction to extend 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. Impacts European industry, especially SMEs and technology providers, substantially opening up markets for niche components and increases cost-effectiveness
- Indirect effects, via adoption and dissemination of pSafeCer results in other projects and activities, including increased attention in academic education and research.

TECHNICAL *innovation*

Examples of concepts with technical excellence within the scope of pSafeCer:
For a number of years, work has progressed on Component-Based Development (CBD) approaches to improve both the reuse and maintainability of systems. The concept of a contract has been used. During system composition contracts are compared to determine compatibility. The majority of this work has concentrated on the functional properties of systems with some focus timing properties. However, much less work has considered how CBD can be applied to other non-functional properties. Dependability properties must be captured in the contract for effective CBD of safety-relevant, software-intensive-, embedded systems. In recent years, modular safety arguments and safety argument contracts have been developed to support the needs of incremental certification, but in a relatively informal way. Our aim is to enhance existing CBD frameworks by extending them to include dependability aspects so that the design and the certification of systems can be addressed together with a manageable amount of work.



SafeCer

PROJECT COORDINATOR	START
Volvo	April 2011
INSTITUTION	DURATION
Advanced Technology & Research	30 months
EMAIL	TOTAL INVESTMENT
safecer-coordinator@safecer.eu	€10.4 M
WEBSITE	PARTICIPATING ORGANISATIONS
www.safecer.eu	23
	NUMBER OF COUNTRIES
	6