ARTEMIS Call 2010 Project
269265

pSafeCer

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

EXECUTIVE *summary*

SafeCer is an international research collaboration targeting increased efficiency and reduced time-to-market by the composable certification of safety-relevant embedded systems. The two and a half-year pSafeCer (pilot SafeCer) project was started in April 2011 and is funded partly by the ARTEMIS Joint Undertaking (the European Public-Private Partnership for Advanced Research and Technology for EMbedded Intelligence and Systems) and partly by national funding.

CONTRIBUTION *to SRA*

pSafeCer 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 while facilitate the establishment of a competitive market in the supply of embedded systems technologies and provide market access for SMEs as suppliers of trustworthy (pre-qualified) components, qualified tools and software (meeting specific SME related target of ARTEMIS Innovation Environment). pSafeCer applies mainly existing/adapted methods and techniques by integrating them via interfaces and transformations, thereby clearly meeting the ARTEMIS JU over-arching objective of closing the design productivity gap between potential and capability.

MARKET INNOVATION *& impact*

pSafeCer brings about market innovation and impact in several respects, for instance:

- 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 of safety-related, software-intensive, embedded real-time systems.
- Instantiation of methods and tools for automotive, avionics, construction equipment and rail domains. Creation of integrated certification and development framework. Impacts the markets for the development, verification, and certification of 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 by allowing product lines/variants across multiple domains
- Indirect effects, via adoption and dissemination of pSafeCer results in other projects and activities, including increased attention in academic education and research.

RELEVANCE & CONTRIBUTIONS *to Call 2010 Objectives*

pSafeCer 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 trustworth, 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 Designs and Architectures by (1) supporting composability

of trustworthy 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, pSafeCer covers the following Artemis JU objectives:

- Contribution to a European Standard Reference Technology Platform (meta-models, methods, and tools for development of safety-relevant embedded systems) from the modular view point, 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 or recertification after change), and
- To establish analysis methodologies to support safety arguments and decision making in industrial contexts, with particular regard to safety properties.

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

R&D INNOVATION *and technical excellence*

The main pSafeCer challenges are to reduce the cost of qualification, certification and verification and to provide a framework for compositional development and certification of systems. The examples below demonstrate 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 contract comparison has been used to determine compatibility during system composition. The majority of this work has concentrated on the functional properties of systems along with some focus on timing properties, e.g. based on Eiffel, reliability guarantees and Time-Triggered Protocols. However, much less work has considered how CBD can be applied to other non-functional properties, including such dependability properties as safety, reliability and availability. 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. This would allow reasoning about the design and safety aspects of parts of the systems in relative isolation and allow their interfaces and emergent behavior to be dealt with afterwards in a more structured manner without having to revert to current holistic practices. This would additionally facilitate a more automated (and hence quicker) modular safety argument approach.

PROJECT *partners*

THALES
VOLVO
DELPHI
intecs the Brainware company
LDZ
VOLVO
akhela
CAF Power & Automation
AVL
AdaCore The GNAT Pro Company
cr-ss-c-ntr-l
magillem DESIGN SERVICES
ULMA
Embedded Solutins TTTech
Algorego
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
MÄLARDALEN UNIVERSITY SWEDEN
SP your Science Partner
RĪGAS TEHNISKĀ UNIVERSITĀTE
virtual vehicle
POLITÉCNICA
FONDAZIONE BRUNO KESSLER
MONDRAGON UNIBERTSITATEA

ARTEMIS

www.artemis.eu

SafeCer — Safety Certification of Software-Intensive Systems with Reusable Components

PROJECT COORDINATOR
Volvo

INSTITUTION
Advanced Technology & Research

EMAIL
safecer-coordinator@safecer.eu

WEBSITE
www.safecer.eu

START
April 2011

DURATION
30 months

TOTAL INVESTMENT
€10.4 M

PARTICIPATING ORGANISATIONS
23

NUMBER OF COUNTRIES
6