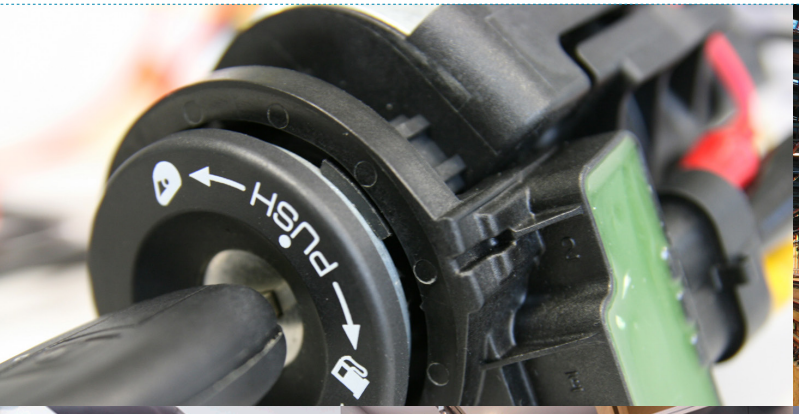
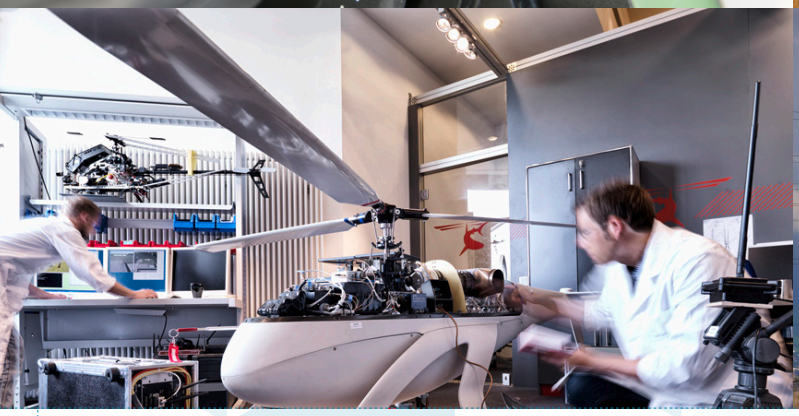
ARTEMIS Call 2011 Project
295354

SESAMO

Security and Safety Modelling





EXECUTIVE *summary*

The SESAMO project addresses the root causes of problems arising with the convergence of safety and security in embedded systems at architectural level. A component-oriented design methodology based upon model-driven technology will address the safety and security aspects of networked embedded systems in multiple domains (e.g., avionics, transportation, industry control, mobile medical).

CONTRIBUTION *to SRA*

SESAMO contributes directly to the "Design methods and tools" Industrial Priority by establishing integrated system design methods and chains of tools.

The approach is entirely model-based, in terms of both tools and processes. The developed tools will work from system level (e.g. using SysML) and cover the life cycle through to model-based verification and validation. The compositional design will follow the SESAMO approach of property (safety and security) preservation guaranteed by construction, thereby also contributing to the "Reference designs and architectures" Industrial Priority. The architectural approaches developed in SESAMO will also support design for safety and security with the certification and safety case argumentation processes.

MARKET INNOVATION *& impact*

All the technological results are embedded in a process-related, methodological context, accompanied by guidelines for using them within the SESAMO design process. The introduction of SESAMO is expected to considerably diminish safety and security related damage to products that rely on embedded IT systems. The introduction of a disciplined analysis and design process together with component and tool support is known to have a positive impact on costs; SESAMO is expected to produce a 15% reduction in development cycles and the re-validation and recertification of systems after changes. The building blocks developed in SESAMO are intended to be reusable across domains and, if reused within a methodology-driven process supported by SESAMO tools, less effort will be required to obtain systems with verifiable safety and security related characteristics.

RELEVANCE & CONTRIBUTIONS *to Call Objectives*

The key elements of the SESAMO approach are:

- a methodology to reduce interdependencies between safety and security mechanisms and to jointly safeguard their properties
- constructive elements for the implementation of safe and secure systems
- procedures for the integrated analysis of safety and security

- an overall design methodology and tool-chain utilising the constructive elements
- integrated analysis procedures to ensure that safety and security are intrinsic characteristics of the system
- use cases in five domains: automotive, aerospace, medicine, metropolitan rail transport, public energy utilities / process control.

SESAMO contributes to more than one ARTEMIS sub-programme:

- **ASP1** - Methods and processes for safety-relevant embedded systems: by providing a model-driven process for the compositional development of safety and security critical systems and by developing analysis methodologies that consider the joint constraints of safety and security in system development and their interaction, in particular the trade-off between various conflicting constraints.
- **ASP6** - ES for Security and Critical Infrastructures Protection: by emphasising a model-based compositional common conceptual framework for safety and (especially) security requirements and policies that permit not only dynamic reformulation of policies in response to system reconfigurations, but also the integrated management of safety certification artefacts and security accreditation evidence.
- **ASP5** - Computing platforms for embedded systems: through support for platform-independent compositional development and the construction of a tool chain enabling system-level conservation and predictability of appropriate levels of safety and security.
- **ASP2** - ES for healthcare systems: through its use case in the domain of mobile medical systems in the context of Ambient Assisted Living, providing support for telemedicine and enabling therapy at home.

R&D INNOVATION *and technical excellence*

1. Definition of generic safety and security process, which is based on the idea of establishing points of contact between parallel safety and security lifecycle activities.
2. Development of a method for constructing security-informed safety cases, based on extending a structured safety case with explicit claims, arguments and evidence about security.
3. Analysis of selected safety and security building blocks. Study of synergies and trade-offs between safety and security properties of these blocks.
4. Integration of various tools related to safety and security processes or analyses. The tools include ASCE, CHESS, K3B, IMACT, medini analyse, PIA, PikeOS/CODEO, Simulink and others.
5. Validation of the generic process and the tool-chains on industrial use cases:
   - integrated modular avionics gateway,
   - motor control in automotive and industrial environments,
   - car infotainment system,
   - safe & secure communication in railway and medical applications,
   - smart-grid security, security of SCADA systems in oil and gas refineries.
6. Standardisation activities: AUTOSAR standard now includes SESAMO-based safety extensions; interactions with standardization groups such as IEC TC65 AHG1 (safety & security in industrial automation).
7. Introduction of "Decentralized Label Mode" extension for C language that allows automated checking of information flow security.

PROJECT *partners*

Danmarks Tekniske Universitet, DTU, GM, ADELARD, intecs the Brainware company, SYSGO EMBEDDING INNOVATIONS, UniControls, Czech Technical University in Prague, City University London, Sapienza Università di Roma, ftw Creating Communication Technologies, Infineon technologies, AIRBUS DEFENCE & SPACE, eesy-id, IIT Istituto di Informatica e Telematica, ikv, SYSGO EMBEDDING INNOVATIONS, EDF, PSA PEUGEOT CITROËN, SIEMENS, akhela

ARTEMIS

www.artemis.eu

SESAMO Security and Safety Modelling

PROJECT COORDINATOR
Silvia Mazzini

INSTITUTION
Intecs S.p.a.

EMAIL
silvia.mazzini@intecs.it

WEBSITE
http://sesamo-project.eu

START
May 2012

DURATION
36 months

TOTAL INVESTMENT
€12 M

PARTICIPATING ORGANISATIONS
20

NUMBER OF COUNTRIES
8