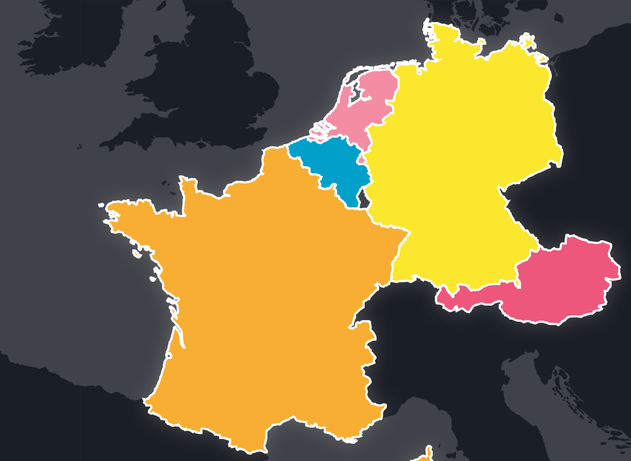
EURO-MILS

Secure European virtualisation for trustworthy applications in critical domains.



Contact:

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55 – 0
Fax: +43 4242 233 55 – 77
E-mail: coordination@euromils.eu
Web: www.euromils.eu

Technical Leader
Dr. Sergey Tverdyshev
SYSGO AG
Am Pfaffenstein 14
55270 Klein-Winternheim
Germany
Tel.: +49 6136 9948 – 788
Fax: +49 6136 9948 – 10
E-mail: sergey.tverdyshev@sysgo.com

Consortium:

The EURO-MILS consortium consists of six leading European industrial companies, one leading European Research Company, four European SMEs, and three European universities. These fourteen project partners from five European Countries (Austria, Germany, Belgium, France, and Netherlands) form a complete chain stretching from basic research and service design, via applied research, independent assessment, up to end-user oriented service providers.

Technikon Forschungs- und Planungsgesellschaft mbH (Austria, Villach)

SYSGO AG (Germany, Klein-Winternheim)

Deutsches Forschungszentrum für künstliche Intelligenz GmbH (Germany, Kaiserslautern)

Universiteit Gent (Belgium, Gent)

Airbus (France, Toulouse)

EADS Deutschland GmbH - Innovation Works (Germany, Ottobrunn)

OpenSynergy GmbH (Germany, Berlin)

European Aeronatic Defence and Space Company EADS France SAS (France, Paris)

University of Paris-Sud 11 / LRI (France, Orsay)

Thales Communications & Security SA (France, Colombes)

Open Universiteit Nederland (Netherlands, Heerlen)

T-Systems International GmbH (Germany, Bonn)

SYSGO SAS (France, Le Pecq)

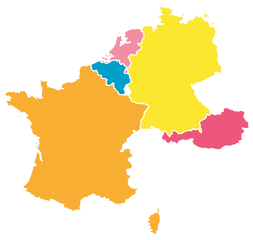
JEMM Research SARL (France, Mareil Marly)

Project number: **318353**
Project website: **www.euromils.eu**
Project start: **October 1, 2012**
Project duration: **3 years**
Total costs: **EUR 8.447.558,-**
EC contribution: **EUR 6.000.000,-**

The project is co-financed by the European Commission (under the Seventh Framework Programme).

Mission of EURO-MILS:

EURO-MILS: Secure European virtualisation for trustworthy applications in critical domains. The mission of the **EURO-MILS** project is to develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods.



Motivation:

Based on embedded systems, cyber-physical networks are part of our society, and gain wider spread and importance. Next generations of aircraft and cars will be tightly interconnected with each other, with the internet, and other infrastructures. The same holds for many industries and areas of our life such as healthcare, energy, finance, and mobile. Non-secured network devices can be hacked and exploited to affect their functionality, change control, or steal specific information. In order to provide secure and safe trustworthiness and exclude devastating, unauthorized use of critical systems, to control access in an organized and certifiable fashion, the EURO-MILS project is introducing into the European trustworthy ICT landscape a verified and design-validated MILS platform: a small virtualisation platform that offers the secure decomposition of complex embedded systems into independent components.

As the aim is ambitious, our work is put onto very strong foundations:

- The MILS approach in generally has already been tried and tested in the US.
- The separation kernel to be used in the **EURO-MILS** project has undergone avionic certification and is deployed in commercial aircrafts.
- **EURO-MILS** consortium members have high industry expertise and experience in computer-supported verification ("formal methods") and assurance validation ("Common Criteria" certification).

Objectives:

To address the problem of trustworthiness, we introduce the certified MILS platform into the ecosystem of European trustworthy ICT. The **EURO-MILS** platform will

- fit the technological, business, and legal environments
- generate trust by design – the **EURO-MILS** platform will allow composition of complex trustworthy systems following the MILS approach
- generate trust by high-assurance – the **EURO-MILS** platform will go through a computer-supported verification ("formal methods") as well as a strong human validation ("Common Criteria" security standard certification)
- be strongly aligned with European industrial needs and two prototypes in avionics and automotive will be co-developed to the MILS platform.

Key concepts: MILS and embedded virtualisation

Multiple Independent Levels of Security (MILS) is a high-assurance security architecture based on the concepts of resources separation and controlled information flow. The cornerstone of the architecture and the MILS platform is a separation mechanism that encapsulates trusted and untrusted applications in compartments. It reduces mutual dependencies to communications over channels explicitly defined by policies. This key component has to be non-bypassable, evaluatable, always invoked, and tamperproof (NEAT).

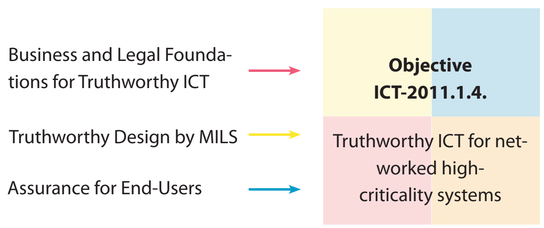
A powerful way to implement a MILS architecture is using embedded virtualisation techniques, where multiple virtual machines can run simultaneously on the same processor. To be relevant to the objectives of the project, the embedded virtualisation solution must be sufficiently safe and secure.

Overall Strategy:

The strategy of the **EURO-MILS** project is built on three activities:

- The first activity provides solid business, legal, and social-legal foundations for the developed technology.
- The second activity provides trustworthiness by design employing the MILS concept.
- The third activity significantly enhances the end-users' trust by providing them high-assurance guarantees based on rigorous cross-European security certification.

The Figure 1 provides a high-level representation of the project strategy.



Technical Approach:

The EURO-MILS project has three technical activity lines and one management activity line. Every activity line has its own objective, goals, work packages, and interfaces to other activity lines.

Activity A1 "Business and Legal Foundations for Trustworthy ICT"
provides a solid foundation for the project that consists of industrial requirements, certification requirements, as well as business impacts and legal implications.

Activity A2 "Trustworthy Design by MILS"
focuses on developing MILS technology as the base for trustworthy designs and its applications on the use cases from avionics and automotive defined in A1, including the developments of an avionics and automotive prototype.

Activity A3 "Assurance for End-Users"
focuses on assurance techniques for end users comprising certification requirements from A2, usage of the Common Criteria standard for high-assurance security evaluation including formal methods in a CC conformant form, and providing a cross-European high-assurance security evaluation methodology.

Activity A4 "Programme Management and Dissemination"
wraps the project by focusing on standardisation, dissemination and management activities.

Project Results and Innovation:

The main outcomes of the EURO-MILS project are to develop market relevant technologies and concepts for virtualisation of heterogeneous (embedded) systems and the formal verification for those systems as part of rigorous cross-European security certification. These outcomes can be further broken down as follows:

Outcome 1. Trustworthy foundations by the MILS approach, architecture, and applications
Provide Trustworthy ICT for high critical automotive and avionics domains by using the MILS approach. The base of such ICT is MILS architectures for compositional security and compositional assurance.

Outcome 2. MILS platform and its usage
Provide trustworthiness by design, by development and usage of a MILS platform based on virtualisation technique. The virtualisation platform will provide a framework to develop secure and safe products as well as to integrate domain specific functionality and components, e.g. functionality in heterogeneous networks, IMA compatibility for avionics, heterogeneous virtualisation (CPU, network controllers, other I/O devices such as storage or GPUs) for automotive, building running demonstrators and assessing them from security view.

Outcome 3. High Assurance
Provide trustworthiness by security evaluation and certification using the "Common Criteria for IT Security Evaluations" standard (http://www.commoncriteriaportal.org). To achieve high assurance in the trustworthiness of the MILS platform, a high evaluation assurance level (EAL) is chosen for the evaluation. Develop a pragmatic approach to the use of formal methods in the scope of a certification as the ultimate means to gain end-user trust. Develop an innovative approach for compositional security assurance. Provide a harmonized approach for high-assurance vulnerability analysis.

Outcome 4. European MILS virtualisation platform
Offer European market participants the opportunity to use a certified virtualisation made in Europe – as virtualisation is often used for containment of otherwise insecure or mix-criticality systems (e.g. think of systems deployed in heterogeneous networks), having a locally developed virtualisation solution is also of European strategic interest (it is best illustrated by the Stuxnet attacks, e.g. in Iran).

Outcome 5. True cross European certification
Establish a precedent for a cross-European usage of the CC for high EALs in the domain of separation kernels. Recent developments, e.g. cooperation between French and German authorities (BSI and ANSSI, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/BSI-ANSSI_050210.html, http://www.ssi.gouv.fr/site_article175.html) have opened the door for a European approach. **EURO-MILS** aims at building a generic process that will be generally acceptable for national certification authorities in Europe.