Publishable Summary

Project number:	318353
Project acronym:	EURO-MILS
Project title:	EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains
Start date of the project:	1st October, 2012
Duration:	36 months
Programme:	FP7/2007-2013

Date of the reference Annex I:	28.06.2012
Periodic report:	Publishable Summary (as part of D42.2 "1st periodic report according to EC regulations of the model contract")
Period covered:	01.10.2012 – 30.09.2013
Activities contributing:	All
Due date:	September 2013 - M12
Actual submission date:	8th January, 2014 – V1.1

Project Coordinator:	Dr. Klaus-Michael Koch Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@euromils.eu
Project website:	www.euromils.eu

Chapter 1 Publishable Summary

Project name: **EURO-MILS**
Grant Agreement: **318353**
Project website: http://www.euromils.eu/
Contact: coordination@euromils.eu

Start date: 1st October 2012
Duration: 36 months

Mission of EURO-MILS: *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.*

The EURO-MILS Project: The main goals 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 goals can be further broken down as follows:

- **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.
- **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 prototypes and assessing them from security view.
- **High Assurance:** Provide trustworthiness by security evaluation and certification using the “Common Criteria for IT Security Evaluations” (CC) standard. 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.
- **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, having a locally developed virtualisation solution is also of European strategic interest.
- **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) 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.

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 communication. 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 placed onto very strong foundations:

- The MILS approach in general 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 (CC certification).

Objectives & Overall Strategy: 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 (CC 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.

The strategy of the EURO-MILS project is built on four activities (A1-A4):

- The first activity “*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.
- The second activity “*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.
- The third activity “*Assurance for End-Users*” focuses on assurance techniques for end users comprising certification requirements from A2, usage of the CC standard for high-assurance security evaluation including formal methods, and providing a cross-European high-assurance security evaluation methodology.
- Activity four “*Programme Management and Dissemination*” wraps the project by focusing on standardisation, dissemination and management activities.

The work plan of EURO-MILS encompasses four independently managed activities and eleven tightly integrated work packages.

Description of the work performed and results in the first project period

The EURO-MILS project started in October 2012 and is set to run for 36 months. During the first project phase, corresponding to the first project year, the focus was placed on the analysis of industrial and certification requirements. All work packages, apart from WP 33 (WP22 started in M12) that has not yet started, initiated work and produced altogether 9 deliverables (including this first Periodic Report) throughout the first project year.

At the beginning, major effort was put into the successful launch of the project. The major goal was to establish a sound basis for a good and fruitful cooperation of the project partners towards the research objectives. We managed to develop collaboration while creating a large number of publications and presentations documenting ideas that we can leverage and extend in subsequent years. This has been achieved by strong leadership and by optimizing the organisation and infrastructures. All relevant management components on contractual, financial, legal, technical, administrative and ethical topics were created and provided as well as catching upcoming obstacles well ahead of time. Furthermore, a public project website and the internal IT communication infrastructure were implemented.

The progress achieved by all work packages within the first project year is in line with the initial plan and can be summarized as follows.

The objective of ***WP11 (Industrial Requirements)*** is to collect a set of industrial requirements for virtualisation of resources. A specified set of requirements helps identifying system components, interfaces and responsibilities between components. These requirements will help to define a high-level architecture for the prototypes developed in EURO-MILS project.

One of the focus areas of deliverable D11.1 is to clearly define those requirements, characteristics, and the scope of the virtualisation platform, which is to provide assurance, integrity, and security as the base for the trustworthiness for critical embedded systems with scarce resources. Moreover, the document should ease formal specifications. The delivered document is organized in the following way:

- In Chapter 1, a classification of those requirements is proposed to help the developers and the CC evaluators to keep track of the separation kernel requirements for different MILS use cases. Requirements are described as system components, with indications about their scopes of responsibility.
- Chapters 2 and 3 respectively collect requirements in the avionics and automotive domains based on existing and future uses cases where virtualisation is used. The localisation in architecture, the environment, the security and functional requirements, are described with a focus on separation kernel requirements suitable to run on very restricted modern hardware platform with an embedded RTOS like PikeOS and several AUTOSAR/ARINC applications on a platform with typically 1 GB RAM with instant boot support. A high level description of system architectures is provided as well.
- The two usage domains automotive and avionics provide the base to interoperability of the developed architecture in Chapter 4.

Based on an analysis of available assurance techniques, a security target (ST) for PikeOS as a MILS separation kernel has been prepared within ***WP12 (Certification Requirements)***. The ST is intended to be evaluated in accordance to Common Criteria both in France and in Germany. The assurance level chosen was EAL 5+ with extensions that support the robust and reliable separation of partitions.

The objective of ***WP13 (Business, Legal and Social Acceptance)*** is to analyse the business impact of such a trustworthy technology in markets adjacent to the core automotive and avionics targets. It studies the potential of the EURO-MILS platform in markets such as healthcare, finance, smarthome, mobile communication, etc. During the first period, we worked first on the common definition of trustworthiness, virtualization, security, and safety. They are the starting point of our work. Defining the project terminology and glossary allows members of the EURO-MILS project to discover and to reduce potential ambiguities and to ensure a consistent, complete and common understanding of the terms. A document is published internally and will be included in WP13 final deliverable (D1.3.1 MILS for business, legal and social domains) in month 36. We also contacted an informal industry panel, made up of professionals in different industries where the EURO-MILS technology could make sense (medical, finance, energy…). We have contacted 245 professionals, received 72 direct answers and made 39 interviews on the following themes: security and safety, virtualisation and partitioning, certification and user assurance. To guide the interviews, we created a questionnaire. The idea behind the questionnaire is to understand the value of the EURO-MILS deliverables in adjacent markets. We are starting now the process of analysing the answers to setup guidelines to the project. We are also preparing an end-user survey to understand how end-users valuate security and safety in the products they buy.

The first scope of ***WP21 (MILS Architecture)*** is to establish a common understanding between partners on what a MILS architecture means and what are its components given the absence of a standardized view. Then it serves to define a common architecture for the prototypes. A workshop on PikeOS was held in Mainz in cooperation with WP22 (see WP22). As first deliverable (D21.1), by many teleconferences, svn repository interactions, and a two-day workshop at AOS in Toulouse, the partners have developed a common view on “MILS architecture” consisting of an introduction to the MILS background coming from both security and safety, a common view of a MILS architecture template that can be applied to individual MILS systems instantiating the template and a set of definitions, defining, for example, MILS components, resources, security policies, partitions. One of the insights gained was that software and hardware components are best treated as having equal status, thus a chapter on components lists both software (separation kernel, generic device abstraction component, console system component, network system component, file system component, audit system component, generic application component) and hardware components (processing unit, memory management units, input/output memory management units, I/O sharing, timers). A software component treated in much detail is the separation kernel, where the virtualisation provided by a separation kernel is distinguished from the virtualisation provided by other types of hypervisors. The deliverable concludes with a discussion on how components depend on each other, and to what extent a set of secure design principles established by Saltzer and Schroeder is applicable to MILS architectures. Partners also received and acted upon some feedback from Rance DeLong of Open Group who viewed parts of an early version of the text. D21.1 has been delivered on time at M12. Other ongoing work in WP21 is on defining the architecture instantiations generated from applying the architecture template to the two prototypes, for this a first framework for D21.2 “MILS architecture for avionics and automotive” has been set up. Partners also did first analyses on how to support Common Criteria compositional certifications of the prototype architecture, e.g. by focusing on the security services and security policies provided by components and how one component provides security services needed by another component. The formal model of an integrated MILS system has started by defining a framework for trusted components where a trusted component acts as intermediate (e.g. filter of a firewall) between two other components. For this, the “purge” function of the traditional Rushby non-interference model has been extended by a new purge function, and the security of the new purge function has been proven in the integrated MILS system model.

WP22’s (MILS Components) goal is to research, design and implement the infrastructure defined in WP21, which will be required by the automotive and avionics prototypes of WP23. This means that PikeOS must be ported to the chosen hardware platforms and extended with support for hardware-based I/O virtualisation. We started with a well-attended (20+ participants from 11 partners) workshop organised by SYSGO in Mainz (Germany) on the PikeOS separation kernel. It covered all aspects of the development process, from setting up the basic environment to finding a security issue in a device driver. The first step into getting PikeOS to run on a new platform consists of creating a so-called Platform Support Package (PSP). This package enables the PikeOS separation kernel to use a number of basic facilities of the underlying hardware, such as a timer, interrupt vectors and memory mapping. This work is well underway, but the results have been delayed from M12 to M13, primarily due to issues of non-delivery by project-external hardware suppliers. Once the platforms were decided upon in WP12, in parallel with the aforementioned work we also started investigating the I/O virtualisation capabilities of the selected hardware. We have created a comparative overview of these properties, which we will use in the coming period to design and implement a generic I/O virtualisation interface and infrastructure for PikeOS.

WP23 (Prototype Integration) has officially started in Month 12. First preparation work and the kick-off of that WP already took place. Considering package AVA_VAN.5 in the context of CC evaluation, and provided inputs on PikeOS architecture, we have verified that its internal vulnerability assessment tool (ramooflax) could be considered for performing some tests within AVA_VAN.5, targeting for example specific kernel/userland memory manipulation patterns (time-to-check-to-time-of-use) that are potential vulnerabilities.

The most critical automotive use cases described in chapter 3.1 of EURO-MILS_D11.1-Industrial-Requirements are related to connectivity to the external world, such as Internet and cloud. We started to develop a testbed to cover all connectivity interfaces of the automotive prototype. This shall be used as an input for the certification activities in EURO-MILS.

During the first year of the project, the main work within ***WP31 (Assurance by Formal Methods)*** has been towards a generic model of Separation Kernels and the demonstration that parts of PikeOS are instantiations of this model. At the end of the first period, such a generic model is described in Deliverable D31.1 and one system call (IPC) of PikeOS is proved to be an instantiation of this model. A paper is also being prepared describing this result. This new model provides a model of separation with interrupts and control, two aspects needed in practical applications like PikeOS. These aspects were missing in all existing models. To achieve this result, a deeper understanding of separation properties was necessary. A thorough literature study shows that two formulations dominate. The Greve, Wilding, and Vanfleet model and the model proposed by Rushby. A paper is currently being prepared describing the conclusion of this comparison of information flow policies. Beside a comparison between the two main models, a conclusion of the literature study was that out-of-the-box models were not directly applicable to PikeOS and a new model was needed.

Within ***WP32 (Common Criteria Security Evaluation)*** the evaluation of the CC assurance class ASE was completed (task 3.2.1) apart from potential comments by the German certification body. Also, the evaluation of further CC assurance classes could be prepared.

For ***WP41 (Dissemination, Standardisation and Exploitation)***, a robust IT infrastructure (web site, SVN repository including web access, mailing lists including mailing list archives) was established as early as M02 (D41.1; http://www.euromils.eu/) and regularly updated since. EURO-MILS has also been advertised by web pages, press releases and internal partners' newsletters. Hardcopies of the EURO-MILS project flyers have been distributed by partners at various events. The project is visible on twitter and LinkedIn. A newsletter has been published and distributed, amongst others, to industrial partners contacted in the context of WP13. The project is represented in an EU year book. Dissemination activities are announced via http://www.euromils.eu/index.php/news. In terms of dissemination management, to ease communication on publications, a mailing list for publication proposals has been established. A list of dissemination activities has been compiled and updated periodically. The deliverable D41.2 "Initial report on dissemination, standardisation and exploitation" [D41.2] has been compiled and lists 4 scientific publications, 10 participations in exhibitions and conferences, 4 upcoming dissemination activities, and 9 activities summarised as "web, flyers, and press releases and articles in the popular press". Dissemination activities have focused on relevant forums, e.g. EURO-MILS was present with two talks at the ICCC (International Common Criteria Conference). Standardisation activities (Section 2.2 of [D41.2]) have included following AUTOSAR, GenIVI in automotive, RTCA SC216 on avionic security, the MILS Open Group Real-Time Embedded Systems group, including two presentations of EURO-MILS in that context. EURO-MILS itself is designed to provide input to standardisation by having a protection profile as well as a high-EAL-level assurance methodology for vulnerability analysis and formal methods in Europe as deliverable. Concerning exploitation, EADS IW works closely with AOS on making sure that the EURO-MILS work can be used in future AOS products and planes. Board support for the boards used in EURO-MILS is going into the PikeOS product. The security target has already been presented to the national certification bodies in Germany and France (BSI and ANSSI) and has been used for the ASE work unit of a Common Criteria evaluation. As a measure of exploitation management, partners have been asked to identify any potential Intellectual Property rights issues.

WP42 (Project Management & Activity Coordination) was responsible for the effective organization of the project and covered all relevant management components. Some of the main achievements so far have been: the organization of meetings (e.g. Kick-Off and GA Meeting), the implementation of monthly EB Telcos, monitoring of the work plan (Quarterly Management Reporting), supporting partners in everyday issues (handling day2day requests), etc.

Expected final results and their potential impact and use

The technology and the framework that is developed within the EURO-MILS project aims at providing a technical infrastructure for building generic and secure virtualisation solutions while providing high guarantees of the claimed functionalities. The emerging technology of trustworthy virtualisation solutions is a rapidly growing market. Today, virtualisation has left mainframes and servers, spread across home and office computers, and has reached concurrent embedded systems. Moreover, analyses (e.g. Balacco et al., “Virtualization for Mobile & Embedded Systems”) show that the trend goes that the hypervisor will become the operating system of the future, and the guest OS’es will be reduced to user level run time systems managing the processes, and designed to run on a hypervisor, e.g. current research by Microsoft on Hyper-V. To be at the forefront, it is important to invest in embedded virtualisation, as this will give Europe a competitive advantage in future OS’es too. The impact of security and safety of these systems will have a significant influence on how fast European companies will reach the market. Furthermore, as several server virtualisation solutions were initially developed in Europe too, EURO-MILS is also continuing a tradition. The MILS approach not only can lower costs by protecting computing systems from costly malicious security attacks and accidental errors, it also will enable and drive entirely new business models. In recent years, the economic impact of security attacks (e.g. attacks of virus Stuxnet on Iranian SCADA systems) has shown that we need a more setup-friendly and secure environment to run applications provided by third parties. EURO-MILS has a key technology for enabling new business models with a high economic impact, e.g. running trusted, non-trusted, and legacy software tightly integrated under control of a certified MILS platform. The project aims at empowering the European software and specifically virtualisation and integration business and its competitiveness not only by supporting a highly innovative technology, but also by bringing together the essential European players, be it research, industry or SME.

The EURO-MILS Consortium: The consortium comprises 14 partners from 5 different countries: reputable universities and recognised companies from five European Union member states (Austria, Netherlands, Germany, France, and Belgium). All partners are experts in their field. This partnership of experienced professionals is anticipated to result in a successful project.

Figure 1: The EURO-MILS Consortium

EURO-MILS Disclaimer: Public information is marked with the following EURO-MILS project disclaimer: "*The EURO-MILS project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT – 318353.*"

Project Public Website: The official EURO-MILS project website is available at the following link: http://www.euromils.eu