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:	16.09.2014, V2
Periodic report:	Publishable Summary (as part of D42.3 “2nd periodic report according to EC regulations of the model contract”)
Period covered:	01.10.2013 – 30.09.2014
Activities contributing:	All
Due date:	September 2014 – M24
Actual submission date:	17th December 2014 (V2)

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.

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.

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 independently managed activities (A1-A4) and eleven tightly integrated work packages (WP):

- 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.

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

The EURO-MILS project started in October 2012 and is set to run for 36 months. During the second project phase, corresponding to the second project year (October 2013-September 2014), the focus was to initiate and support works on all project topics including defining MILS architectures and components, implementing defined elements and implementing execution environment, formal modelling, common criteria evaluation as well as creating a base for the out-of-the-project MILS community and MILS standardisation. The progress achieved by all work packages within the second project year is in line with the initial plan and can be summarized as follows.

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. Based on the security target written in the in the previous reporting period a draft of a protection profile (PP) for MILS kernel has been prepared. The PP is referenced in the ST. Therefore, it’s assurance level is EAL 5+ as well. It has been submitted to both the French and the German CC certification authorities (ANSSI and BSI).

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, smart home, 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. During the second period, we continued to analyse the Industry panel answers and documented them into the WP13 deliverable. We also ran the end-user survey in six geographies all across Europe including Germany, United Kingdom, France, Spain, Italy, and Benelux. This consumer survey theme was about analyzing the social value of secure products and understanding the user assurance mechanisms. We received more than 500 answers and started the analysis. Finally we published a draft of the final document to the European Commission.

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.

The next step of WP21 was to apply the MILS architectural template to the EURO-MILS demonstrators in automotive and avionics, which means that components were located with regards to the EURO-MILS architectural template (e.g. MILS system, MILS platform and MILS core). Moreover WP11 requirements have been assigned to individual components. This work has been documented in D21.2 "MILS architecture for avionics and automotive" (delivered on time at M15). Based on a comparison worked out by the subcontractor Fraunhofer IESE, on the two prevalent Common Criteria methods for Compositional Certification, Composed Assurance Package (CAP), and Composite Product Evaluation according to CCDB (CEP), with regards to obligations for development, functional and vulnerability testing, for several components, we decomposed the avionics demonstrator into component-level requirements and specified CC artefacts for them. Based on our experience with T2.1.1 and WP31, we agreed that the most interesting security property to formally model was non-interference. An approach was developed that allows the expression of local security properties of applications and show that they remain valid within a system with a separation kernel. The separation properties of the kernel required are similar to those established in WP31, and work was started by implementing in Isabelle/HOL a model of a firewall based on a separation kernel.

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 consisted of creating a so-called Platform Support Package (PSP). This PSP 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. The PikeOS support for the avionics platform was finished in M14, while the support for the automotive platform was eventually provided to project partners only in M22. The reason for the latter delay was repeated failure by a project-external hardware supplier to provide correct and complete specifications, necessitating yet another platform change around M15. 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 first created a comparative overview of these properties, tabulating the properties of the various I/O memory management units (IOMMUs). This overview was amended every time we had to switch platforms for the automotive prototype. Next, based on the existing IOMMU support for x86 in PikeOS, we created an IOMMU interface and implementation for the avionics platform. This experience, combined with the requirements analysis of the automotive prototype and capabilities analysis of its IOMMU, has lead to the design of a generic I/O virtualisation interface for PikeOS. Work on the implementation of the IOMMU support for the automotive platform is ongoing due to the aforementioned issues with the hardware supplier. Fortunately, since M25 we finally have received all necessary documentation and sample code, and the work is now progressing well.

WP23 (Prototype Integration) targets two major topics, integration of the prototype and the prototype test-bed, for the domains avionic and automotive, respectively. In both domains we have worked on the prototype platform to integrate supporting software from WP22 to enable the security features each platform offers. At the same time, test concepts for each domain have been developed, and the respective test-beds have largely been implemented. According to the project plan, this work is still continuing. In the avionics domain, the major prototype software modules have been developed and integrated to PikeOS, running on the P8080 demonstrator platform. Some of the use-cases can already be shown. For the automotive prototype, PikeOS has been enabled to use the hardware virtualization features of the ARM Cortex A8 cores, and a pre-integration of the automotive prototype architecture has been achieved. Since the test-beds in both domains should support penetration tests on network interfaces, they both integrate the tool Scapy, which was developed for this purpose by Airbus and provided to the team. In addition, the hypervisor test tool Ramooflax has been adapted to test PikeOS. While the avionic test-bed is a standalone hardware-in-the-loop setup, the automotive test-bed is integrated in a larger automatic test environment consisting of continuous integration, functional test, robustness and safety test as well as penetration test of external and internal interfaces.

During the second year, advances in ***WP31 (Assurance by Formal Methods)*** have been made in both the generic model and the implementation model. Additionally, we have identified implicit assumptions behind the model, i.e., the assumptions that are not formulated in Isabelle but which have been made during modelling. We have published a paper about that topic. Two major aspects have been added to the generic model. First, it has been given an explicit notion of time. This allows proving both time and space separation. The unwinding methodology has been extended with new proof obligations that ensure time separation. Currently, a paper is under review about this topic. Secondly, we have finished a draft version of a multicore model. Currently, we are investigating whether multicore PikeOS satisfies the assumptions made for the multicore model. All relevant PikeOS API calls have been modelled in the implementation model. Besides the IPC, the event API, the memory, ports, external file providers and user locks have been modelled. For all these models, all necessary proof obligations have been discharged. In other words, all of these actions have been proving to ensure time and space separation.

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. The project partner in WP32 synchronized the evaluation activity in WP32 telcos and during the technical meetings in Toulouse and Munich/Ottobrunn. All preparatory steps of the documents were performed by SYSF. For a various parts of the evaluation activity, TCS, SYSF and TSYS performed kick-offs and synchronization of the evaluations. SYSF prepared for evaluation by document review and internal audits. Within WP32 (Common Criteria Security Evaluation) the evaluation of the CC assurance classes ADV and ALC were significantly improved (tasks 3.2.2 and 3.2.3) by TSYS apart from potential comments by the German certification body BSI. Regarding the ALC and ADV assurance class main parts of the evaluator work units were performed by TSYS and will be resumed by TCS. The documentation of the CC assurance classes AGD (task 3.2.4), ATE (part of 3.2.2) delivered by TCS have been reviewed by TSYS and the evaluation can be started in November 2014. Recently the evaluation is delayed since the kick-off the BSI was delayed before and the input by the developer was timely but not fully appropriate for a Common Criteria Evaluation. Therefore the evaluation started delayed. In the second half of the second period (i.e. after overcoming the described hesitation) the evaluation activity increased significantly.

WP33 (Cross-European Certification) deals with assurance for high EAL (above 4) and with composition. During workshops, the challenge of high assurance (eg; missing work units of the CEM) and of composition have been introduced to all partners. The JIL approach has been followed and a draft version of "D33.1 has been published. In addition, artefacts have been published on "application of attack potential" and "attack method" in the MILS context. Furthermore, a draft version of "composition for software platform" has been released.

Within ***WP41 (Dissemination, Standardisation and Exploitation)***, the early established robust IT infrastructure (web site, SVN repository including web access, mailing lists including mailing list archives) was regularly updated. 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 the project results. The project is represented in an EU year book. Dissemination activities are announced via http://www.euromils.eu/index.php/news. A list of dissemination activities has been compiled and updated periodically. Details regarding dissemination activities can be found in section **Fehler! Verweisquelle konnte nicht gefunden werden.**. 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. GA Meeting), monthly EB Telcos, monitoring of the work plan (Interim 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 have 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 15 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.