Guide to EURO-MILS Results

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:	42 months
Programme:	FP7/2007-2013

Submission date:	18th July 2016
Abstract:	This document starts with a project summary and is a "cookbook" for developers and researchers in respect to development of high assurance MILS systems based on the EURO-MILS results. It includes a guide to the project deliverables, with embedded links to the public reports. Furthermore it is a roadmap for a novice who would like to develop and get certified high assurance.

Table of content

1 Project Summary 3

1.1 Review of Major Project Outcomes 3
1.2 MILS Community 4
1.3 Innovations 5
1.4 Barriers 5
1.5 Certification Aspects for Policy Makers 6

2 Busy Person Guide to Reading Project Results 8

2.1 MILS Architecture 8
2.1.1 Concepts and Definitions 8
2.1.2 Instantiations and Requirements 8
2.1.3 Components and Testing 8
2.2 Formal Methods 8
2.2.1 Separation Kernel 9
2.2.2 MILS systems 9
2.2.3 Formal Testing 9
2.3 Common Criteria 9
2.3.1 Protection Profile and Security Target 9
2.3.2 Use of Formal Methods for CC certification 9
2.3.3 Other CC Evaluation Aspects 10
2.3.4 High-EAL Assurance 10
2.3.5 Compositional Certification 10
2.4 Business, Legal, and Social Acceptance 10

Abbreviations 12

Bibliography 13

REMARK: For all public deliverables, links to the documents are provided. The other project deliverables are confidential.

Disclaimer

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 318353."

1 Project Summary

Cyber-physical networks based on embedded systems are part of our society and gain spread and importance. Next generations of aircrafts 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. Ubiquitous, highly critical systems go online and create a domain of mixed criticalities, where security and safety requirements of different levels mix. Today, state of the art technology does not provide trustworthiness for such interconnection and mix.

The project's cornerstone is MILS (Multiple Independent Levels of Security), a high-assurance security architecture that supports the coexistence of untrusted and trusted components, based on verifiable separation mechanisms and controlled information flow.

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

For the first time in Europe, EURO-MILS embarked on a complete "Common Criteria" security evaluation of a MILS system to its highest levels of assurance, including formal verification engineering. Hardware dependencies are addressed from the beginning by prototype development on two hardware platforms in automotive and avionics. EURO-MILS was strongly market oriented, is carried out in pan-European context, and had an advisory board with government IT security authorities (BSI-Germany and ANSSI-France). In addition, the methodology gained from this high-assurance certification and investigating MILS business, legal, and social acceptance benefit not only the MILS domain but all high-assurance security certifications in Europe.

1.1 Review of Major Project Outcomes

The following five outcomes have been targeted in the project's description of work ([DoW] text in italics) and achieved in the following way.

Outcome 1. Trustworthy foundations by the MILS approach, architecture, and applications

Provide Trustworthy ICT for high critical automotive and avionics domains through using the MILS approach. The base of such ICT is MILS architectures for compositional security and compositional assurance. This outcome has been achieved by the implementation-validated "MILS Architecture" [D21.1], which is the most downloaded document from the EURO-MILS website (see [D41.3], Section 1.2.3.2), Google hit #4 for "MILS Architecture". The application of the MILS architecture template by automotive and avionics application is described in [D21.2].

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 a secure and safe product 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. This outcome has been achieved by virtualisation of I/O by an IOMMU (PAMU in avionics and Jacinto Firewall in automotive), virtualisation of 2D/3D graphic unit on Jacinto, virtualisation of DPAA (Network), BSPs for P4080 (avionics), Jacinto (automotive), security audit, and failsafe file system SATA/CFS on P4080.

Outcome 3. High Assurance

Provide trustworthiness by assurance through rigorous certification along highest levels of "Common Criteria for IT Evaluations" (CC) standard, i.e. provide trustworthiness guarantees. 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 harmonized approach for high-assurance vulnerability analysis. This output has been achieved by doing CC evaluation of CC ASE, part of ALC, ADV, ATE, AVA [D32.1], developing a pragmatic approach for formal methods usage [AN, CCDEV, D31.1, D31.2, D31.3]. [D33.1] describes an innovative approach for (apriori) compositional assurance and 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). This output has been achieved by that SYSGO developed a Security Certification Kit for Common Criteria.

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, 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. This output has been achieved by joint work on ANSSI/BSI compliance for formal methods [AN], the addendum to CEM for high assurance [D33.1], a white paper on non-interfering composed evaluation [FSW+16], interaction with the advisory board. In European context, during 86 teleconferences we worked out formal models [D31.1, D31.2, D31.3, VSH+16, VTH+14] and their certification [AN, CCDEV], and build the MILS community (see Section 1.2) with participation of European and US domain stakeholders.

1.2 MILS Community

The MILS Community is a global international, open membership, not-for-profit technology consortium with potential to become the leading competence network on MILS architecture and technologies. This MILS community is an interest group for architecture-based security, which aims to exchange ideas about meaningful work that could be done (in industrial or research context).

The first International Workshop on "MILS: Architecture and Assurance for Secure Systems", in January 2015 in Amsterdam, was co-located with the HiPEAC Conference and focused mainly on the MILS architectural approach for security and safety, MILS components and eco-system as well as the certification or the possible MILS use-cases. Furthermore, real-time separation kernels and cross-European and world-wide high-assurance security were among the discussed topics.

The second workshop on MILS took place on 20th January 2016 in Prague as well as the MILS community meeting on 21 January 2016 for which, additionally, it was offered the possibility to join the sessions via teleconference. Hot topics were Common Criteria

certification, hardware (testing versus compliance), how to agree on common definitions in the form of a glossary, a possible catalogue of known (published) MILS systems, and how to complement other standardisation efforts.

For more information about the MILS Community, please follow http://mils-community.euromils.eu/ and we kindly invite you to subscribe to the MILS Community mailing list via the web form http://lists.euromils.eu/mailman/listinfo/mils.

1.3 Innovations

The following innovations have been achieved. They are described in more detail in Section 2.

- Executable implementations:
  - MILS Core Component: Secure I/O on PowerPC and ARM
  - Secure Network: PowerPC DPAA
  - Automotive and Avionics exploitation
    - Security policy for information flow
    - Network manager component
    - Device management techniques
  - Analysis tool Ramooflax
- Common Criteria Artefacts and Methodology
  - Apriori compositional evaluation methodology
  - Pave the way for the innovation for a separation kernel certification
    - Common Criteria Certification Kit for a Separation Kernel incl. CC Compliance approach
    - TSFI definition for separation kernels
    - Hardware/Software interface in Security Target (SFRs) and in formal model
- Formal Methods
  - Formal model modelling preemptible code
  - Formal model for multicore (MCISK)
  - CC developer statement approach for FM
  - Used formal methods and guideline
- Business analysis on MILS and security

1.4 Barriers

One identified barrier for high-assurance certification were US certification authorities, as they have been pushing for low mutual (= EAL2) recognition except for where cPPs have been made. Moreover, NSA/NIAP support for secure small OS has been lacklustre e.g. SKPP was recalled in 2010 after two years of operation [NIAP10]. Moreover, NSA/NIAP support for OSPP cPP has been disappointing too [Don14].

The next barrier was hardware/software integration, there is no common understanding how to certify a system consisting of COTS HW and SW components, e.g. in some schemes a separation kernel can be certified with assumptions on hardware but without including hardware in other schemes there are understandings that system software and HW should be evaluated jointly. However, on the market, it is no problem to buy a CC-certified smartcard, but one cannot buy any CC-certified CPU. This problem might be addressed by compliance for hardware. [TB14]. One of the possible directions is to involve hardware vendors and with their support develop an approach to cover hardware in a protection profile for a separation kernel.

Another barrier concerns clashes of safety and security certification: On one side, adding security must not invalidate safety properties and certifications; and on the other side adding safety must not invalidate security properties and certifications. Safety is mainly regulated by non-governmental private schemes, whereas security certification with national authority may appear as/result in a bottleneck reducing flexibility. Some stakeholders state that for some product classes this could result in higher assurance due to assessing classified information. In safety, industry is active in IEC 62443-based solutions (e.g. recent norms for railway signaling are based on this) and private schemes for these IEC safety norms are being established. Thus, a research on combining Common Criteria knowledge and industrial driven safety certification is needed and would strengthen the assurance for the overall ICT security.

1.5 Certification Aspects for Policy Makers

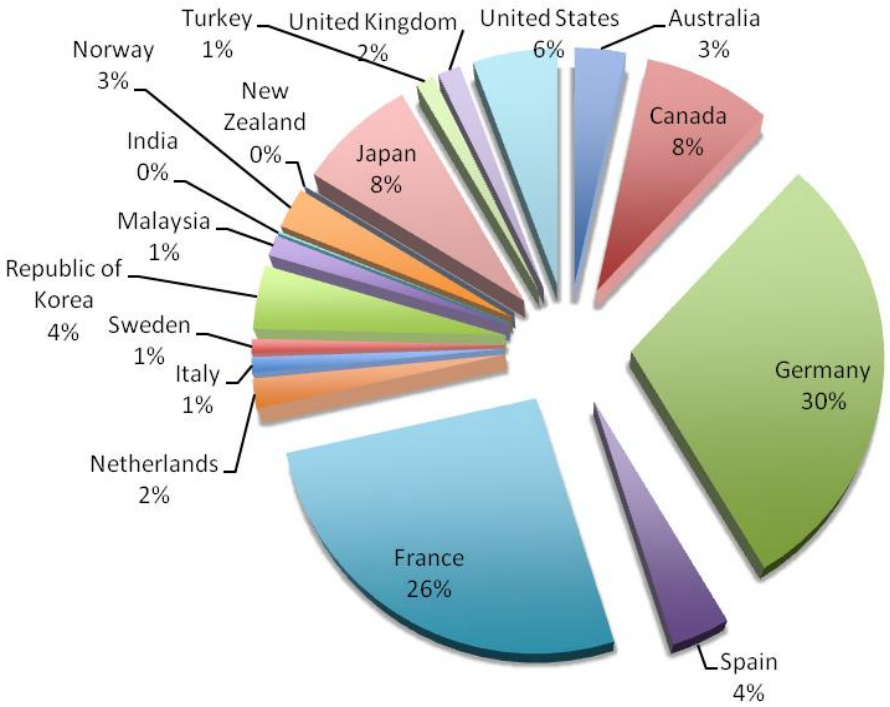

Figure 1: World-wide CC certifications, based on [CCP]

As shown in Figure 1, Europe is strong in CC certification (65% of the certifications published in [CCP] are in the EU). Moreover high-assurance is done mainly in Europe, for instance all 39 listed EAL6 products are from the EU and 4 of the 5 listed EAL7 products are from EU. However, these high-level products are mostly smart cards and there is none targeting assurance on COTS HW, e.g. CPU, SoC, or other hardware IPs. In the area of high-assurance OS there is Only US Green Hills Integrity with disputed EAL6 which, tellingly, is not even counted in the official CC statistics page, according to the revoked US Separation

Kernel Protection Profile (SKPP) and the only operating system at EAL5+ is IBM PR/SM zSeries 800/900, which is relevant for banking, but not used in embedded systems, e.g. there are no communication channels between VMs at all and we could not have built the demonstrators on PR/SM with zOS. IBM PS/SM is not portable and not "COTS" since specific IBM HW is needed. In summary, today end-product certifications prevail, this approach is hardly scalable for complex cyber-physical systems and IoT applications.

However, the current CC does not converge in recognition, e.g. new CCRA with lowered mutual recognition level, SOGIS members positions with respect to the new CCRA. Our experience shows that European efforts for common high-assurance are still needed. For cyberphysical systems there is IEC 62443, but the link between CC and cyberphysical systems is weak. IEC 62443 with CC would bridge cyber-physical systems and IT security, e.g. railway, smart grids. The balance between industrial driven certification (e.g. as in safety) and governmental-driven certification needs to be researched.

For the specific point of security-by-design (such as) MILS, safety standards such DO-178 [DO-178C, Section 2.1] recommend design methods such as "*system requirements allocated to software may include [...] safety strategies, design constraints and design methods, such as, partitioning, dissimilarity, redundancy or safety monitoring*". The networking information security directive 2013/0027 (COD) has a clause that operators of essential services "*provide information needed to assess the security of their networks and information systems, including documented security policies.*" We suggest that, for a policy for cyberphysical systems, IoT, or similar directive is designed, to require producers of critical products to develop security strategies and apply design methods such **as attack surface reduction, partitioning, formal modelling, redundancy and/or security monitoring**.

2 Busy Person Guide to Reading Project Results

We suggest the following order of reading and skimming the delivered documents to reduce efforts.

- For MILS component developers and users (system integrators) Section 2.1 is of special interest.
- For formal modellers, Section 2.2 and 2.3.2 are of special interest
- For CC evaluators or MILS component developers wishing to obtain CC certification, Section 2.3 is of special interest.
- For a business context, start with Section 2.4.
- For complete novices, start with Section 2.1.1, and then proceed according to your interests.

2.1 MILS Architecture

2.1.1 Concepts and Definitions

MILS Architecture [D21.1]: This document formulates the project partners' common understanding of terms related to "architecture" in general and to MILS architecture. We introduce a generic description of MILS systems (Chapter 2), and the MILS architecture template (Chapter 3). Chapter 4 discusses the MILS main components.

2.1.2 Instantiations and Requirements

From a system perspective, in EURO-MILS, the MILS architecture template of D21.1 has been instantiated by the automotive, using ARM-based hardware (TI Jacinto), and avionics prototypes, using an NXP/Freescale-based board (P4080). The architectures of these instantiations and how they relate to the MILS architecture template have been described in [D21.2, FSW+16] in a unified treatment. That unified treatment is accompanied by a more detailed report on the avionics [D23.1] and automotive prototype [D23.2] themselves. The initial formulation of the requirements the instantiations have to fulfil is in [D11.1]. [D22.1] is the document that describes how the PikeOS separation kernel serves as instantiation of the generic separation kernel described in [D21.1].

2.1.3 Components and Testing

[D22.1] discusses components that were used for the platforms. [D22.2] focuses specifically on the IOMMU that was designed on each of the prototypes and how the design can be used for multiple architectures. [D23.3] describes the testbeds used for testing the prototypes as well as penetration testing performed on the separation kernel with the help of the introspection tool ramooflax, and [D23.4] discusses the testing results.

2.2 Formal Methods

This section builds on Section 2.1.1.

2.2.1 Separation Kernel

We have used the tool Isabelle/HOL version 2013-2 for security policy modelling of the separation kernel. A specific security policy model of the separation kernel used in EURO-MILS has been defined in [D31.3]. The specific model is accompanied by the CISK single-core [VTH+14] and MCISK multi-core models [VSH+16] applicable to a generic separation kernel with interrupts. Further documentation can be found in [VHS+15, VST+14].

2.2.2 MILS systems

If one is a system integrator, one is not only interested in the correctness of the underlying of a separation kernel, but also of the system built atop of it. [D21.4, KS16] develop the formal models for entire MILS systems based on a separation kernel and how to apply them to the automotive and avionics demonstrators.

2.2.3 Formal Testing

[D31.4] explains how the HOL-TestGen framework has been used for automatic generation of symbolic testing for IPC as provided by the separation kernel.

2.3 Common Criteria

2.3.1 Protection Profile and Security Target

This section builds on Section 2.1.1.

The specification of requirements to be evaluated in a CC security evaluation is specified in a Security Target. A CC security target for the EURO-MILS separation kernel has been provided by [D12.2], with the contents as required by the CC, such as Security Problem Definition for PikeOS, SFRs, argument why security objectives are fulfilled by SFRs, TOE Summary Specification with Architectural Design Summary (ASE_TSS.2). Moreover, the experience of building a security target has been used to create a Protection Profile draft for the whole product class of separation kernels [D12.3].

2.3.2 Use of Formal Methods for CC certification

This section builds on Sections 2.1.1 and 2.3.1

During the project, it became obvious that the formal methods must be carefully linked to the CC requirements. The CC Developer Statement [CCDEV] is a statement by the EURO-MILS formal methods developers how the formal security policy model is to be used for claiming a formal model of security policies and SFRs, including “properties” and “features” in ANSSI Note 12 and BSI AIS 34 terms. Chapter 2 (ARG_TOOL in terms of ANSSI Note 12) describes our usage of the Isabelle/HOL theorem prover, Chapter 3 (ARG_SPM) describes our formal model of Separation and clearly states which policies it models, Chapter 4 (ARG_CDS) treats the correspondence between our formal model and the modelled policies and associated SFRs in the security target. Chapter 5 (ARG_PROOF) shows model consistency. Chapter 6 (ARG_FSP) makes the correspondence between our functional specification and our formal security policy model. [CCDEV] is accompanied by [AN], which contains statements on evaluability of SPM artefacts based on ANSSI Note 12 and BSI AIS 34. These statements have been developed by the formal modelling team of the EURO-MILS project with feedbacks from the ITSEFs Thales, T-Systems, and DFKI.

The previously mentioned ARG_TOOL is further detailed in [D31.2], to be useful to *anyone* who uses Isabelle/HOL for certification: Chapter 1 describes how Isabelle/HOL works and how to use it in a certification process in a sound way. Chapter 2 (style guide) describes how

to write Isabelle theories so that they are suitable for collaborative work and human readers in a certification context. Chapter 3 (compliance statement) states in the EURO-MILS project, the developed theories are compliant with Chapter 1 and Chapter 2.

2.3.3 Other CC Evaluation Aspects

[D32.1] is a complete evaluation technical report of the CC evaluation of the PikeOS separation kernel.

2.3.4 High-EAL Assurance

This section builds on Section 2.3.2

As build-up step, EURO-MILS collected the state of the art of high-assurance evaluation in [D12.1]. The next step was to do practical CC evaluations, centring on the separation kernel, but also taking into account compositional aspects for the prototypes [FSW+16]. The output of this activity [D33.1] was an addendum to the Common Methodology for Information Technology Security Evaluation (CEM). This document interprets the current version of the CEM for MILS. First, it provides evaluation methodology and guidance metrics to calculate attack potential required by an attacker to perform an attack on MILS products and interprets the Common Criteria for high-EAL levels.

2.3.5 Compositional Certification

[D21.3, FSW+, D33.1] describe Common Criteria composition of software platforms. [D21.3] starts out with a comparison of two existing CC evaluation approaches, which evaluate the underlying platform for *each* evaluation. As new innovation, [FSW+, D33.1] then proceed to describe an-priori approach, where separation properties of a platform are established once and for all, so that all systems built on that platform avoid recertification of the underlying platform. Note: the reader interested in compositional certification also might be interested in compositional formal models, a topic that was discussed in Section 2.2.2.

2.4 Business, Legal, and Social Acceptance

Business/legal/social values have been discussed in [D13.1, D13.2]. [D13.2] consists of the following parts:

- Part I defines the project terminology. As often in information and telecommunications technologies, generic concepts as trustworthiness, security, and safety have different meanings for markets, providers and consumers. The meaning of the terms varies considerably from one context to another. So, it is an important starting point to define the common vocabulary when discussing with experts in different technical domains or even with simple end-user consumers.
- Part II presents the results of the business impact analysis of MILS cross-sectorally beyond the avionics and automotive sectors. MILS is a platform that allows the horizontal integration, which is more open than vertically stacked products. In every industry sector, a trend to such horizontal platforms has been observed. We investigated the business value of a trustworthy ICT from a horizontal platform perspective and identified market requirements of MILS systems.
- Part III presents the results of the social impact analysis with a strong focus on consumers. Using a survey, we questioned consumers on their security awareness and practices. We wanted to understand the main security expectations when buying and using a connected device such as a smartphone. We also listened to what

consumers where saying on the connected device and security theme using a Big Data analysis.

- Part IV presents the results of the legal impact analysis of a certified platform with a specific focus on the new paradigm of the Internet of Things and its legal implications and issues.
- Part V concludes the work.

Abbreviations

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
COTS	Custom off-the-Shelf
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
HOL	Higher-Order Logic
IOMMU	Input/Output Memory Management Unit
MILS	Multiple Independent Levels of Security
NIAP	National Information Assurance Partnership
SoC	System on a Chip
TOE	Target of Evaluation
TSFI	Target of Evaluation Security Functionality Interface
CO	Confidential, only for members of the consortium (including the Commission Services)
PP	Restricted to other programme participants (including the Commission Services)
RE	Restricted to a group specified by the consortium (including the Commission Services)

Bibliography

[ABC+13] Saswat Anand, Edmund K. Burke, Tsong Yueh Chen, John Clark, Myra B. Cohen, Wolfgang Grieskamp, Mark Harman, Mary Jean Harrold, and Phil Mcminn. An orchestrated survey of methodologies for automated software test case generation. J. Syst. Softw., 86(8):1978–2001, August 2013

[AN] EURO-MILS project, AIS34/Note 12 Compliance Statement, delivered document

[CCDEV] EURO-MILS project, CC Developer Statement ADV_SPM, delivered document

[CCP] Common Criteria Sponsoring Organizations, Certified Products, 2016, http://www.commoncriteriaportal.org/products/ , accessed 17 May 2016.

[D11.1] EURO-MILS project, Project Requirements: Classification, Cross-domain analysis and High-Level Architecture, project deliverable [Dissemination level: RE]

[D12.1] EURO-MILS project, Technical analysis of available assurance techniques, project deliverable, http://dx.doi.org/10.5281/zenodo.47296

[D12.2] EURO-MILS project, Security Target (ST) for a Highly Robust OS in Europe: project deliverable [Dissemination level: CO]

[D12.3] EURO-MILS project, EURO-MILS proposal for Projection Profile (PP) for a Highly Robust OS in Europe: project deliverable, http://dx.doi.org/10.5281/zenodo.51582

[D13.1] EURO-MILS project, MILS: business, legal and social acceptance - draft, project deliverable [Dissemination level: CO]

[D13.2] EURO-MILS project, MILS: business, legal and social acceptance, project deliverable, http://dx.doi.org/10.5281/zenodo.47301

[D21.1] EURO-MILS project, MILS architecture, project deliverable, http://dx.doi.org/10.5281/zenodo.45164

[D21.2] EURO-MILS project, MILS architecture for avionics and automotive, project deliverable [Dissemination level: CO]

[D21.3] EURO-MILS project, Trustworthy MILS: CC composite evaluation approach, project deliverable, http://dx.doi.org/10.5281/zenodo.47300

[D21.4] EURO-MILS project, Formal framework for MILS integration, project deliverable, http://dx.doi.org/10.5281/zenodo.57413

[D22.1] EURO-MILS project, MILS virtualisation platform implementation on adapted PikeOS, board support, documentation, project deliverable [Dissemination level: CO]

[D22.2] EURO-MILS project, Multiarchitecture module for secure concurrent I/O, project deliverable [Dissemination level: CO]

[D23.1] EURO-MILS project, Prototype avionics, project deliverable [Dissemination level: CO]

[D23.2] EURO-MILS project, Prototype automotive, project deliverable [Dissemination level: CO]

[D23.3] EURO-MILS project, Testbed, project deliverable [Dissemination level: CO]

[D23.4] EURO-MILS project, Validation report, project deliverable [Dissemination level: PP]

[D31.1] EURO-MILS project, Formal specification of a generic MILS seperation kernel, project deliverable, http://dx.doi.org/10.5281/zenodo.47299

[D31.2] EURO-MILS project, Used formal methods, project deliverable, http://dx.doi.org/10.5281/zenodo.47297

[D31.3] EURO-MILS project, Formal security policy model of the TOE inclusive Formal Proofs, project deliverable, accompanied by Isabelle/HOL theory sources, EURO-MILS-D31-3-Formal-Security-Policy-Model-Isabelle-Theories.tgz, can be run in Isabelle/HOL 2013-2. [Dissemination level: CO]

[D31.4] EURO-MILS project, Test-case generation environment, generated test-cases for PikeOS, project deliverable, http://dx.doi.org/10.5281/zenodo.47302

[D32.1] EURO-MILS project, Complete evaluation technical report, project deliverable [Dissemination level: CO]

[D33.1] EURO-MILS project, Addendum to CEM, project deliverable, http://dx.doi.org/10.5281/zenodo.47298

[D41.1] EURO-MILS project, Project website, project deliverable, http://www.euromils.eu/downloads/Deliverables/Y1/EURO-MILS-D41.1-Project-website-PU-M02.pdf

[D41.2] EURO-MILS project, Initial report on dissemination, standardisation and exploitation, project deliverable, http://www.euromils.eu/downloads/Deliverables/Y1/EURO-MILS-D41.2-Initial-report-on-dissemination-standardisation-and-exploitation-PU-M12.pdf

[D41.3] EURO-MILS project, Final dissemination, standardisation and exploitation report, project deliverable

[D42.1] EURO-MILS project, Project internal and external IT communication infrastructure, project deliverable, http://www.euromils.eu/downloads/Deliverables/Y1/EURO-MILS-D42.1-Project-internal-and-external-IT-communication-infrastructure-PU-M02.pdf

[D42.2] EURO-MILS project, 1st Periodic Report according to EC regulations of the model contract, project deliverable; publishable summary: http://www.euromils.eu/downloads/Deliverables/Y1/02-EURO-MILS-318353-D42.2-1st-periodic-report-publishable-summary-v1.1.pdf

[D42.3] EURO-MILS project, 2nd Periodic report according to EC regulations of the model contract, project deliverable; publishable summary: http://www.euromils.eu/downloads/Deliverables/Y2/02_EURO-MILS-318353-D42.3-2nd-periodic-report-publishable-summary.pdf

[D42.4] EURO-MILS project, 3rd Periodic Report according to EC regulations of the model contract, project deliverable, publishable summary: http://www.euromils.eu/downloads/Deliverables/Y3/02-EURO-MILS-318353-D42.4-3rd-periodic-report-publishable-summary.pdf

[DO-178C] RTCA SC-205 / EUROCAE WG-71, DO-178C: Software Considerations in Airborne Systems and Equipment Certification, December, 2011, Radio Technical Commission for Aeronautics (RTCA), Inc., 1150 18th NW, Suite 910, Washington, D.C. 20036.

[Don14] Donndelinger, Position Statement regarding the CC evaluation of General Purpose Operating Systems, 2014, https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/GPOS%20Position%20Statement.pdf.

[DoW] EURO-MILS project, description of work, 2012.

[FSW+16] Igor Furgel, Viola Saftig, Tobias Wagner, Kevin Müller, Reinhard Schwarz, Axel Söding-Freiherr von Blomberg, Non-Interfering Composed Evaluation, MILS Workshop at HiPEAC 2016, http://dx.doi.org/10.5281/zenodo.47979

[KS16]. Ruud Koolen; Schmaltz, Julien, Information Routing with Noninterference, MILS Workshop at HiPEAC 2016, http://dx.doi.org/10.5281/zenodo.47980

[NIAP10] http://www.niap-ccevs.org/announcements/Separation%20Kernels%20on%20Commodity%20Workstations.pdf

[TB14] Paul Theron, Sandro Bologna, Proposals from the ERNCIP Thematic Group, "Case Studies for the Cyber-security of Industrial Automation and Control Systems", for a European IACS Components Cyber-security Compliance and Certification Scheme, 2014, http://publications.jrc.ec.europa.eu/repository/handle/JRC94533.

[VST+14] Freek Verbeek, Julien Schmaltz, Sergey Tverdyshev, Holger Blasum, Oto Havle, Implicit Assumptions in a Model for Separation Kernels, Vienna Summer of Logic: 2nd VeriSure Workshop, 2014.

[VHS+15] Verbeek, Freek, Havle, Oto, Schmaltz, Julien, Tverdyshev, Sergey, Blasum, Holger, Langenstein, Bruno, Stephan, Werner, Wolff, Burkhart, Nemouchi, Yakoub, Formal API Specification of the PikeOS Separation Kernel, NASA Formal Methods, LNCS, vol. 9058, p. 375-389, 2015, Springer International Publishing.

[VSH+16] Freek Verbeek, Julien Schmaltz, Oto Havle, Burkhart Wolff, Bruno Langenstein, MCISK, http://dx.doi.org/10.5281/zenodo.48658

[VTH+14] Freek Verbeek, Sergey Tverdyshev, Oto Havle, Holger Blasum, Bruno Langenstein, Werner Stephan, Yakoub Nemouchi, Abderrahmane Feliachi, Burkhart Wolff, Julien Schmaltz, Formal Specification of a Generic Separation Kernel, Archive of Formal Proofs, 2014, http://afp.sourceforge.net/entries/CISC-Kernel.shtml