D 41.2

Initial report on dissemination, standardisation and exploitation

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

Deliverable type:	Report
Deliverable reference number:	ICT-318353 / D41.2 / 1.0
Activity and Work package contributing to the deliverable:	Activity 4 / WP 41
Due date:	September 2013 – M12
Actual submission date:	30th September, 2013

Responsible organisation:	SYSGO
Editor:	SYSGO (Holger Blasum)
Dissemination level:	Public
Revision:	1.0

Abstract:	This deliverable reports on the progress of dissemination of the project as well as on standardisation and exploitation of project results during the first EURO-MILS project year. Chapter 1 describes the dissemination approach in EURO-MILS. Chapter 2 covers the standardisation approach and Chapter 3 describes the exploitation approach in EURO-MILS.
Keywords:	Dissemination, Standardisation, Exploitation, IPR

Editor

Holger Blasum (SYSGO)

Contributors (ordered according to beneficiary numbers)

Kathrin Niederbichler, Günther Bürger (TEC)

Holger Blasum, Sergey Tverdyshev (SYSGO)

Andreas Nonnengart (DFKI)

Jonas Maebe (UGENT)

Bertrand Leconte (AOS)

Kevin Müller, Michael Paulitsch (EADS IW)

Axel Söding-Freiherr von Blomberg (OPSYN)

Axel Tillequin (EADS F IW)

Burkhart Wolff (PSUD)

Jean-Christophe Courrège (TCS)

Julien Schmaltz (OUNL)

Igor Furgel (TSYS)

Jacques Brygier (SYSF)

Christophe Toulemonde (JR)

Partner names (ordered according to beneficiary numbers)

TEC	TECHNIKON Forschungs- und Planungsgesellschaft mbH, Austria
SYSGO	SYSGO AG, Germany
DFKI	Deutsches Forschungszentrum für künstliche Intelligenz GmbH, Germany
UGENT	Universiteit Gent, Belgium
AOS	AIRBUS Operations SAS, France
EADS IW	EADS Deutschland GmbH, Germany
OPSYN	OpenSynergy GmbH, Germany
EADS F IW	EADS France SAS, France
PSUD	Université Paris-Sud, France
TCS	Thales Communications & Security SA, France
OUNL	Open Universiteit Nederland, Netherlands
TSYS	T-Systems International GmbH, Germany
SYSF	SYSGO SAS, France
JR	Jemm Research SARL, France

Acknowledgement

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318353.

Executive Summary

This deliverable reports on the progress of dissemination of the project as well as on standardisation and exploitation of project results during the first EURO-MILS project year.

Chapter 1 describes the dissemination approach in EURO-MILS. Chapter 2 covers the standardisation approach and Chapter 3 describes the exploitation approach in EURO-MILS. Both, project-wide as well as per-partner considerations are taken into account. In particular, the use of deliverables for joint standardisation and joint exploitation is discussed. In the context of exploitation, also a preliminary market overview is covered. Further, as IPR issues are directly related to exploitation activities, IPR issues are covered within this deliverable.

Overall, remarkable dissemination, standardisation and exploitation activities to raise the public awareness of the EURO-MILS project within the scientific and industrial communities have been reached in the first project year:

- Participation at scientific and industry oriented conferences, such as Avionics Europe, EUROSEC, RTES forum, TAP (Test and Proof)
- 4 scientific publications
- 2 EURO-MILS related presentations at the International CC Conference 2013
- Establishment of an active and lively project website
- Raised awareness of EURO-MILS in form of Announcement Letter, Leaflet, Newsletter as well as in social media (Twitter, LinkedIn)
- active Cooperation with other FP7- and national projects
- EURO-MILS presence ICT 2013
- EURO-MILS will be part of the EU Yearbook
- Active contact with EURO-MILS related standardisation bodies

Contents

List of Figures

List of Tables

Chapter 1 Dissemination

Dissemination activities are provided to ensure the visibility and awareness of the project and to support the widest adoption of its results in industry and research. The strategy for the dissemination of EURO-MILS aims at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties.

1.1 Dissemination Strategy

The EURO-MILS dissemination strategy adopted for the entire project duration is based on the following pillars:

- Presentation of the research results within the scientific community (Section 1.2.1),
- Presentation and demonstration at national and international exhibitions & fairs and dedicated road-show events and industrial days (Section 1.2.2).
- Backing by robust infrastructure (Section 1.2.3).
- Presentation of the project to the general public (press, web, etc.), Section 1.2.4:
  - ✓ Regular communication with the press shall be installed (e.g. press releases at beginning of project, before main fairs/exhibitions)
  - ✓ Posters, handouts, and templates will be provided to all partners
  - ✓ A public project website will be installed and maintained. In addition, some partners have dedicated one page on their website to explain the project and their involvement
    - http://www.technikon.com/index.php/projects/euromils,
    - http://www.sysgo.com/company/about-sysgo/rd-projects/the-euro-mils-project/,
    - http://www.jemmresearch.com/euro-mils-la-s%C3%A9curit%C3%A9-des-syst%C3%A8mes-embarqu%C3%A9s
  - ✓ At the end of the project the results can be presented to journalists (dedicated press tour or during the above road show)
  - ✓ Mention the project on the website of the FP7 HiPEAC network of excellence

1.2 Dissemination Activities Started in M01-M12

The project and its results have been disseminated by invited talks at conferences, by publications at scientific and industry oriented conferences (such as Avionics Europe, EUROSEC, RTES forum, TAP (Test and Proof)) and by organising technical workshops within the project. The following section presents our dissemination activities in order to document the extent to which we have executed our above mentioned dissemination strategy.

1.2.1 Scientific Publications

The following scientific peer-reviewed publications have been published within the first EURO-MILS project year.

Title	Authors	Title of the Periodical or the Proceedings	Number, Date or Frequency	Publisher	Year of Publication	Relevant Pages	Permanent Identifier[1] (if available)	Is/Will open access[2] provided to this publication?
Decreasing System Availability on an Avionic Multicore Processor Using Directly Assigned PCI Express Devices	Kevin Mueller	EuroSec (2013 European Workshop on Security), http://www.syssec-project.eu/eurosec-2013/, 14 April 2013	2013	ACM	2013		https://mediatum.ub.tum.de/node?id=1141647	No
Test Program Generation for a Microprocessor	Achim Brucker, Abderrahmane Feliachi, Yakoub Nemouchi, Burkhart Wolff	Test and Proofs (TAP 2013), http://www.spacios.eu/TAP2013/, 18-19 June 2013	2013	Springer LNCS	2013	76-95	10.1007/978-3-642-38916-0_5	No
The Circus Testing Theory Revisited in Isabelle/HOL	Abderrahmane Feliachi	International Conference on Formal Engineering Methods (ICFEM 2013)	2013	Springer LNCS	2013		N/A	No
HOL-TestGen/FW: An Environment for Specification-based Firewall Conformance Testing	Achim D Brucker, Lukas Brügger and Burkhart Wolff	International Colloquium on Theoretical Aspects of Computing (ICTAC)	2013	Springer LNCS	2013		http://www.brucker.ch/bibliography/download/2013/brucker.ea-hol-testgen-fw-2013.pdf	Yes

Table 1: List of publications

[1] A permanent identifier should be a persistent link to the published version full text if open access or abstract if article is pay per view or to the final manuscript accepted for publication (link to article in repository).

[2] Open Access is defined as free of charge access for anyone via Internet. Please answer “yes“ if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.

1.2.2 Presentations, Participation in Exhibitions and Conferences

1.2.2.1 M01-M12

Type of Activities	Main Leader	Title	Month	Year	Place	Size of Audience	Type and Goal of the Event	Countries Adressed
Exhibition	SYSGO	Poster exhibit	1	2013	Berlin	N/A	Hipeac conference, wwww.hipeac.net	International
Presentation	SYSGO, SYSF	MILS-related information flow control in the avionic domain: software architectures and verification	2	2013	Munich	10-15 (attending the talk), 1000s (attending show)	Dissemination of results to relevant audience in Europe, Avionics Europe, http://www.avionics-event.com/, trade fair + talk at exhibitor's forum (20 Feb 11h15-11h50).	International
Exhibition	OPSYN, SYSGO, SYSF	Presenting EURO-MILS at Embedded World	2	2013	Nuremberg	several 10000s	Posters and flyers at Embedded World, http://www.embedded-world.de/	International
Exhibition	JR	Meeting software and hardware vendors to present EURO-MILS project and to ask for participation in the industry panel.	2	2013	Nuremberg	several 10000s	Posters and flyers at Embedded World, http://www.embedded-world.de/	International
Exhibition	SYSF	Presenting EURO-MILS at rts EMBEDDED SYSTEMS	4	2013	Paris	several 1000s-10000s	http://www.salons-solutions-electroniques.com/	International
Conference	JR	EURO-MILS Project Teleconference	6	2013	Multiple	60	EURO-MILS Industry panel	International
Presentation	EADS	EURO-MILS: Secure European Virtualization for trustworthy applicationsin Critical Domains	7	2013	Philadelphia	20	Presentation of EURO-MILS at The Open Group Philadelphia 2013, Real-Time Forum, by Michael Paulitsch (EADS)	International
Presentation	TSYS	How to createa slim and comprehensive PP	9	2013	Orlando	600	Presentation at International Common Criteria Conference (ICCC) 2013, by Igor Furgel (TSYS); http://www.fbcinc.com/e/ICCC/	International
Conference	TSYS, SYSGO	Compositional Assurance: EURO-MILS ST/PP for Separation Kernel Based Virtualization	9	2013	Orlando	600	Presentation at International Common Criteria Conference (ICCC) 2013, by Sergey Tverdyshev (SYSGO), Holger	International

Type of Activities	Main Leader	Title	Month	Year	Place	Size of Audience	Type and Goal of the Event	Countries Adressed
							Blasum (SYSGO), Igor Furgel (TSYS) ; http://www.fbcinc.com/e/ICCC/	
Presentation	JR	EURO-MILS Project	9	2013	Paris	40	Introduction to EURO-MILS and potential industry outputs (Smarthome)	National

Table 2: Participation in exhibitions and conferences

Especially the industrial partners will present the project and its results at various trade shows such as: EU showcases like Aerodays, Embedded World, Nuremberg, Germany, Avionics Europe, rts EMBEDDED SYSTEMS, Paris, Embedded Technology, Yokohama, Grand colloque STIC (French fair organised by the Computer Science Department of ANR), ERTS Toulouse. In the 3rd year, the project partners will organise a road show through several European cities (e.g. Munich, Stuttgart, Toulouse) to promote the results to stakeholders in the safety and security industry.

1.2.2.2 Upcoming EURO-MILS Dissemination Activities

Type of Activities	Main Leader	Title	Day	Month	Year	Place	Size of Audience	Type and Goal of the Event	Countries Adressed
Article published in the popular press	OPSYN	Vertrauen durch Virtualisierung für das vernetzte AUTO	8	10	2013	Germany	11580, 32.870	Raise the public profile of EURO-MILS	National
Exhibition	TEC	ICT 2013 – Create, Connect, Grow	6	11	2013	Vilnius, Lithuania	4000+	conference, exhibition, networking sessions, investment forum, activities for students and young researchers	International

Type of Activities	Main Leader	Title	Day	Month	Year	Place	Size of Audience	Type and Goal of the Event	Countries Adressed
Presentation	TSYS, SYSGO, OPSYN	Multiple Applications Platform with Certified Separation	14-15	11	2013	Frankfurt		Presentation at the Embedded Security in Cars Conference Matthias Gerlach (OPSYN), Igor Furgel (TSYS), Sergey Tverdyshev (SYSGO) and Holger Blasum (SYSGO); www.escar.info	International
Presentation	JR	EURO-MILS Project	4	10	2013	Paris	20	Introduction to EURO-MILS to an Industry Automotive & Transportation working group (Systematic)	National

Table 3: Upcoming dissemination activities

ICT 2013 - The EURO-MILS project management team at TEC has successfully applied for a Technology and Innovation Stand at the exhibition of ICT 2013 – Create, Connect, Grow taking place in Vilnius (Lithuania) on 6-8 November 2013. This important networking event includes a conference, an exhibition, networking sessions, an investment forum as well as activities for students and young researchers. The idea is to present the EURO-MILS project and to get in contact with potential partners for future projects.

1.2.3 EURO-MILS Project Website

1.2.3.1 Public EURO-MILS Website http://www.euromils.eu

For the purpose of visibility, the project website was launched in month two of the project. It provides an overview of the project and up-to-date information on its activities and results, as well as contact details, information on partners and events. The website is based on the Content Management System (CMS) "Joomla!", a webserver which provides the public website and additionally restricted areas for members only. The website can be viewed with a standard web browser and will be kept alive throughout the project period and at least 3 years afterwards. Our website has been designed such that it can be handled intuitively and gives an introduction to the technical and organisational aspects of the project.

The project website has been updated continuously by the Project Coordinator, whereas all partners participate in the process by notifying the Coordinator of important news and developments.

The following illustration (Figure 1) shows the Welcome page of the EURO-MILS website. Project details of EURO-MILS are summarized on the left side, while on the right side the content of the respective section is given.

Figure 1: Welcome page of the EURO-MILS website

The structure of the official part of the website includes the following Links:

Home

- General introduction to the project – Mission and Motivation of the EURO-MILS project

News

- Conferences, Workshops and Meetings (date, topic and location)
- Press releases (date and link to the press releases)

Publications & Deliverables

- Publications by EURO-MILS partners (Public and approved Deliverables, other Publications, e.g. EURO-MILS Leaflet or Newsletter)

Partners

- Consortium of the EURO-MILS project

Feedback

- A template for website visitors' feedback.

Login

- Login area for project internal use.

The project website serves as the most versatile information and communication tool, as on one hand it provides information for a worldwide audience and on the other hand it enables a working platform for the project team. Therefore, it provides a user-friendly and informative environment.

As mentioned above, the website offers the users general information about the EURO-MILS project, its activities, achievements as well as background information, contact details and events. By clicking on the "News"-button, a list of conferences, workshops and meetings as well as press releases appear as illustrated in the following figure (Figure 2). Furthermore, the user can access the adequate site of the preferred news.

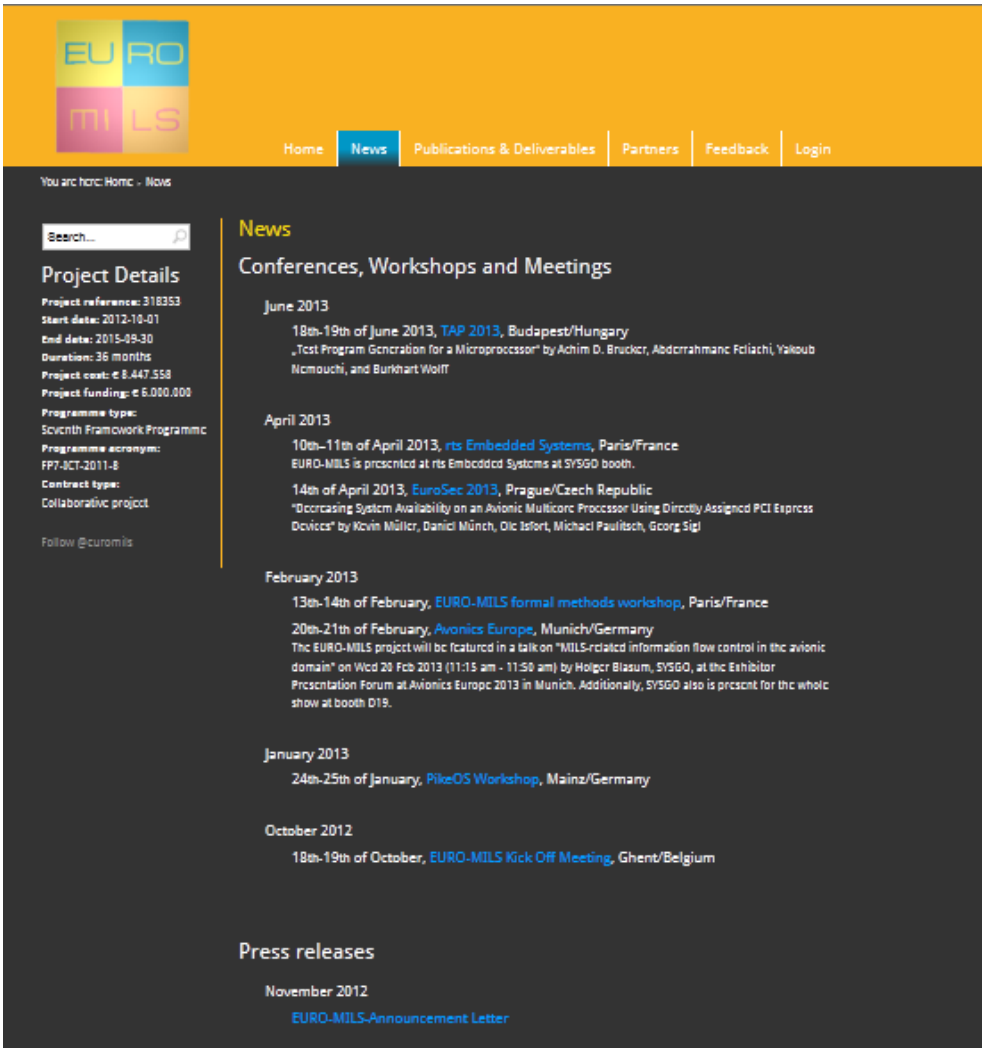

Figure 2: News page of the EURO-MILS website

A statistical analysis of access to the EURO-MILS project website (graphical visualisation) has been created; it is presented in the figure below. The statistics has been generated via *AWStats*. This log analyzer works as a CGI or from command line and shows all possible information in few graphical web pages. It uses a partial information file to be able to process large log files, often and quickly (further information, see http://awstats.sourceforge.net/).The following figure (Figure 3) highlights the first project period from the launch of the website December 2012 to the end of August 2013.

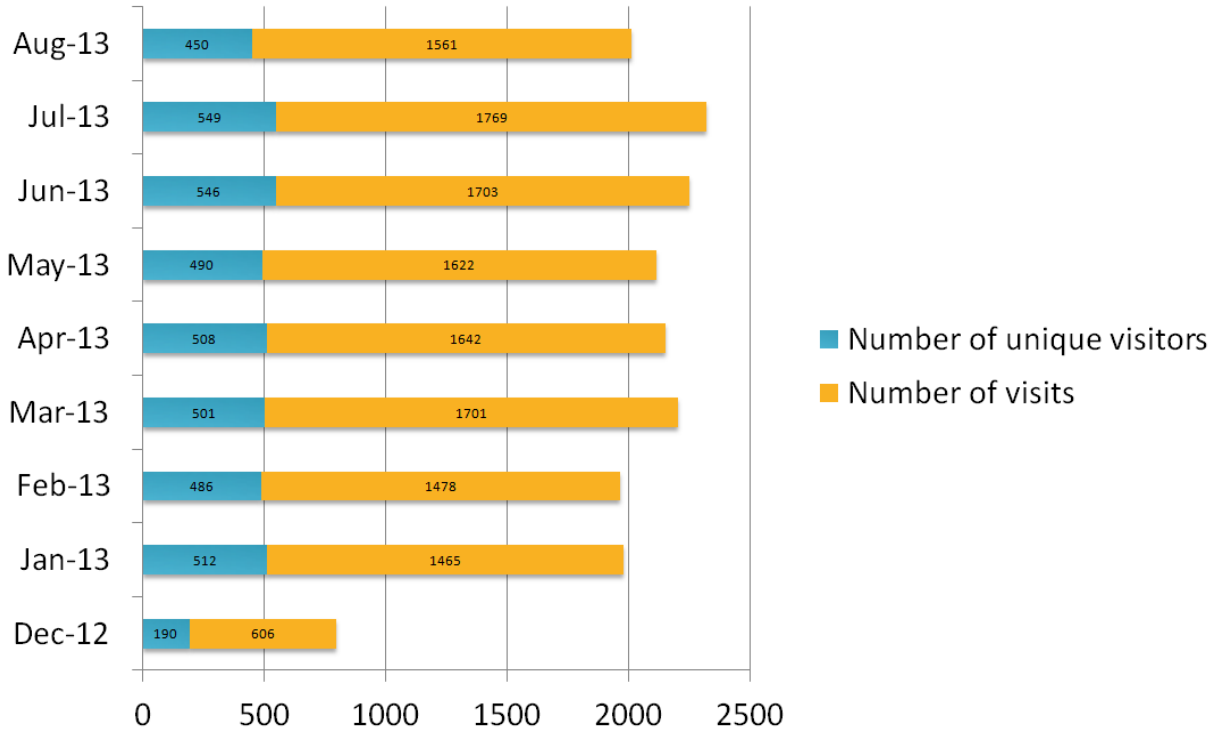

Figure 3: EURO-MILS website visitors/visits

The Figure 4 shows the sources of traffic.

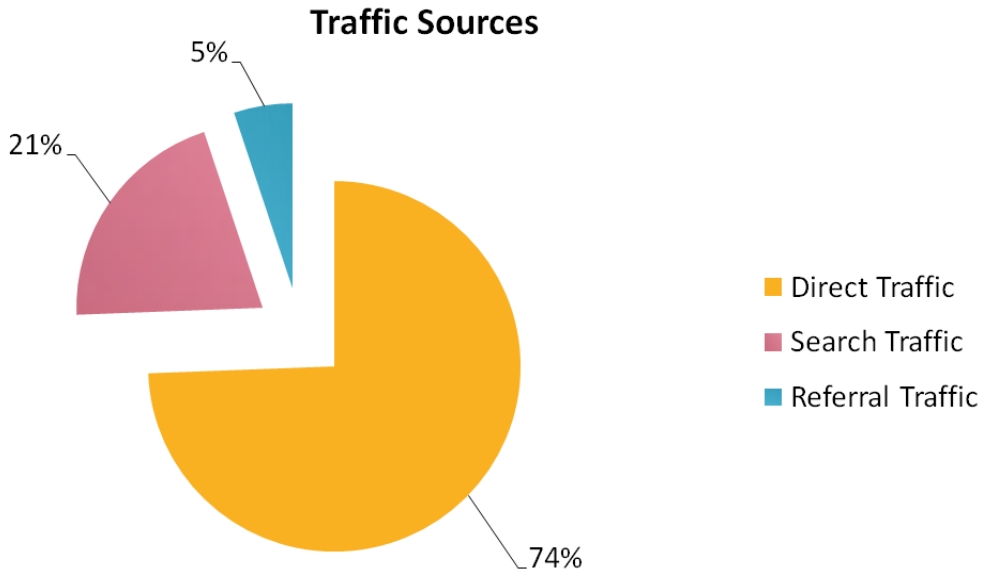

Figure 4: Sources of traffic

An overview of the three top downloaded documents from our EURO-MILS website is shown in the next table (Table 4).

Rank	Name of File	Downloads
1	Announcement Letter	469
2	EURO-MILS leaflet	358
3	EURO-MILS newsletter	137

Table 4: Top downloads

1.2.3.2 Restricted Area of EURO-MILS Website

Beside the public area, there is a password-protected area which is reserved for project participants in order to share project-internal data only (Figure 5). Thus only registered partners are able to enter it and can benefit from the options offered there, e.g.:

- Documentation and tutorials related to EURO-MILS,
- Calendar for appointments and meetings,
- Mailing lists for reaching special mailing groups,
- Archives of the mailing list emails,
- SVN repository,
- Partners' personal profile for managing details.

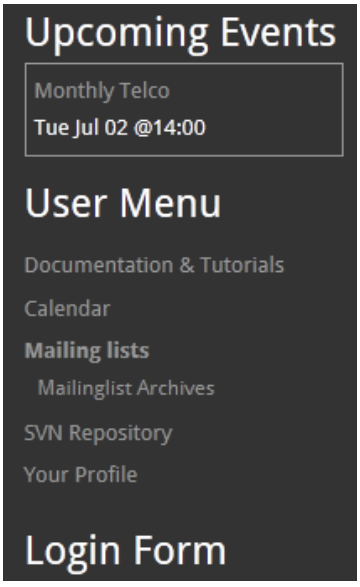

Figure 5: Content of the restricted area

1.2.4 Presentation of the Project to the General Public

1.2.4.1 Web, Flyers and Press Releases and Articles in Popular Press

Type of Activities	Main Leader	Title	Day	Month	Year	Place	Size of Audience	Type and Goal of the Event	Countries Adressed
Press Release	TEC, ALL Partners	EURO-MILS Announcement Letter http://www.euromils.eu/downloads/EURO-MILS_Announcement_Letter_nov2012.pdf	28	11	2012	Online	N/A	Press Release can be downloaded from EURO-MILS website http://www.euromils.eu/downloads/EURO-MILS_Announcement_Letter_nov2012.pdf	International
Web	TEC, ALL Partners	Website / Logo		11	2012	Online	N/A	Official Project Website: http://www.euromils.eu/ Logo will be used for EURO-MILS deliverables/publications	International
Article published in the popular press	OUNL, UGENT	"Europese partners willen EAL7-waardige software met PikeOS", Bits & Chips	14	1	2013	Online	N/A	http://www.bits-chips.nl/artikel/europese-partners-willen-eal7-waardige-software-met-pikeos.html	International
Other	TEC, ALL Partners	Leaflet http://www.euromils.eu/downloads/EURO-MILS_Leaflet.pdf		1	2013	Online	N/A	Official EURO-MILS leaflet can be downloaded from project website; Logo will be used for EURO-MILS deliverables/publications	International
Web	TEC, ALL Partners	EURO-MILS @ Twitter	10	4	2013	Online	N/A	EURO-MILS @ Twitter: http://www.twitter.com/euromils	International
Web	TEC, ALL Partners	EURO-MILS @ LinkedIn	14	6	2013	Online	N/A	EURO-MILS @ LinkedIn	International
Web	TEC, ALL Partners	Newsletter published on website	25	6	2013	Online	N/A	http://www.euromils.eu/downloads/EURO-MILS-Newsletter-Issue-1-June-2013.pdf	International
Flyer	OPSYN	PROJECT - EURO-MILS	1	8	2013	Berlin	N/A	Advertising	International
Article published in the popular press	SYSF, SYSGO	MILS – Multiple Independent Levels of „Sicherheit“, Elektronikpraxis	13	9	2013	Online	N/A	http://www.elektronikpraxis.vogel.de/softwareengineering/betriebsysteme/articles/417913/	International

Table 5: Dissemination activities

1.2.4.2 Project Logo

For the improvement of its visibility, the EURO-MILS project has adopted a project logo (Figure 6). The logo is used on all internal templates as well as on external dissemination tools.

Figure 6: EURO-MILS logo

1.2.4.3 Project Announcement Letter

The intention of the EURO-MILS Announcement Letter was to communicate the project start and ideas towards the general public. It was released in January 2013 giving a summary of the project addressed to non-specialist citizens and outlines what the project is about and how its planned results would matter for citizens and consumers. It can be found on the EURO-MILS website following

http://www.euromils.eu/downloads/EURO-MILS_Announcement_Letter_nov2012.pdf

1.2.4.4 Project Folder

The official EURO-MILS leaflet is a four page informative and graphically appealing A4 flyer, highlighting the objectives and the work programme of EURO-MILS (Figure 7). It can be and has already been used for distribution at conferences or certain other events in order to provide further visibility to the EURO-MILS project. TEC was mainly responsible for the design of the leaflet and distributed it to all partners after finalisation. An electronic version of the leaflet is available on the EURO-MILS website.

http://www.euromils.eu/downloads/EURO-MILS_Leaflet.pdf

Figure 7: EURO-MILS leaflet

1.2.4.5 Project Newsletters

In the first quarter of the project (M09), a newsletter of the EURO-MILS project was launched in order to address project related news (Figure 8). Furthermore, the newsletter offers current information and disseminates important events. The newsletter can be found on the EURO-MILS website and is also posted via the EURO-MILS Twitter and EURO-MILS LinkedIn account to catch further public awareness. It is planned to publish newsletters in a regular basis, in order to keep external partners and the public updated.

Figure 8: EURO-MILS newsletter issue 1

1.2.4.6 Social Media: EURO-MILS Twitter Account and EURO-MILS LinkedIn Group

Making use of the advantages of social media helps spreading project information to a large audience. As a consequence, they are valuable means to disseminate project ideas and results.

Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". The EURO-MILS project is available on http://twitter.com/euromils_project.

LinkedIn is a social networking site for people in professional occupations or simply a social network for business. The EURO-MILS group is a closed group. This ensures that only people who have been approved by the manager or admin can see the content of the group. It can be accessed via http://at.linkedin.com/groups?gid=5065069

1.2.4.7 Cooperation with Other Projects

As part of EURO-MILS project management and dissemination activities, other projects in the same area have been identified. The EURO-MILS project management team at TEC contacted coordinators of these EURO-MILS-related projects and provided them with the most important information on the EURO-MILS-project. The intention is to place the links to the websites of the related projects on the EURO-MILS-website allowing interest groups to come across related projects when visiting our homepage as well as an exchange of experiences between the project consortia. - http://www.euromils.eu/index.php/links

1.2.4.8 Interview for EU Yearbook

Based on an interview given by the Coordinator, an article about the EURO-MILS project will be published in the EU Yearbook, which will be compiled by the Effectplus/SecCord project team. This article is another way of making the public community aware of EURO-MILS.

1.3 Per-Partner Dissemination Plans

In this section, the per-partner dissemination plans are given. Partners have been asked to update their dissemination plans listed within Annex I – Description of Work, if necessary.

TEC: TEC provides the EURO-MILS-project IT-infrastructure – more precisely the whole set of tools which fosters the project cooperation, communication and dissemination, whereby the project website serves as the most versatile external information and communication tool for a worldwide audience. In addition, TEC elaborated a EURO-MILS-project leaflet, a press release as well as periodic newsletters together with the other partners. Furthermore, we intend to widely disseminate the EURO-MILS project ideas and its results at various conferences and workshops and social media. TEC was able to acquire a project booth for the EURO-MILS project at the ICT 2013 in Vilnius. [Updated]

SYSGO: In 2011, SYSGO has actively participated in Embedded World 2011, Avionics Europe, ISORC 2011, Aerodays 2011, HiPEAC Computing Systems Week, NFM 2011, VirtuOS Fachtagung OpenSynergy, Ada Deutschland Workshop 'Development of reliable SW systems', DSEI - Defence and Security Equipment International, Elektronik im Kraftfahrzeug, DASC – Digital Avionics Systems Conference 2011, SAE 2011- Aerotech Congress & Exhibition, Real-Time Embedded Linux Workshop, Aerospace & Defense Meetings Torino, or safetronic 2011. The planning for 2012-2015 is about similar scale, with a stronger emphasis and growth in security R&D; contribution to scientific conferences (in 2011: ISORC, NFM, DASC, Aerotech) will vary according to acceptance of papers. For example, for 2012, we also a plan to submit to the ICCC and the Cambridge Critical Labs safe & secure systems workshop. As the EURO-MILS is a showcase for SYSGO's engineering it will be prominently displayed at these dissemination events. [No updates]

DFKI: As with the other academic project partners, DFKI will exploit the project results for presentations at relevant scientific events (FM, SAFECOMP, CAV, ICCC, ...), publishing of papers, giving courses, lectures, and tutorials to graduated students, and in due course of future research project acquisition activities. No commercial exploitation is planned. [No updates]

UGENT: Ghent University will publish the results of its work on the hypervisor in the scientific literature, and include them in the different undergraduate, graduate and postgraduate courses. Additionally, Ghent University will also actively promote the use of any open source technology coming out of the development of the hypervisor. This will be done through tutorials on international conferences, and through the virtualisation cluster of the FP7 HiPEAC network of excellence, coordinated by Ghent University. This cluster meets 2-3 times per year, and it is an ideal dissemination platform for a European virtualisation platform. UGENT also cooperates with the University of Manchester on ARM virtualisation research. [Updated]

AOS: AOS will present the EURO-MILS project and its achievements to EUROCAE WG72. This dissemination will be done by meeting proposal and presentations. [No Updates]

EADS[3]: EADS IW will disseminate work EADS-internally and externally. Externally, public conferences and workshops are the focus; internally, EADS maintains an internal research technology group networks (called RTGs). EADS IW will disseminate results in these RTGs. [Updated]

[3] EADS IW and EADS F IW updated their dissemination plans in common.

OPSYN: For the dissemination activities in EURO-MILS, OpenSynergy focuses on delivering technical presentations, as well as showing technology demonstrators on high-profile events such as Embedded World (Nuremberg), CeBit (Hannover), Consumer-Electronics-Show (Las Vegas, USA). In addition, dissemination activities will include publications in industry-publications targeting potential customers ("Hanser Automotive", "Automobil Industrie"). [No updates]

PSUD: Université Paris-Sud /LRI will publish the general, re-usable results of its policy-modelling techniques (UPF, other) used in this substantial case-study, and the improvements that the HOL-TestGen System underwent when the system model was explored. The system and library-improvements will be captured in a public release (following prior releases, under Berkeley License). Parts of the project will also inspire technology development in Isabelle itself, which is regularly published as open-source system (with an estimated user-based of 200 persons world-wide). [No updates]

TCS: Thales will publish important results in relevant security conferences (such as ICCC). [No updates]

OUNL: OUNL plans to publish results in scientific conferences and journals. OUNL is considering integrating some of the results in forthcoming course developments. [No updates]

TSYS: There is currently neither international nor national guidance for evaluations beyond EAL6 according to the Common Criteria. Outside the security evaluation, T-Systems closely works with Thales to create an European guideline for application of CC for evaluation according to high assurance levels. TSYS and TCS will jointly document developed / evolved evaluation methodology for high assurance levels up to EAL7 and propose it to BSI resp. ANSSI to enrich German AIS34 and French application notes, resp. The final, reconciled edition of the evaluation methodology shall be pushed by both ANSSI & BSI.

Subsequently, T-Systems will join appropriate international conferences to promote the evaluation guidance for high assurance evaluation in the standards and also to publicly inform about these efforts (example: the annual International Common Criteria Conference). Its dissemination will be supported by its pre-existing standardisation activity in working groups dedicated to smart cards and terminals like ISCI WG1, JHAS, and JTEMS – the JIL Terminal Evaluation Methodology Subgroup. [No updates]

SYSF: SYSF will disseminate the knowledge gained at least at Real-Time Systems, SAE, or various other IC/IP seminars like at Freescale or ARM. Our contribution to scientific conferences like Aerotech or DASIA will vary according to acceptance of papers. As the EUROMILS is a showcase for SYSF security activities it will be prominently displayed at these several public events. [No updates]

JR: JEMM Research will exploit the project results for presentations at relevant commercial events, publishing of research notes, giving awareness lectures to interested embedded IT professionals. [Updated]

Chapter 2 Standardisation

Due to the cross-domain nature of our work, we consider the standardisation setting particular to this project to be characterized by five major standardisation fields: MILS security, MILS API, CC high assurance harmonisation, avionics, and automotive frameworks. Judging from our own experience when participating in e.g. DO-178C standardisation [DO-178C], it is not realistic to predict deterministically how these standardisation efforts will evolve, as a broader community is involved. However, we describe current achievements and developments in each of the areas and we recall that the project is backed by the advisory board consisting of the national German and French IT security agencies BSI (Bundesamt für Sicherheit in der Informationstechnik) and ANSSI (Agence nationale de la sécurité des systèmes d'information), a first advisory board meeting has taken place adjunct to the ICCC in September 2013.

2.1 Standardisation Work in M01-M12

For MILS security, there is not yet an ongoing international standardisation effort. The technical preparation for a contribution to MILS security standardisation in the future has been "built in" into WP12. This specification work is based on the Common Criteria for Information Technology Security (CC, [Com12]) standard and can be used as input for further community-based protection profiles. SYSGO has presented the security target at the national German and French IT security agencies BSI (Bundesamt für Sicherheit in der Informationstechnik) and ANSSI (Agence nationale de la sécurité des systèmes d'information). As additional outreach, our MILS security work has been presented at the ICCC (International Common Criteria Conference) in September 2013. ICCC is the conference for security certification according Common Criteria.

Furthermore, the EURO-MILS partners are developing evaluation methodology for high assurance levels up to EAL7, to later propose it to ANSSI resp. BSI to enrich French application notes and German AIS34, resp. For guidance on use of formal models, PSUD and TCS have identified Eric Jaegers "Remarques relatives à l'emploi des méthodes formelles (déductives) en sécurité des systèmes d'information" [Jae08] as starting point and are working out an adaptation for the Isabelle tool, including guidance both to developers and evaluators of Isabelle/HOL models. For guidance on vulnerability analysis, some partners are considering to work out attack scenarios in the way it has been done by ISCI JHAS (JIL Hardware Attack Subgroup, smart cards) and ISCI JTEMS (JIL Terminal Evaluation Methodology Subgroup, payment terminals) groups, ways to do this have been discussed during the September 2013 EURO-MILS technical meeting.

Concerning MILS API standardisation, SYSGO has already communicated feedback on the "MILS Application Programming Interface for Assured Subject" (MILS API) standardisation to Open Group in July 2013. EADS IW has presented the EURO-MILS work at OpenGroup in August 2013.

SYSGO made contact to members of SC-216, EUROCAE Working Group 72 "Aeronautical Systems Security", within Thales, and for the automotive side, linkage of our work to AUTOSAR and GenIVI industry consortia is ensured by OPSYN. EURO-MILS is also presented to AUTOSAR and GenIVI members by submitting our work in July 2013, at the Embedded Security in Cars (www.escar.info) conference in November 2013.

2.2 Use of Deliverables for Joint Standardisation

Deliverable D12.3 “EURO-MILS proposal for Protection Profile (PP) for a Highly Robust OS in Europe” is, by design, a standardisation proposal that is intended to be the input for a cPP (collaborative Protection Profile). While there is ongoing community standardisation for generic operating systems (OSPP) that targets low to medium assurance, currently there is not yet a comparable community effort for embedded operating systems that have quite different portability and resource usage requirements (real-time). D12.3 aims at being able to put on the table as a proposal for a protection profile for embedded operating systems. Contributions relevant for the PP are expected from TSYS, TCS, SYSGO, SYSF, DFKI. Work on the PP has already benefitted from input from all related partners to the Security Target (D12.2) preceding it.

Additionally, deliverable D33.1 “Addendum to CEM” covers high-level assurance methodology for vulnerability analysis and formal methods in Europe (for example, targeting specifically at standardisation within the SOG-IS framework). Deliverable D33.1 is intended to be written in a form that takes into account similar documentation in the domain of smart cards (JIL JHAS) and payment terminal (JIL JTEMS) communities, where partners TCS and TSYS have standardisation experience.

Automotive and avionics industrial partners have expressed great interest in CC compositional certification. A natural place for the specific aspect of compositional certification in principle can be addressed by both possible standardisation pathways, either by additional guidance how to use the PP for compositional certification or for additional guidance for the vulnerability analysis of composed systems. This would be up-taking work done in the A2 activity track on the CC composite evaluation approach for MILS, including integration of a formal framework.

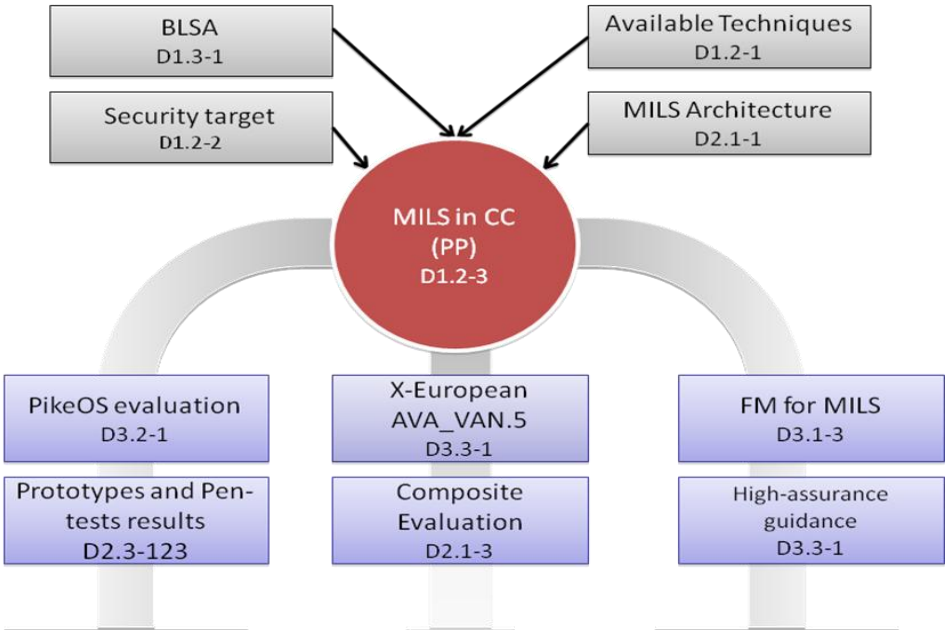

Figure 9: Standardisation as viewed from the perspective of the PP

Figure 9 shows an overview of EURO-MILS deliverables contributing or supporting standardisation from the perspective of the PP: Business, Legal and Social Acceptance (D13.1) of separation kernels, an overview of available techniques for high-assurance CC certification (D12.1), an analysis of the MILS architecture (D22.1) and working out a security target (D12.2) serve as input to the proposal for a MILS separation kernel Common Criteria protection profile (PP). The PP proposal is validated by the prototypes, and penetration testing (D23.1-D23.3), the evaluation of PikeOS (D32.1), composite evaluation (D21.3), and formal models (D31.3) and will the process experience gained can be used for working out a common evaluation methodology (CEM) with special respect to cross-European security vulnerability analysis approaches and high-assurance guidance in general (D33.1).

2.3 Per-Partner Standardisation Plans

2.3.1 Changes to Standardisation Plans

Partners have been asked to update their standardisation plans published within Annex I – Description of Work, if necessary.

TEC: TEC, as coordinator, actively supports the standardisation activities of the consortium and provides assistance where needed and appropriate. [No updates]

SYSGO: Open Group MILS API working group: POSIX is a very successful but large API mainly for desktop operating systems. Therefore, subsets of POSIX for generic embedded systems exist, such as PSE51 (“Minimal Realtime System Profile”). The Open Group MILS API working group is about standardising a subset of POSIX even smaller than PSE51 that can be certified to a high security level. At the moment, the focus of the standardisation work is to include guidance on dependability, to restrict insecure or unsafe usage of API calls (for example, locks). For the future, the WG plans that standardisation work will include formal models of parts of the API. SYSGO is contacting Thales representatives in RTCA 216 (“avionic security”) standard. The production of a Protection Profile also is a standardisation and platform-building activity. To exploit the Protection Profile draft, SYSGO plans to be communicating with interested parties in the field, for example, outreaches have been made to the generic operating system protection profile (OSPP) group and to the creators of the SKPP. SYSGO is also participating in joint work on secure systems and their vulnerability analysis. [Updated]

DFKI: The experience from the CC development and certification activities in this project will not only flow into reports as deliverables of the work packages but also into publications and presentations on conferences, where they may be discussed with representatives of relevant standardisation bodies. An example of such a conference is the International Common Criteria Conference.

The main concern of the DFKI will be the role of Formal Methods within a high level certification and in particular with certification in the context of MILS and separation kernels. In the current version of the Common Criteria the coverage for these aspects is rather unsatisfactory. [No updates]

UGENT: No standardisation plan was listed for UGENT within the Annex I – DoW.

AOS: AOS will contribute to EUROCAE WG72. [No updates]

EADS[4]: EADS IW has been following and contributing to SC-216. EADS is a member of The Open Group. The Open Group targets standardisation of MILS building blocks. EADS follows activities and contributes where appropriate. [Updated]

OPSYN: Where applicable, OPSYN will contribute results from EURO-MILS to AUTOSAR working groups. At the same time OPSYN will feed-back requirements from the AUTOSAR community to the EURO-MILS project. The AUTOSAR working groups OPSYN is active in, "Definition of requirements and analysis of existing solutions in the area of basic software modules and automotive operating systems" (corresponding to generic MILS systems) and "Specification of an AUTOSAR Runtime Environment to provide inter- and intra-ECU communication across all nodes of a vehicle network." (corresponding to the specific router implementation) are highly relevant to the MILS approach and its demonstrators in the project. [No updates]

PSUD: PSUD will participate in the standardisation efforts of this project to integrate the Isabelle Documentation & Test-Case-Generation tool chain into of FM-oriented certification processes. [No updates]

TCS: The EURO-MILS project will allow Thales ITSEF to gain European recognition of its competences through participation to national and European standardisation groups on EAL7 applications notes. TCS is active in ISCI WG1, ISCI JHAS and JTEM and has contributed to the Joint Interpretation Library. [No updates]

OUNL: OUNL plans to contribute to guidelines about assurance cases for CC certification based on theorem proving techniques. [No updates]

TSYS: There are currently neither international nor national guidance for evaluations beyond EAL6 according to the Common Criteria. Outside the security evaluation, T-Systems closely works with Thales to create an European guideline for application of CC for evaluation according to high assurance levels. TSYS and TCS will jointly document developed / evolved evaluation methodology for high assurance levels up to EAL7 and propose it to BSI resp. ANSSI to enrich German AIS34 and French application notes. The final, reconciled edition of the evaluation methodology shall be pushed by both ANSSI & BSI. Accordingly, TSYS is active in Common Criteria smart card and terminal working groups like ISCI WG1, JHAS, and JTEMS – the JIL Terminal Evaluation Methodology Subgroup It will share its experience of having being the driver of the CCDB-2007-09-001 document in the ISCI WG1 that has initiated Common Criteria Composite Product Evaluation (see "Progress Beyond the State of the Art", Section B1.2). [No updates]

SYSF: SYSF will participate with SYSGO in the POSIX MILS API standardisation group. [No updates]

JR: No standardisation plan was listed for JR within the Annex I – DoW

[4]EADS IW and EADS F IW updated their standardisation plans in common.

Chapter 3 Exploitation

3.1 Introduction

Exploitation is recognised as the key enabler for the success of the EURO-MILS project. Hence, all EURO-MILS partners are aware of and committed to the exploitation of the project results. It is the principle of all exploitation activities to use research results to create value within all participating organisations and thus to improve their competitive advantage. Only by scaling up the results into commercial offerings, all European constituents can be reached while ensuring profitability through economies of scale.

Wherever possible, research results will be used for the creation and support of new products and services. These products and services will lead to a competitive advantage of the participating organisations and will substantially contribute to the benefit of the targeted constituents. In order for the exploitation to be effective, an integrated approach will be necessary, combining experience and expertise from the development department and solution management, and the involvement of a user base represented by the consortium partners and industrial contacts.

3.2 Preliminary Market Overview

One of the goals of the project is to understand the affinity of EURO-MILS outcomes to different markets. This process is based on market analysis, interviews with industry professionals, and background researches. JR has started the interview process and a preliminary analysis is given in the following paragraphs.

Based on the analysis outcome, a small number of core target markets will be identified. For these core markets, further background researches, including analysis of 3rd party market research, will be done within EURO-MILS. Results will be reported to project partners on a regular basis and via D13.1.

3.2.1 Feedback from Industrial Contacts

The ongoing activity of research on business acceptance and business value in EURO-MILS within the first year has created 39 documented interviews from different markets. The main focus of EURO-MILS is on automotive and avionics markets. To understand its value in other markets, an informal Industry panel have been constituted. 236 professionals in different industries (see Figure 10) have been personally solicited to participate in the panel, 71 answered (30%) and 39 persons (16%) were interviewed. During a phone conversation, the interview consisted in a EURO-MILS presentation, followed by a guided discussion on “security / safety”, “virtualisation / partitioning” and “certification / user acceptance”.

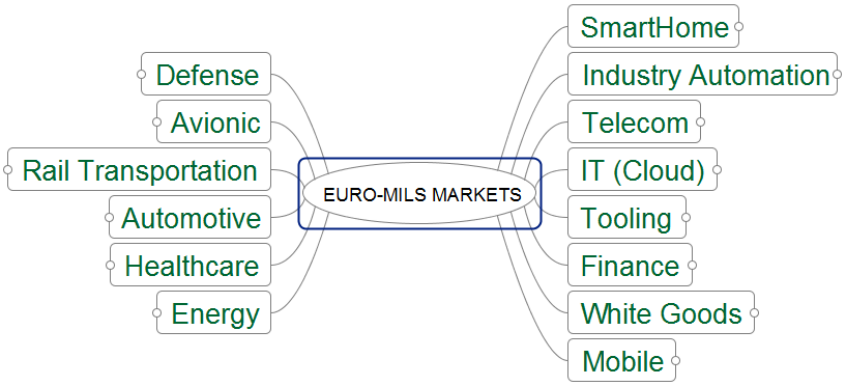

Figure 10: Markets targeted by industrial contacts

3.2.2 General Market View

As a general feedback, the industry is very interested in project and its output. "*Interesting stuff you're working on, all the best!*" is an example of a feedback. Some organisations want to organize specific follow-on with the project to explore, for example, "*how this technology could be adapted to the PC and the Cloud Computing*" or "*to discuss virtualisation and security*" for set-top boxes. Although impossible, one university wanted to participate in the project: "*My head of lab asked me to tell you that we are ready to apply for partnership.*"

3.2.3 Security and Safety

In the different industries considered, there are still lots of ambiguities in the definitions and the understanding of security and safety. This was expected as the two concepts are very close and, even in our project, the avionic demonstrator will implement "Security for Safety".

The second general feedback is that many markets do not integrate yet security requirements. Some (for example home automation) focus on interoperability and integration, others, (for example telephony) focus on Time to Market but all panellists recognize that Mobility, Internet of Things or M2M will have a big impact on communication security with a strong confidentiality requirement. In the mass markets, there is also a concern on how to secure products without slowing down business.

As an early conclusion on Security, we can quote one panellist, "*Fear [*will be*] the primary motivation for Safety and Security.*"

3.2.4 Virtualisation and Partitioning

Many industries require installing or updating independent software stacks with different criticalities in their embedded systems (for example, the Set-top box (phone and television services), Mobile (personal and professional areas)), therefore partitioning of the EURO-MILS platform is an interesting capability for different markets.

Many industries are working on virtualisation to implement partitioning and evaluating both hardware and software mechanisms. They target a mix of the two solutions. They also try to leverage the multicore complexity of the new chips in their products as the "*hardware capability is much ahead of the industry requirements*".

Complexity can be a barrier in the consumer markets where Time-to-Market and product evolution are key. Costs need also to be kept under control for mass-market products (smartmeter, mobile).

3.2.5 Certification and User Acceptance

One of the feedbacks about Common Criteria certification was its complexity that will increase with virtualisation and multicore. Cost and length of certification are also in the mind of all participants.

Two interesting questions come out of the conversions around certification.

First, different industries have different positioning relative to the security certification authorities. They wonder: what is the value of the authority compared to the value of the product or service supplier. In the avionic market, the role of the European Aviation Safety Agency makes a consensus when it comes to safety and security. However, customers make their market decisions more on reputation of an automaker (for example BMW) for selling safe cars rather than by studying the levels of compliance to the related safety regulations issued by a government authority.

Second, some industries are wondering if the Common Criteria and its defined processes can react rapidly enough to quickly evolving security requirements and changing developments in information security technologies.

3.3 Use of Deliverables for Joint Exploitation

A core pillar of the project is leadership by example in certification. The deliverable D12.2 “Security Target (ST) for a Highly Robust OS in Europe” is exploited for a Common Criteria (CC) evaluation of the PikeOS operating system, flagship product of SYSGO and SYSF. Together with the Common Criteria D32.1 “Complete evaluation technical report”, that is the main artefact in a Common Criteria certification, it is immediately exploited by doing such a certification within the project. Naturally, the certification partners as well as the developer benefit from the exercise. In a broader sense, in a vertical marker view, the availability of a certified embedded operating system is also very useful to European system builders. In a horizontal market view, doing first certification lowers the barrier of entry for future market participants.

Secondly, the deliverable D22.1: “MILS virtualisation platform implementation on adapted PikeOS, board support documentation” leads to work on Board Support Packages, documentation and drivers for components. Within this context, improvements of PikeOS will go into the PikeOS product at SYSGO and SYSF. Similarly, the deliverable focusing on a multi-architecture module for secure concurrent IO (D22.2) is to be directly exploited by SYSGO and SYSF in the PikeOS product. The IO/MMU framework is to be integrated closely into the kernel. Partners gain experience in the development of drivers that are e.g. aware of SR/IO and can reuse this know-how for driver development within separation kernels.

The avionics prototype (D23.1) is to be industrially exploited by the avionics partners AOS, EADS IW and EADS F IW for a potential future aircraft device, as well as a showcase by SYSGO and SYSF. Avionics partners also note that the experience gained in EURO-MILS will be useful for the development of similar product variants. Due to the interoperability of the developed MILS architecture, the exploitability of the avionics prototype does not depend on specific separation kernel. Similarly the automotive prototype (D23.2) is to be industrially exploited by the automotive partner OPSYN and some of the automotive EURO-MILS results are already expected by customers. Both prototypes are supported by the work on test beds focusing on MILS properties. We expect that MILS test scenarios are to be integrated into the test suites by the provider of the separation kernel as well by the automotive and avionics partners.

3.4 Per-Partner Exploitation Plans

3.4.1 Changes to Exploitation Plans

Partners have been asked to update their exploitation plans published within Annex I – Description of Work, if necessary.

TEC: For the last 14 years, our business has been to provide both general and engineering services for technology-related challenges. Our general services focus on feasibility studies, the creation of business plans and the planning and management of industrial research activities. Our core customers are early adopters of new technologies and we will use the knowledge created within the project to strengthen our image as technology scout and spearhead. Participation in this project leads to the early identification of novel technology, which is a prime asset for our business success. Our requirement engineers will sharpen their expertise while working together with some of the world's leading industrial scientists in this project. As an emerging SME, the reputation gained from the project will positively influence our future acquisition activities. TEC's "Trusted knowledge Suite", a workflow based management support system, has highly benefited from its employment in European research projects. Critical project users have constantly triggered improvements and the introduction of new features which elevated the market position of our IT tool. [Updated]

SYSGO: So far, the products of SYSGO are mainly used in safety-critical applications (within the meaning of functional correctness). In addition to the functional safety security issues (e.g. secure authentication, access control and integrity of data) play an increasingly important role. Accordingly, in the "Embedded Security" the highest growth rates are expected (see, e.g. market analysis VDC "Embedded Software Market 2009"). The results of the EURO-MILS project will broaden the product PikeOS from a safety-certified kernel (in very high assurance avionics, but nonetheless specific, deployments) to a MILS platform in the broad sense that is a system that includes deployment-independent end-user trust by high-assurance security certification. Close cooperation with partners from airspace and automotive industries will ensure the market orientation of that solution. On the one hand the growing security requirements in the traditional markets such as avionics and automotive are met, but also new markets to be addressed in the high security area. There are currently no national or European suppliers. Our medium term goal is to provide a European alternative to the predominantly American suppliers. SYSGO membership in the Thales group gives assurance of long-term availability and sustainability of the PikeOS product.

Demonstrators will show applicability of the MILS architecture developed in D2.1 and PikeOS as its MILS core. This will give SYSGO a strong position and head-start. Results of Activity A3 with Common Criteria reports will enable to address existing customer requests for CC certification in short to mid- term time. [Updated]

DFKI: DFKI operates an official Common Criteria evaluation facility approved by the Federal Office for Information Security (BSI), and uses its expertise in CC-compliant development, software safety and formal methods in the context of advisory and training roles. The project will strengthen the position of DFKI in several ways and increase its market potential. Not only for economic reasons, separation kernels will serve as the foundation and central part of a steadily growing number of secure software systems. As a result, it is expected that this type of systems will amount to a substantial portion of the consulting and development services for secure systems provided by DFKI. In terms of formal development techniques, EURO-MILS promises a significant advance in the area of largely standardised security modelling and a methodological integration of verification techniques.

Furthermore, the competence of the DFKI will be strengthened significantly with respect to evaluation of high-security operating systems. Given the increasing importance of such

systems, this will constitute a promising business area and a solid foundation for further application-driven research activities. [No updates]

UGENT: Ghent University will use the infrastructure developed in the project in current and future research projects. In particular, PhD students will be able to take advantage of the work done in this project to reduce the amount of engineering work they have to do before they can start working on their actual research. [No updates]

AOS: AOS will spread the knowledge built in this project in several Airbus departments, specifically for internal supplier teams and security teams. Further AOS (together with EADS) brings in a use case for a potential future device in an aircraft via its use case. The knowledge obtained via the demonstrator built during the EURO-MILS project can be transferred to future variants of similar product and part of products. [Updated]

EADS[5]: EADS IW is part of the EADS group with the current business units Eurocopter, Cassidian, Airbus and Astrium. EADS IW itself does not hold any products and hence can only exploit the Euro-MILS project via its business units. It will inform different BU on the progress.

Furthermore, AOS and EADS bring in a use case for a potential future device in an aircraft via its use case. The knowledge obtained via the demonstrator built during the Euro-MILS project can be transferred to future variants of similar product and part of products. [Updated]

OPSYN: With COQOS, OpenSynergy provides an automotive solution to integrate different types of applications on one platform. Strengthening security aspects of COQOS enables OpenSynergy to better address the marked needs in the future. Key results from the project will become part of Open Synergy's COQOS operating platform. OPSYN will use the software developed for secure software update and device management as part of its existing product COQOS. As COQOS uses PikeOS as a microkernel solution, the results about certification and formal verification of the microkernel will be directly relevant to open up new market opportunities for automotive embedded systems with higher safety requirements. OPSYN expects the formal verification methods developed in the project to also contribute to ISO 26262 compliance, which will be necessary for future automotive safety relevant systems. The project will also further deepen the collaboration between SYSGO and OPSYN. OPSYN will periodically present the results of EURO-MILS in internal review meetings. For those meetings, interested developers, as well as the general management will be invited, potentially in different types of meetings. [No updates]

PSUD: PSUD will contribute to Isabelle (Kernel optimisation, support for anti-quotations specific to software-engineering processes). Results will be published as part of the Isabelle Releases. Furthermore, PSUD will continue its tradition to organise Isabelle Developer Workshops; this can be used also for internal communication inside the project to use new techniques in propagation. Research results on modelling and test-generation will be published in international conferences such as ITP, FM, ICST, ICTSS, (for which group members have been member of the program committee or chair). [No updates]

TCS: Thales will strengthen its position in product evaluations to higher EAL of the CC. The project will also allow to gain the needed experience to create an evaluation approach for higher and highest EAL of CC and push it on both European and international levels. At the same time, the EURO-MILS project will allow Thales ITSEF to gain European recognition of its competences through participation to national and European standardisation groups on EAL7 applications notes. [No updates]

OUNL: No exploitation plan was listed for OUNL within the Annex I – DoW.

[5] EADS IW and EADS F IW updated their exploitation plans in common.

TSYS: The project will strengthen the position of T-Systems in security evaluations on higher EAL of Common Criteria. Developing the evaluation methodology for evaluation on the highest EAL will generalise the experience gained in the project. Making this methodology available to European and international community will extend business opportunities for the evaluation facility of T-Systems. [No updates]

SYSF: SYSGO SAS will integrate the modularisation into a new driver MILS compatible framework. The framework has two major expected outcomes:

- Match the development of drivers to the MILS requirements by providing an API for both trusted and untrusted drivers.
- In general, by providing a security-aware interface to the MILS kernel, give guidance for security-aware applications.
- Moreover, SYSGO SAS intends to profit from SYSGO's contribution (CC evaluation) as on the French market there is a huge interest in high-assurance solutions for critical systems.
- Demonstrators will show applicability of the MILS architecture developed in D21.1 and PikeOS as its MILS core. This will give SYSGO a strong position and head-start. Results of Activity A3 with Common Criteria reports will enable to address existing customer requests for CC certification in short to mid- term time. [Updated]

JR: JEMM Research is a European research and advisory firm. The project will strengthen the position of JEMM Research in the world of embedded IT and increase its market potential. As embedded systems become ubiquitous, embedded IT end-users and providers will have to set up a strategy to identify and capitalize on these new opportunities. Furthermore, the competence of JEMM Research will be strengthened significantly with respect to evaluation of virtualisation, security and safety markets. Given the important of such domains, this will constitute a promising business area and a solid foundation for further research activities. [No updates]

3.5 IPR Issues Identified in the EURO-MILS Project

In the environment of international applied research projects with industrial partners such as EURO-MILS, the careful handling of intellectual property rights (IPR) issues is of strategic importance. Within the EURO-MILS project, many individuals of numerous organisations cooperate across national borders. In order to develop novel technologies, concepts or processes, exchanging information with other parties is a necessity. Furthermore, jointly creating new intellectual properties is common. Therefore confidentiality is a very important issue for participants in EURO-MILS, from the project start-up phase of joint activities to the implementation phase and further to the exploitation of results.

All efforts related to IPR issues aim to create a favourable environment for respecting IPR. Without IPR protection the joint creativity of natural persons or legal bodies as well as the dissemination and exploitation of results would be highly restricted not to risk a substantial drain of knowledge. Intellectual property (IP) is an intangible asset and created as a result of intellectual creative effort of the human mind in relation to works of authorship and/or inventions. With the ownership of intangible assets certain legal exclusive property rights which are established by law or by contractual obligation are connected and maintain the control in relation to the protection of the interests of the creators by excluding these creations from public property. This means that right to permit or deny the use and exploitation of the creative work. So IPR provides a protection of the creations and inventions to the owners by preventing users from using or copying them without reservation or payment for a certain period of time.

Intellectual property can be classified into:

- Industrial property items like inventions which can be a product or a process providing new solutions for solving (technical) problems and which can be protected by registering a patent and
- Copyright items which provide exclusive rights to the creator to prohibit the authorized copying, adaptation and reproduction of its intellectual work.

The protection of the knowledge developed within EURO-MILS is vital for each of the participants.

3.5.1 Prerequisites for the EURO-MILS Project

The management of intellectual property in EURO-MILS was already important at the project proposal set-up stage where the first development of appropriate ideas for the joint research activities and the assembling of the project consortium took place.

Even at this early stage, discussions and exchange of information between different people from institutions with different knowledge, background and interests was required and IPR issues needed to be discussed and integrated into the appropriate sections within the proposal.

Later on, the grant agreement (GA) represents a contract which establishes the beneficiaries' rights and obligations towards the European Community and towards each other. It contains a specific provision on confidentiality that defines the obligation and its term. Moreover, it also covers an intellectual property related section.

Furthermore, in order to guarantee a uniform approach by the EURO-MILS participants, internal rules should be defined, including confidentiality clauses for the use of dissemination of results, which can be incorporated in the consortium agreement (CA).

In the present section, all stages and contracts, which are important IPR prerequisites for the project set-up will be briefly explained, with the focus on their implementation in the EURO-MILS project.

3.5.2 Drafting of Proposals

In writing the project proposal for EURO-MILS, the management of IPR was already outlined because the exchange of information between the partners in such an early stage is of certain risk. Although copyright allows some legal protection against unlawful copying of works, all parties should nevertheless only reveal any such information under terms of confidentiality in order to protect the contained ideas in a broader sense.

During the EURO-MILS proposal drafting phase, it was laid down that the consortium agreement, as an outline contract between the partners, would define the rules and measures as well as the rights and duties for protecting the IP within the EURO-MILS project. Through signing the consortium agreement and its confidentiality clauses the EURO-MILS partners committed themselves to protecting the confidential information brought into or resulting from the EURO-MILS project. Also plans for the use and protection of the results have been considered (more in "Consortium Agreement" chapter).

Additionally, the management structure has been set up with the protection of knowledge in mind, which foresees the permanent monitoring of IPR issues during the project.

3.5.3 Contracts

Within the EURO-MILS project, two agreements have been prepared, which all partners had to sign in order to participate in the project: the grant agreement and the consortium agreement. Both of these agreements include IPR regulations for the project and therefore represent the contractual basis for IPR within EURO-MILS.

3.5.3.1 Grant Agreement (GA)

The grant agreement is the contractual basis for the European Commission (EC) funded project EURO-MILS, which is the principal agreement between the EC and the coordinator. This contract sets out in writing the key project details such as the parties involved, the scope, the duration and start date of the project, the reporting periods, the maximum financial contribution of the EC, the main contact data of the contracting parties as well as some specific issues.

It was clear to the project partners from the beginning that due diligence would be required with regard to confidentiality. Therefore they determined the level of confidentiality of information that would be provided in deliverables throughout the EURO-MILS project when the work to be done in the project was defined and stated in Annex I to the GA.

3.5.3.2 Consortium Agreement (CA)

The consortium agreement is signed between the project participants of the consortium and implements the grant agreement, establishing provisions related mainly to consortium management, the distribution of the Community financial contribution and IP. The CA is a negotiated and agreed mandatory contract between the project partners, which has to be signed by all partners before the entry into force of the Grant Agreement. The legal requirements are singled out in the Grant Agreement but the details regarding the cooperation are given in a specific Consortium Agreement. The EURO-MILS Consortium Agreement was signed by all partners in October 2012 and it sets out the internal management guidelines for the consortium including established rules, structures and processes for handling IPR.

The CA includes guidelines for the project internal management of the cooperation by providing rules for the following issues:

- the parties' obligations for the implementation of the GA
- project internal organisation and project structure (project bodies and their functions, rights and duties, voting regulations)
- handling of commission payments (distribution of the funding by the coordinator)
- provisions about the ownership and licensing of intellectual property (e.g. foreground, publications, access rights, dissemination of results)
- handling of matters of liability and confidentiality
- procedures for settling internal disputes
- handling of defaults and remedies (exclusion/withdrawing)

Knowledge, or foreground[6], generated within the project will be protected by patent filing or publication in accordance with the consortium agreement that also represents an outline

[6] **Foreground** is understood to be tangible and intangible project results in terms of information, materials and knowledge generated inside the project. Foreground is principally owned by the partner who generated it; when

contract between the partners. The status of background[7] and sideground[8] brought in or developed in parallel is also covered by the CA. Amendments to the CA can be done on a per partner basis as the needs for knowledge and protection varies between the partners. With their signature of the CA, all partners agreed to the content of the binding Agreement.

Besides the general principles relating to access rights, the EURO-MILS CA deals with clauses concerning access rights for affiliates as well as special provisions concerning access rights to software, standards and access rights for parties joining or leaving the project. Furthermore, the CA covers rules regarding the confidentiality period, exceptions, disclosure of confidential information in compliance with a court order and to the Commission as well as disclosure of confidential information to affiliates and it covers regulations regarding the disclosure of results to the public as well as the provided information to the EC.

3.5.4 Status Quo of the Project with Regard to IPR issues

On the basis of the above-mentioned contractual framework defined and agreed in the run-up to the project, the relevant intellectual property rights must be maintained during the project. Therefore, the management structure, workflows and tools are designed with the protection of knowledge in mind. The project management is responsible for the monitoring of IPR issues. All partners are obligated to report any protection of intellectual property to the project management.

New knowledge produced during the project belongs to the supplying partner and any commercial exploitation or public disclosure of new knowledge can only be done after the owner gives his consent. The decisions to patent any results belong to the owner; the other partners must not interfere in this process. In case of jointly developed new knowledge the ownership needs to be agreed upon before any dissemination and/or exploitation.

The protection of knowledge, or Foreground generated within the project, is vital for each of the EURO-MILS participants and is mainly realised by patent filing and/or publications.

The following subchapters should provide an insight regarding the current situation concerning different IPR issues within the EURO-MILS project.

3.5.5 Licenses

EURO-MILS uses several software products, that are protected by licenses and therefore need to be distributed, as follows:

SYSGO distributed PikeOS licenses to partners in order to work within the project.

PSUD: Isabelle/HOL and Isabelle/HOL-TestGen belong to the background; they are both under BSD Licence. Isabelle/HOL and Isabelle/HOL-TestGen remain under BSD Licence including newer versions released during the project.

OPSYN: In addition to PikeOS licensed by SYSGO, OPSYN uses the COQOS license (OPSYN) for EURO-MILS work.

---

the generation of the foreground is a joint process, it is - unless the partners do not agree on another solution - jointly owned by the participants.

[7] **Background** is understood to be information, knowledge and any IPR relevant to the project already held by the project partner before the accession to the EC Grant Agreement.

[8] **Sideground** is intellectual property created during a contract but which is not considered to be part of the contract.

3.5.6 Patents

Until now, no patents were applied in reference to work generated within EURO-MILS. However, it is a possibility that patents will emerge from results obtained in the EURO-MILS project.

3.5.7 Copyrights

In general, there were no copyright issues taken into the EURO-MILS project. Therefore, it was not necessary to take this into account. By default, everything developed by a partner is copyrighted by this partner, unless it is explicitly given a different status. The following partners gave further details on copyrights issues:

UGENT: The copyright on software developed by UGENT belongs to UGENT and will be shared/licensed according to the consortium agreement terms and the dissemination status as described in the DoW.

PSUD: .The copyright of publications has been transferred to Springer Verlag according to general agreement in the consortium.

TSYS: According to sec. 8.3.5 of the Consortium Agreement, TSYS as a licensed evaluation facility acts according to the BSI Common Criteria certification scheme. The copyright of TSYS is applicable to all the items stated in Attachment 2, letter e. of the Consortium Agreement. It means a.o. that the analysis, evaluation methodology and tools developed by TSYS remain in its ownership as well as all the reports by TSYS documenting evaluation results.

3.5.8 Violations

During the preparation phase of this document, all EURO-MILS partners were asked whether they noticed any violations concerning IPR issues inside or outside of the project and none of them reported anything in this regard.

3.5.9 Partnerships with Other Projects/Partners Outside EURO-MILS Dealing with a Related Topic

Also in partnerships with other projects or partners, it is necessary to adhere to the IPR regulations and to share only ‘public’ EURO-MILS-related information.

There have been several partnerships with other projects or partners dealing with a topic related to EURO-MILS which were for example:

During the pre-project phase DFKI participated in the German BMBF project SeSaM. Partner UGENT coordinated the virtualisation cluster in the HiPEAC and HiPEAC 2 Networks of Excellence.

EURO-MILS established relationships with related FP7- and national projects (contacted projects: DMILS, WEBSAND, ARAMiS, SESAMO, Multipartes). The technical leader of EURO-MILS, SYSGO is in deep contact with the D-MILS project and the SESAMO project.

Currently, the partner DFKI participates in the EU-project KIARA. Partner UGENT has a joint project with the University of Manchester concerning the development of an ARM hypervisor. Partner AOS participates in several EADS internal projects on related topics. Furthermore, partner EADS takes part in the German ARAMiS project in which 30+ partners research on safe and secure use of mulitcore processors. EADS also participates in the German SIBASE project which deals with the use of embedded communication and computing elements in secure systems and the ARTEMIS project SESAMO which focuses on research on overlaps

on safety and security in architectures and tools. PSUD has a partnership with System X of my group, where other partners (CEA, Trusted Labs, Thales) work on a PikeOS-like platform, but has no direct working contact to them in this project. PSUD joins other partners (SAP) in vaguely related issues (no development involved).

Partner DFKI has planned to remain active in EURO-MILS related projects in the future. AOS will continue to participate in several EADS internal projects on related topics. Partner EADS will stay involved in the ARAMiS, SIBASE and SESAMO projects.

3.6 Project Results

The following subchapter describes the development of project results (deliverables, reports and scientific publications) as well as the regulations of such results within the EURO-MILS project.

3.6.1 Deliverables

All project participants are obliged to take care that the information provided in the deliverables and reports corresponds to the IPR regulations, especially when compiling public deliverables and reports.

In order to ensure that only public content is contained in public deliverables and that IPR rules have been considered, the EURO-MILS consortium defined an internal review process for deliverables.

This process requires the approval of both the Project Management, and a reviewer external to the work package, before a deliverable is released. This ensures that the qualitative targets are reached with regards to technical content, the objectives of the project and adherence to formal requirements established in the GAs and CAs.

Figure 11: Deliverables and publications process

The editor is responsible for appointing an external reviewer and sending a draft to the Project Management at least 21 days before the planned publication or delivery. This draft is also sent to the internal reviewer. A copy is similarly sent to owners of Intellectual Property related to the content. The reviewer and Project Management shall send their comments back to the editor within 5 days. The editor updates the deliverable within 5 days and sends it back to the Project Management for final approval.

The deliverable will be forwarded to the Coordinator who submits it to the Commission. The editor of any deliverable is by default the work package leader. It is the responsibility of the work package leader to ensure that the review form has been filled out correctly.

Review Form
for Project Management and Internal Reviewer

	Project Management:			Internal Reviewer:		
	Answer	Comments	Type*	Answer	Comments	Type*
1. Is the deliverable in accordance with						
(i) The Annex I - Description of the Work?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) the international State-of-the-Art?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
2. Is the quality of the deliverable in a status						
(i) which allows to send it to the EC?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) which needs improvement of the writing by the author of the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(iii) which needs further work by the partners responsible for the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a

Figure 12: Deliverable review form

3.6.2 Scientific Publications

For scientific publications, we use a publication mailing list to notify all partners about any future paper submission in order to prevent possible IPR conflicts. The basic rules are that the notification should be send 45 days before the submission as foreseen in the Consortium Agreement (CA 8.3.1). However, the EURO-MILS Consortium has agreed that it can be sent at least 1 week before and should contain the following information:

1. Title
2. Authors
3. Abstract
5. Connection to EURO-MILS
6. Is/Will open access provided to this publication?
7. SVN URL of the draft/Attach Draft
8. Target date and conference/journal (including URL)

One further rule is that the acknowledgement clause has to be part of the acknowledgements of each article: *"The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n°318353 (EURO-MILS project: http://www.euromils.eu)."*

Chapter 4 List of Abbreviations

Note: Abbreviations of partner names are given in the frontmatter on page I.

ANSSI	Agence nationale de la sécurité des systèmes d'information
BSI	Bundesamt für Sicherheit in der Informationstechnik
BU	Business Unit
CA	Consortium Agreement
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
GA	Grant Agreement
ICCC	International Common Criteria Conference
IO/MMU	Input/Output Memory Management Unit
IPR	Intellectual Property Rights
ISCI	International Security Certification Initiative
ISO	International Organization for Standardisation
JHAS	JIL Hardware Attack Subgroup
JIL	Joint Interpretation Library
JTEMS	JIL Terminal Evaluation Methodology Subgroup
MILS	Multiple Independent Levels of Security
MMU	Memory Management Unit
OSPP	Operating System Protection Profile
PP	Protection Profile
RTES	Real-time embedded system
SOG-IS	Senior Officials Group Information Systems Security
SR/IO	Single-Root Input/Output

Bibliography

[Com12] Common Criteria Sponsoring Organizations, Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 4, vol. 1--3, September, 2012, http://www.commoncriteriaportal.org/cc/.

[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.

[Jae08] Eric Jaeger, Remarques relatives à l'emploi des méthodes formelles (déductives) en sécurité des systèmes d'information, 2008, http://www.ssi.gouv.fr/IMG/pdf/ssi_formelle.pdf.