Project no: 100204

pSHIELD

pilot embedded **S**ystems arc**HI**tectur**E** for multi-**L**ayer **D**ependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems / Rail Transportation Scenarios

Liaisons Report

For the
pSHIELD-project

Deliverables D1.2.1

Partners contributed to the work:

SESM, Italy
Ansaldo STS, Italy
Critical Software, Portugal
Selex Elsag, Italy
THYIA, Slovenia

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2012)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Authors and Approvals

Authors		Date	Signature
Name	Company		
Przemyslaw Osocha	SESM		
Gareth May-Clement	CS		
Roberto Uribeetxeberria	MGEP		
Marco Cesena	SE		
Francesco Flammini	ASTS		
Eguia Elejabarrieta	Tecnalia		
Andrea Fiaschetti	UNIROMA1		
Paolo Azzoni	ETH		
Spase Drakul	THYIA		
Reviewed by			
Name	**Company**		
Marco Cesena	SE		
Approved by			
Name	**Company**		

Modification History

Issue	Date	Description
Draft A	25 February 2011	Initial Draft Structure
Draft B	12 December 2011	Incorporates comments from Draft A review
Issue 1	22 December 2011	Incorporates comments from Draft B review
Issue 2		Incorporates comments from issue 1 review

Contents

1 Introduction 6

2 Liaisons activities 7

2.1 Liaisons at events 7

2.1.1 ARTEMIS & ITEA2 Co-summit 2011, Helsinki 7

2.1.2 ARTEMIS & ITEA2 Co-summit 2010, Ghent 7

2.1.3 Other events 7

2.2 On-line liaisons 8

2.2.1 On-line collaboration tools 8

2.2.2 Projects' exchange of information 8

2.3 Partners liaisons 8

2.3.1 Ansaldo STS Liaisons 8

2.3.2 Critical Software Liaisons 9

2.3.3 Eurotech Liaisons 9

2.3.4 Mondragon Goi Eskola Politeknikoa Liaisons 9

2.3.5 SESM – Finmeccanica Liaisons 10

2.3.6 SELEX Elsag Liaisons 10

2.3.7 Tecnalia Liaisons 12

2.3.8 Università di Genova Liaisons 12

2.3.9 Università di Roma Liaisons 13

2.3.10 THYIA Liaisons 13

3 Conclusions 14

Glossary

ESs	Embedded Systems
SPD	Security Privacy Dependability
FSK	Frequency-Shift Keying
AFSK	Audio Frequency-Shift Keying
UCS	Use case Scenario
HW	Hardware
SW	Software

This Page is intentionally left blank

1 Introduction

The goal of this deliverable is to report liaisons established with other EC FP7 and Artemis funded projects, concerning topics related to pSHIELD to share and improve the results of the single project and of the whole Artemis technology platform. Such relations permit for a useful exchange of knowledge among consortia and an improved, coordinated and synergetic continuation of the standardization processes.

The SHIELD identified technologies and solutions will represent a reference guideline for the design and development of ESs where SPD capabilities are required. In particular, the SHIELD results will be used for the cross fertilization among projects and will be available for possible reuse to provide SPD features to the ESs that might be designed and developed in other projects.

2 Liaisons activities

2.1 Liaisons at events

Very important possibility to exchange information on the project achievements between pSHIELD and other projects are organized events, like conferences, meetings and exhibitions. In particular Co-summit exhibition organized every year is place where ARTEMIS JU and ITEA2 projects are presented in public.

2.1.1 ARTEMIS & ITEA2 Co-summit 2011, Helsinki

Co-summit 2011 'Cross border cooperation for Clean Technologies' was the fourth edition of this annual event took place on 25-26 October 2011 in Scandic Marina Congress Center in Helsinki, Finland. The project exhibition, showcasing active projects of ARTEMIS and ITEA, highlighted this event. Interesting key notes, ARTEMIS and ITEA sessions completed this annual get-together of European embedded systems community.

The event is hosted by the ARTEMIS Joint Undertaking and ITEA 2. Both organisations are active to help Europe to achieve and maintain European leadership in the field of Embedded Systems, Software-intensive Systems and Services. Both innovation programmes want to address Europe’s big societal challenges like affordable healthcare and wellbeing, green and safe transportation, reduced consumption of power and materials, reduction of food waste, smart buildings and communities of the future, and an imminent lack of natural resources. To underline this ambition the joint theme for the Co-summit 2011 is well chosen: ‘Cross-border cooperation for Green Technologies’.

The pSHIELD project was presented at the exhibition in its own booth with number of prepared posters, leaflets, presentations and mini demonstrator. The project was also presented to the audience at general session. Many partners of pSHIELD consortium were also present at the exhibition as a visitors or at other project stands, they are involved in.

Two floors of congress center were filled with different ARTEMIS and ITEA projects stands. The Co-summit event was a perfect opportunity for exchange of information between projects.

2.1.2 ARTEMIS & ITEA2 Co-summit 2010, Ghent

Co-summit 2010 was annual event organized together by ARTEMIS and ITEA2, on 25-27 October 2011 in International Convention Center ICC in Ghent, Belgium.

The Co-Summit is explicitly targeting the Public Authorities of not only all countries, but also the European Commission. The purpose is to show them the status of the projects. The implicit goal is to motivate the Public Authorities to provide and reserve sufficient budget for such projects in the Call for Projects of the next year. The location of the Co-Summit is determined in close cooperation with the Public Authorities. It is known from the feedback that the Public Authorities value this exhibition of projects very much. They need it in order to see the progress of the programme not only for their own country, but also in relation to the contributions from other countries. Therefore, it is very important for each running project to be visible at this exhibition.

The pSHIELD project was presented in its booth with posters, leaflets and demonstrator. The project booth has been chosen for public presentation for VIPs, which were successfully performed. The exhibition created great occasion for liaisons with other projects.

2.1.3 Other events

The project partner were involved in number of different kind of events, like exhibitions, conferences, and other meetings. They used every possible opportunity to spread information on the pSHIELD project, and to gather information on other projects for possible internal usage, that way building liaisons between different projects. The list of such events is available in deliverable D7.1.2 “Dissemination Report”.

2.2 On-line liaisons

2.2.1 On-line collaboration tools

The pSHIELD project uses three on-line collaboration tools: website, wiki and repository:

- pSHIELD Website, based on Joomla software is available at url: http://www.pshield.eu
- pSHIELD Wiki, running MediaWiki software, is at http://pshield.unik.no
- pSHIELD Repository, based on BSCW Server software, is available at http://bscw.juartemis-pshield.eu

Two of them have publicly available areas, those are website and wiki.

The pSHIELD project website is kind of business card for the project. It provides reader with general project information, partners description, list of public deliverables and contact data. It is described in details in deliverable D7.1.1.

The pSHIELD wiki is more a collaborative tool for partners, a place to brainstorm and discuss idea, collect information about current work, phone conferences and meetings. It is described in details in deliverable D1.1.1.

Both website and wiki have publicly accessible pages, but a lot information is available only for authorized users and requires authentication.

2.2.2 Projects' exchange of information

The pSHIELD website is listed with other projects in the ARTEMIS website http://www.artemis-ia.eu . All ARTEMIS projects participants may freely have access to general projects' description, what allows to build farther liaisons between them.

ARTEMIS partners from other projects may even get access to non-public areas of on-line collaboration services to review draft yet not published deliverables, and even participants restricted deliverables. This is the case with the pSHIELD successor, that is with nSHIELD partners. The nSHIELD project is expected to continue and enhance pSHIELD achievements, so both consortia are working with close cooperation.

2.3 Partners liaisons

The pSHIELD project consortium is composed of 16 partners from 6 European countries. Partners are big industrial companies and known university. Most of partners teams are involved in various European projects, that way exchanging information from different projects in their work. Selected partners liaisons are listed below.

2.3.1 Ansaldo STS Liaisons

Ansaldo STS is the coordinator of European 7th FP IP Project PROTECTRAIL and participates to the European 7th FP CP Project SECUR-ED. Furthermore, Ansaldo STS (thrugh its formerly controlled company Ansaldo Trasporti Sistemi Ferroviari) has been the coordinator of the TRIPS (Transport Infrastructures Protection System) project funded under the Preparatory Action on Security Research (PASR) 2005 initiative of the DG Enterprise (Grant Agreement no. 111800).

The aforementioned projects focus on the analysis, design, development, testing and deployment of novel computer-based systems for the surveillance and protection of critical assets, including rail and mass-transit transportation systems. Ansaldo STS is putting together the results achieved in all those synergic projects in order to improve the quality, safety and reliability of its solutions (systems engineering approaches, hardware and software products). To that aim, the results achieved in the pSHIELD project (and those that will be achieved in the ongoing Artemis funded nSHIELD project), in particular with the case-study applications in which ASTS is especially involved, will allow to increase resilience, trustworthiness and survivability as well as the scalability and cost-effectiveness of the data integration and management infrastructures, that are essential in any critical monitoring and control applications in the railway and mass-transit domains.

2.3.2 Critical Software Liaisons

As part of the pSHIELD project team Critical Software has needed to draw upon experience that it has gained through its involvement within other FP7 projects. Critical Software is also the consortium leader of the EMMON project (Project full title: EMbedded MONitoring, Grant agreement no.: 100036) and is part of the consortium team on the CESAR project (Project full title: Cost-efficient methods and processes for safety relevant embedded systems, Grant agreement no.: 100016) both of which are FP7 projects. This has enabled Critical Software to take the "best practices" learned within these and apply them to the pSHIELD project.

Critical Software encourages its engineers to develop their skills and to learn new ones. It was with this in mind that Critical set up the internal workshop "pSHIELD and security in embedded systems". This workshop was held on the 8th October 2010 and was designed to allow the information gained and to be developed by pSHIELD to a wider internal audience.

Within pSHIELD the identified technologies and solutions represent a reference guideline for the design and development of Embedded Systems (ES) where Security, Privacy & Dependability (SPD) capabilities are required. In practice this has meant that pSHIELD's results will be used for the cross fertilisation among projects and this has meant they are available for possible reuse to provide SPD features to the ES's that might be designed and developed in other projects. Within Critical Software we have encouraged the reuse of features and technologies between projects, specifically taking ideas from R&D projects such as this and implementing these within real world solutions.

2.3.3 Eurotech Liaisons

Eurotech has been involved in three main events strictly related to the project:

- the Embedded World 2010 exhibition, 1-3 March 2010 in Nuremberg (Germany),
- the ARTEMIS & ITEA Co-summit 2010 exhibition, 24-26 October 2010 in Ghent (Belgium),
- and the ARTEMIS & ITEA Co-summit 2011 exhibition, 25-26 October 2011 in Helsinki (Finland).

During these events Eurotech has been active in exchanging idea, discussing topics and results, present project objectives and results and identifying further evolutions in terms of research of high performance computing in SPD embedded systems.

Further activities have been performed following Eurotech HPC business unit participation to important events in the scientific area of high performance computing:

- Super Computing Conference (SC2010), New Orleans, LA, November 2010,
- Super Computing Conference (SC2011), Seattle, WA, November 2011,
- and International Super Computing Conference (ISC2011), Hamburg, Germany, June 19-23, 2011.

These contexts have been extremely important for the preparation of DEEP project (Dynamic Exascale Entry Platform). DEEP is an innovative European response to the Exascale challenge. The DEEP consortium, led by Forschungszentrum Jülich, proposes to develop a novel, Exascale-enabling supercomputing architecture with a matching SW stack and a set of optimized grand-challenge simulation applications. DEEP takes the concept of compute acceleration to a new level: instead of adding accelerator cards to Cluster nodes, an accelerator Cluster, called Booster, will complement a conventional HPC system and increase its compute performance. These concept are the same that inspired pShield Power Node and, starting from pShield project, will be further investigated and developed in DEEP and nShield.

2.3.4 Mondragon Goi Eskola Politeknikoa Liaisons

Mondragon University is also involved in the following projects:

- Artemis:
    - eDIANA
    - nSHIELD
    - pSAFECER
    - nSAFECER

 - CRAFTERS
- ITEA2:
  - EVOLVE

Even if they are not specifically related to security (apart from nSHIELD) all of them are in the embedded systems domain, which allows Mondragon University to have a broader view of the challenges to be faced by future embedded systems.

2.3.5 SESM – Finmeccanica Liaisons

SESM was involved in number of events, where exchange of topics and achievements between different European projects took part. During events like conferences and exhibitions both information about the pSHIELD project were presented and information from other projects were collected. To list the most important events to be listed are:

- ARTEMIS & ITEA Co-summit 2011 exhibition, 25-26 October 2011 in Helsinki, Finland.
- ARTEMIS & ITEA Co-summit 2010 exhibition, 24-26 October 2010 in Ghent, Belgium.
- EmbeddedWorld 2010 exhibition, 1-3 March 2010 in Nuremberg, Germany.

Selected information on that events were already provided in that document. It is important to highlight that SESM conducted that activities in collaboration with CWIN and MAS, and results of whole the pSHIELD consortium were demonstrated.

As a result of liaisons we consider usage of achievements of ARTEMIS eSONIA project, the winner of the ARTEMIS Co-summit 2011 exhibition for best performance. Interesting topic is usage of eSONIA developed IPv6 stack in lwIP (light weight IP) software, used in pSHIELD FPGA Power Node prototype, to enhance pSHIELD proposed SPD framework with SotA solutions.

2.3.6 SELEX Elsag Liaisons

As has been previously stated, it is the SDR platforms that will be used for the design of the Smart Transmission Layer in SHIELD project. Therefore, security issues and solutions for the Software Defined Radios are the topics of the particular interest for this project.

The following groups are performing work in the area of the security of the Software Defined Radios:
Security Work Group (SecWG), operating within the Wireless Innovation Forum group is momentarily working on the specification entitled "Security Requirements and Profiles Case Studies" (which builds upon their previous report titled „Securing Software Reconfigurable Communications Devices“), with the goal of „providing guidance to designers, developers and manufacturers of SDR devices on the appropriate set of security requirements germane to their class of SDR products. The report will provide a comprehensive set of security requirements that cover all aspects of SDR and software reconfigurable radio devices (SDRD) security for the underlying SDRD platform and its software operating environment“.
LINK:
„Securing Software Reconfigurable Communications Devices“ specification:
http://groups.winnforum.org/d/do/3014

The International Security Services API Task Group (ISS-API) of the Security Work Group, also operating within the Wireless Innovation Forum group, is working on approving the“International Security Services API“ – the specification developed for nations, international organizations and companies who need software interoperability and portability between international and independently developed software radios. The intent of this API is to promote waveform (WF) portability between various radio platforms that provide the API. As such, the focus of this API is on the security interfaces required to meet waveform needs.
LINK:
„International Tactical Radio Security Services API Specification“:
http://groups.winnforum.org/d/do/4986

ESSOR (European Secure SOftware defined Radio) sets its targets on „providing architecture of Software Defined Radio (SDR) for military purposes and a military High Data Waveform (HDR WF) compliant with such architecture, thus offering the normative referential required for development and production of software radios in Europe“, as well as „delivering guidelines which are related to the validation and verification of waveform portability and platform re-configurability, setting up a common security basis to increase interoperability between European Forces.“
LINK:
Essor – general information: http://www.occar-ea.org/36

There have also been several studies done and papers published in the domain of the SDR threats and security, some of the more notable ones being:

- H. Uchikawa, K. Umebayashi, and R. Kohno, "Secure download system based onsoftware defined radio composed of fpgas," in PIMRC, 2002, pp. 437–441.
- A. Brawerman, D. Blough, and B. Bing, "Securing the download of radio configuration files for software defined radio devices," in MobiWac, 2004, pp. 98–105.
- A. Brawerman and J. Copeland, "An anti-cloning framework for software defined radio mobile devices," in ICC, 2005, pp. 3434–3438.
- C.Li, A.Raghunathan, and N. Jha, "An architecture for secure software defined radio," in Proc. Date '09, 2009, pp. 448–453.

There are also groups focusing their research on the security within embedded systems more generally and not necessarily concentrating on the SDR security issues, namely:

Distributed and Embedded Security group (DIES) at University of Twente states their mission as "providing fundamental improvements for the security of distributed and embedded systems, by designing suitable building blocks and fostering systematic reasoning".
Their work, therefore, focuses on the topics of data security, network security and cybercrime prevention, whereas their results are mostly applicable to the following areas:

- health and food management
- critical control systems
- social and enterprise networks

LINK:
Research page of the DIES group: http://dies.ewi.utwente.nl/?page=research

Mälardalens University (MDH) has several ongoing projects concerning security issues in embedded systems.
The main goal of their "TESLA"("Time-critical and Safe wireLess Automation communication") and "GAUSS" ("Guaranteed Automation communication Under Severe disturbanceS") projects is achieving predictability of time-critical and safe wireless communication, in spite of communication taking place in harsh environments. The main application areas are time-critical industrial processes.
LINKS:
TESLA project – more information: http://www.mrtc.mdh.se/index.php?choice=projects&id=0289
GAUSS project – more information:
http://www.mrtc.mdh.se/index.php?choice=projects&id=0330

Cylab at the Carnegie Mellon University also has multiple ongoing projects dealing with the security topics, namely:

- "Adaptive Strategies For Cross-Layer Jamming And Anti-Jamming", whose goal is to study the potential impact of malicious and strategic jamming and the ability for the target network to operate in a degraded state while under attack, with the primary focus on the means for potential adaptation by both the adversary and target network and the resulting impacts on performance and operation.

- "Attacking And Defending Unreliable Hardware"project's scope is on devising attacks exploiting security vulnerabilities within processor and memory hardware (e.g. design bugs, wearing out, transient bit flips), as well as developing hardware-based solutions to prevent such attacks.

LINK:
Cylab – list of ongoing projects: http://www.cylab.cmu.edu/research/projects/index.html

CORASMA (COgnitive RAdio for dynamic Spectrum Management) sets its targets on: Software Radio, NII Communication management, Agile RF Front-end, Channel Aware PHY Layer, Adaptive MAC, Cooperative Routing, Spectrum Monitoring, Localization, Spectrum Usage Policies, Cognitive Manager.
Main objectives are: To make a review and synthesis of the Cognitive Radio Technologies explored within NATO countries in the military field. To make a review of Civilian Technologies available for Military Cognitive Radio now and at mid long term. Investigate the techniques and technologies which could implemented at mid long term in a cognitive radio and provide a technology roadmap planning. To analyze the benefit of cognitive radios integration in NNEC NII architecture. Propose to the NATO community relevant axis of works on Cognitive Radios.
Countries involved: BEL, CAN, DEU, ESP, FRA, GRC, ITA, NOR, NDR, USA

2.3.7 Tecnalia Liaisons

Tecnalia is participating in several projects in ARTEMIS and in FP7 related to security and embedded systems. Particularly, there tow main projects related to nSHIELD: the first one is called IoE (internet of Energy) where Tecnalia is actively working in SC 12 about making both security and privacy visible within the energy application domain. The second project is called CHIRON: Tecnalia is treating to introduce the novel nSHIELD architecture reference into CHIRON framework.

Moreover, nSHIELD has to do with introducing security systematization within the software and system engineering process. ANIKETOS is an Fp7-IP project that aims at helping software and service developers doing a similar thing: constructing built-in security techniques and components for service composition.

2.3.8 Università di Genova Liaisons

University of Genova has currently several research activities that are related to pSHIELD concepts. The ISIP40 research group is responsible for large scale simulation scenarios in the European Secure SOftware defined Radio (ESSOR) project. pSHIELD results will be exploited within this project that sets its targets on providing architecture of Software Defined Radio (SDR) for military purposes and a military High Data Waveform (HDR WF) compliant with such architecture, to deliver guidelines which are related to the validation and verification of waveform portability and platform re-configurability.
The ISIP40 group of the University of Genova is currently coordinating the Erasmus Mundus Joint Doctorate on Interactive and Cognitive Environments (EMJD-ICE http://www.icephd.org) an EU project for financing PhD scholarships. One of the research areas agreed with other partners in the consortium is focused on Networked Embedded System. In this area, pSHIELD results will be exploited dealing with various technological issues concerning embedded systems and networks of the future, which represent a very important basis for the development of many intelligent and pervasive applications. From a scientific-technical point of view, the course provides insights on topics such as simulations of networks, design of processors and embedded systems, communication networks and smart sensors. Seasonal schools and workshops will be organized (the first summer school was organized in September 2011 in Klagenfurt (AT), while the second will be organized in Italy in September 2012) with specific tracks focused on SPD related concepts in Networked Embedded Systems.

As a result of liaisons we consider also several research projects with SELEX Elsag company that are focused on the industrialization of pSHIELD results related with Security Privacy and Dependability in wireless and wired networked systems.

2.3.9 Università di Roma Liaisons

University of Rome "La Sapienza" is involved in several FP7 project and in particular two of them are focused on "security" aspects.

The first one is TASS (Total Airport Security System) an ongoing project with the aim of defining a framework for data collection and analysis to prevent malicious attacks in the airport facilities. Even if the technological foundation is different, both these projects (TASS and pSHIELD) foresee the use of ontology to manage the knowledge associated to the specific environment. The methodology for the definition of a semantic model to describe the airport environment has been considered as input to define the semantic model describing the embedded systems, since both of them share the purpose of the ontology: modeling a system for security purposes.

The output are reasonability quite different, but the adoption of similar concepts and tools (OWL, protégé, …) will be useful, in an exploitation perspective, to push the use of semantics in security context and, maybe, converge to common solutions in future.

The second project, funded in the last FP7 call but not yet started, is CockpitCI and is about the design of a framework to protect critical infrastructure (in particular SCADA systems) from cyber attacks. Liaisons will be established with this project to check if the SHIELD platform can be a suitable candidate (or at least a good guideline) to develop a similar framework suitable for SCADA protection.

Last, but not least, the main liaison will be with the nSHIELD project, the prosecution of pSHIELD. The valuable outcome of the pilot phase, mixed with the enriched expertise brought by the new partner, will help the refinement of solutions and the translation of them into stronger prototypes.

2.3.10 THYIA Liaisons

THYIA is involved in several FP7 projects and in particular one of them is focused on "security" aspects. Another projects is JU Artemis project focused on smart metering and smart grids infrastructures and devices.

The IMSK (Integrated Mobilie Security Kit, http://www.imsk.eu/) is an ongoing IP project with the aim of defining security technology for six different scenarios. This project will employ legacy and novel sensor technologies, design a system (IMSK) that will integrate sensor information to provide a common operational picture where information is fused into intelligence, perform a field demonstration to validate the concept, adapt the system to local security forces and finally disseminate the results after accreditation by end-users. The development of IMSK will be heavily founded on advice derived from operational security professionals.

The second project ME3GAS (Smart Gas Meters & Middleware for Energy Efficient Embedded Services, http://www.me3gas.eu/) is a co-funded project of Slovenia and JU Artemis. ME^{3}GAS addresses the development of a new generation of smart gas and electricity meters, based on embedded electronics, communications and the remote management. The requirements, specifications, implementation, and dissemination of an open architecture for wireless communication between smart devices and gateway device will also be addressed in the project. The utilization of intelligent concepts is what makes energy smart, and is the heart of energy-efficient technologies. Through energy-intelligent control, regulation and communication we can expect to see further improvements in energy yield. ME3GAS will make use of the service-oriented middleware for embedded systems being developed in the Hydra project and use its huge potential to create services and applications across heterogeneous devices to develop an energy-aware and security middleware platform. THYIA responsibilities are related to security technologies and semantic ontology and services.

3 Conclusions

Deliverable D1.2.1 “Liaisons report” is part of the pSHIELD project Work Package 1, Task 1.2. But it represents efforts of all the consortium to provide the highest quality output from the project by usage of information about achievements of other European projects.

References

[1] Technical Annex for ARTEMIS JU pSHIELD project number SP6 100204