Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D1.3: Liaisons Plan

Due date of deliverable: M3 –2011.11.30

Actual submission date: M10 – 2012.06.20

Start date of project: 01/09/2011 Duration: 36 months

Organisation name of lead contractor for this deliverable:

Selex Galileo, SG

Revision [Draft A]

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

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Lorena de Celis	Acorde Technologies		
Esposito Mariana	Ansaldo STS		
Roberto Uribeetxeberria	Mondragon		
Marco Cesena	Selex Elsag		
Nikolaos Pappas	HAI		
Balazs Berkes	S-LAB		
Luigi Trono	Selex Galileo		
Francesco Cennamo	Selex Galileo		
Spase Drakul	THYIA		
Josef Noll	Movation		
Reviewed by			
Name	**Company**		
Approved by			
Name	**Company**		

Applicable Documents

ID	Document	Description
[01]	TA	nSHIELD Technical Annex

Modification History

Issue	Date	Description
Draft A	20.06.2012	

Contents

Figures

Tables

Glossary

Please refer to the Glossary document, which is common for all the deliverables in nSHIELD.

This Page is intentionally left blank

1 Introduction

The purpose of this deliverable is to establish a liaisons plan starting from on-going Horizon2020 / Artemis projects relevant to Security, Privacy Dependability for Embedded Systems concepts.

In the following paragraphs are shown activities which see the nSHIELD partners involved. The relations between such projects and nSHIELD permit a useful exchange of knowledge among consortia and an improved, coordinated and synergetic continuation of the standardization processes. Also, the results obtained from nSHIELD will be useful to future ARTEMIS proposals presented on next calls.

The nSHIELD 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 Partners liaisons

2.1.1 SG Liaisons

SG is actively participating at ARTEMIS & ITEA2 Co-summit which is the annual event for project exhibition, showcasing active projects of ARTEMIS and ITEA. The event is hosted by the ARTEMIS Joint Undertaking and ITEA 2. Both organizations are active to help Europe to achieve and maintain European leadership in the field of Embedded Systems, Software-intensive Systems and Services. Both innovation programs 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.

SG participated for the first time at 2011 event with prepared posters, leaflets, presentations. The Co-summit event was a perfect opportunity for exchange of information between projects.

For the next summits the nSHIELD booth will host one of four demonstrator ready at time. Many partners of nSHIELD consortium will be present at the exhibition as a visitor or at other project stands, they are involved in. The 2012 Summit will be in Paris on 30 - 31 October.

On 20 - 21 September 2012, Selex Galileo will present "nSHIELD Architectural Frameworks for Security, Privacy and Dependability" at the ARTEMIS-Austria Conference.

SG as FINMECCANICA Company has been actively looking for internal projects having a strong relation with the nSHIELD topics. Result of this activity is to have cutting-edge products and competitive in ES markets. Selex Galileo has identified a linked project named as OMNIA which is an open embedded system for avionic architecture.

2.1.2 Ansaldo STS Liaisons

Ansaldo STS is involved in several ARTEMIS and FP7 projects. Currently, Ansaldo STS is the coordinator of European 7th FP IP Project PROTECTRAIL and a partner of the European 7th FP CP Project SECUR-ED. In 2005, Ansaldo STS has been the coordinator of the TRIPS (Transport Infrastructures Protection System) project funded under the Preparatory Action on Security Research (PASR). Those 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.

The participation in the pSHIELD project and the realization of case-study (protection of freight train transporting hazardous materials) has provided some useful results in the protection of critical assets. In particular, an important step has been moved towards the resilience, trustworthiness and survivability as well as the scalability and cost-effectiveness of the data integration and management infrastructures. Those topics are essential in any critical monitoring and control applications in the railway and mass-transit domains. With the nSHIELD application, Ansaldo STS aims at enhancing and generalizing the results achieved in the aforementioned projects in order to improve the quality and cost-effectiveness of its solutions. In fact, using nSHIELD results, the physical security solutions already provided by Ansaldo STS can be enhanced with resilient outdoor infrastructure surveillance of critical sites and assets (e.g. railway bridges, freight cars) even using 'open' communication networks (e.g. wireless links, Internet). Therefore, the project applies particularly to Ansaldo STS security product portfolio, and more specifically to the PSIM (Physical Security Information Management) system developed by our company. In the future, nSHIELD results could be applied to vital infrastructures like those used for railway signalling and control.

2.1.3 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 on software 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, and 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 implement 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

2.1.4 HAI Liaisons

HAI, as the basic Greek defense industry and a publicly-owned company, often consults public bodies for security-related public policies. The company participates in regularly organized international events, where research projects along with their expectations and results are presented. Indicatively:

- The International Fair of Thessalonica, an exhibition with history of eight decades, www.tif.gr
- ExpoSec, a Homeland and Corporate Security Conference and Exhibition, http://www.tsomokos.gr/projects2.php

HAI, being the largest defense company in Greece, participates in numerous research projects. Knowledge acquired there can be utilized in various forms in favor of the project, such as that of SPD requirements or developing SPD technologies, which can be taken into account to inform nSHIELD. In reverse, HAI can publicize nSHIELD technologies and framework to other projects, for dissemination purposes or in view of complementary and compatible developments. Some of the aforementioned related projects and their implications to nSHIELD activities are listed below:

Table 1 HAI Liaisons (FP7 funded projects)

FP7 funded projects	Description
VITRO	Processes the concept of virtual sensor networking to support virtually infinite number of applications. Trusted node connectivity and routing is a main issue in VITRO, as in nSHIELD
ASPIS	Elaborates an incident reporting system with demonstrations in metro networks and ships. The monitoring devices are implemented on a HW and SW embedded system platform
TALOS	Performs border surveillance engaging robotic vehicles

2.1.5 ACORDE Technologies Liaisons

ACORDE has always maintained a strong interest in research and development in innovation related activities, which has allowed to continually improving the catalogue of products. These activities have helped to achieve a high level of technological expertise in the field of telecommunications engineering. Our R&D works mainly on the area of Radio-communications, ranging over several fields from Satellite Communications, to WLAN and WPAN systems and Smart Wireless Sensor networks. We have a wide experience collaborating in R&D projects in the National Research Plan, as well as in European Projects within the different European Union Framework Programmes.

Some of the current European Projects in which ACORDE is collaborating and which are related with the topics of nSHIELD project, (*wireless communication platforms development* and *communication encryption*) are summarized in the following table:

Table 2 Acorde Liaisons (FP7 funded projects)

FP7 funded projects	Description
WHERE2	The WHERE2 project addresses the combination of positioning and communications in order to exploit synergies and to enhance the efficiency of future wireless communications systems. The key objective of WHERE2 is to assess the fundamental synergies between the two worlds of heterogeneous cooperative positioning and communications in the real world under realistic constraints. http://www.kn-s.dlr.de/where2/
BURBA	BURBA project proposes an innovative method to optimize waste management through the application of RFID and Location Based Services technologies integrated into an intelligent waste container (IWAC) for its use in densely populated areas. All the electronics components for waste containers (including high-sensitivity localization devices, RFID reader, sensors and wireless interfaces) will be integrated in hardware package and test in a real scenario. http://www.burbaproject.net/
TIGER	Utilization of GNSS to provide location based authentication and geo encryption services that make use of several anti-jamming and anti-spoofing algorithms to achieve a trusted solution. It is based on a custom designed USB device that supports the Smart Card profile and implements these services in order to add an extra security layer on the system. http://www.tiger-project.eu/
STON	Use of GNSS signals for location based authentication and encryption based on advanced algorithms http://www.ston-project.eu/

2.1.6 S-LAB Liaisons

SEARCH-LAB Ltd. takes part in the following FP7 funded projects, where potential project synergies could be exploited to the benefit of both projects.

Aniketos Secure and Trustworthy Composite Services is an on-going collaborative project (IP) funded under FP7/ICT (Call 5), aligned to the strategic objective 1.4 Secure, dependable and trusted infrastructures that started in 2010. The project helps establishing and maintaining trustworthiness and secure behaviour in a constantly changing service environment. The project aligns existing and develops new technologies, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users. It provides methods for analysing, solving, and sharing information on how new threats and vulnerabilities can be mitigated. A platform is constructed for creating and maintaining secure and trusted composite services.

Website: http://www.aniketos.eu/

SecFutur Design of secure and energy-efficient embedded systems for Future Internet applications is another on-going project (STREP) funded under FP7/ICT (Call 5), aligned to the strategic objective 1.4 Secure, dependable and trusted infrastructures that started in 2010. SecFutur develops a new security engineering process that can flexibly integrate security solutions into an overall framework for the hardware platform based design process and that can be incorporated into the existing design process with a minimum amount of changes. Security solutions are provided in terms of security building blocks that integrate existing hardware and software security mechanisms in order to address complex security requirements.

Website: http://www.secfutur.eu/

uTRUSTit Usable Trust in the Internet of Things is an on-going project (STREP) funded under FP7/ICT (Call 5), aligned to the strategic objective 1.4 Secure, dependable and trusted infrastructures, started in 2010. The main focus of the project lies in its objective to integrate the user directly in the trust chain of the recently unfolding Internet of Things technology, guaranteeing transparency in its underlying security and reliability properties. The results will enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgments on the trustworthiness of such systems. Further, the project's design guidelines on trust help the industry to implement the Trust Feedback Toolkit developed by uTRUSTit in a secure, usable and accessible way.

Website: http://www.utrustit.eu/

2.1.7 THYIA Liaisons

THYIA is an SME that participates in some key FP7 projects. The experiences achieved in pSHIELD and those acquired until now in nSHIELD project represent foundation for dissemination in many future FP7 and FP8 security projects as well as for Embedded Systems and Devices that play an important role for EU industrial policy and programme for 2020.

The main focus is to develop possible policy measures to promote the industrial take-up of KETs (Key Enabling Technologies) by EU industries. There are five KETs: nanotechnology, micro and nanoelectronics, industrial biotechnology, photonics, advanced materials, and advanced manufacturing systems. We can see that SPD ES and ED promoted in pSHILED and nSHIELD are part of KETs at least as sensor technologies with networking capabilities. These new SPD technologies represent foundation for new industrial take-ups and enhanced competitiveness in EU. Therefore, the liaison with other EU and JU Artemis projects is extremely important to be carry out by THYIA in the forthcoming years. THYIA is actively contributing at EU level in some key FP7 projects mentioned in TA.

Additionally, some important liaisons are targeted in some standardization bodies: ETSI, CENELEC and 3GPP, i.e., M2M, PLT, and 4G LTE.

2.1.8 MOVATION Liaisons

Movation is one of the founding members of the Internet of Things Value Creation Network http://www.internet-of-things.no/ together with Sintef, Telenor, Standard Norway and other industrial players. We envisage using this platform for first of all for industrialisation. Together with Standards Norway, who is co-founder and steering board member of the IoT Value Creation Network we discuss strategies and impacts for standardisation towards ETSI, CEN and CENELEC. However, due to the lack on national support there is little activity towards standards from the Norwegian cluster.

We also use the Norwegian Internet of Things network as collaboration with the Artemis project Internet of Energy, led by Sintef.

The new nSHIELD partner Alfatroll leads the Norwegian UAV network http://www.uasnorway.org/ and is steering member of the European UAV network. Thus we expect to contribute to both networks with the envisaged nSHIELD solution.

2.2 Exchange and collaboration with Artemis funded project

Table 3 Artemis funded projects

Artemis funded projects	Description
CESAR	Deals with the development of tool-chains for safety critical embedded systems. Experience from formalization of requirements engineering can be exploited by nSHIELD
SIMPLE	Concerns the development of sensor networks and back-end middleware for manufacturing and logistics. The goal of delivery of a self-organizing middleware platform resembles technical aims of nSHIELD
SMART	Treats the development of high-performance low-power wireless sensors with reconfigurable compression and encryption algorithms. The novel authentication systems that will be developed will assist nSHIELD address its own SPD WSN requirements
SMECY	Involves a framework for developing in multi-core platforms
R3-COP	Designs a framework for autonomous robotics
CRAFTERS (ConstRaint and Application driven Framework for Tailoring Embedded Real-time Systems)	CRAFTERS will develop a computing environment for embedded many-core systems. It will provide a model-driven process for the compositional development on many-core systems, including the modeling of safety and **security** related aspects. The security aspects are specifically addressed by WP6 (Trust Assurance and Security Certification Suite) of CRAFTERS, which focuses on tools and methods for covering security throughout the design process (from early design to validation and verification). In addition, interfaces which allow secure interconnection of devices will be developed.
pSafeCer+nSafeCer: SafeCer (Certification of Software-Intensive Systems with Reusable Components)	Deals with the development of process and technology that enable composable qualification and certification. Qualification/certification of systems/subsystems based on reuse of already established arguments for and properties of their parts.
eDIANA Embedded Systems for Energy Efficient Buildings	Its goal is to achieve energy efficiency in buildings through innovative solutions based on embedded systems. Model driven methodology and V&V techniques and tools have been defined for the embedded systems developed in the project. These methodologies and techniques can be reused in nSHIELD.

2.3 Other Liaisons activities

The project partners are involved in number of different kind of events, like exhibitions, conferences, and other meetings. They used every possible opportunity to spread information on the nSHIELD project, and to gather information on other projects for possible internal usage, that way building liaisons between different projects.

3 Conclusions

The Deliverable D1.3 “Liaisons plan” is part of the nSHIELD project Work Package 1, Task 1.2 and it represents efforts of the entire consortium to provide the highest quality output from the project by usage of information about achievements of other European projects.