PROJECT PERIODIC REPORT

JU Grant Agreement number: 269317

Project acronym: nSHIELD

Project title: new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Date of latest version of Annex I against which the assessment will be made:

Periodic report: 1st ☐ 2nd ■ 3rd ☐ 4th ☐

Period covered: from 01.09.2012 to 31.08.2013

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Dr. Josef Noll (MOVATION)

Tel: +47 9083 8066

Fax:

E-mail: josef.noll@movation.no

Project website[2] address: http://newshield.eu

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the grant agreement

[2] The home page of the website should contain the generic European Emblem and the Joint Undertaking's logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm ; logo of the Joint Undertaking: ARTEMIS :). The area of activity of the project should also be mentioned.

Declaration by the scientific representative of the project coordinator[1]

I, as scientific representative of the coordinator[1] of this project and in line with the obligations as stated in Article II.2.3 of the JU Grant Agreement declare that:

- The attached periodic report represents an accurate description of the work carried out in this project for this reporting period;
- The project (tick as appropriate):

  ☐ has fully achieved its objectives and technical goals for the period;

  ■ has achieved most of its objectives and technical goals for the period with relatively minor deviations[3];

  ☐ has failed to achieve critical objectives and/or is not at all on schedule[4].
- The public website is up to date, if applicable.
- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status. Any changes have been reported under section 5 (Project Management) in accordance with Article III.2.f and IV.1.f of the JU Grant Agreement.

Name of scientific representative of the Coordinator[1]: .....

Date: ...../ ...../ .....

Signature of scientific representative of the Coordinator[1]: .....

[3] If either of these boxes is ticked, the report should reflect these and any remedial actions taken.

[4] If either of these boxes is ticked, the report should reflect these and any remedial actions taken.

Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D1.8: Annual Management Report 2

Due date of deliverable: M24 –2013.08.31

Actual submission date: M25 -2013.09.30

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

Organization name of lead contractor for this deliverable:

Selex ES, SES

Revision [-]

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**		
Cecilia Coveri	Selex ES		
Josef Noll	Movation		
Marco Cesena	Selex ES		
Andrea Morgagni	Selex ES		
Nikolaos Pappas	HAI		
George Dramitinos	ISD		
Antonio Bruscino	SESM		
Kresimir Dabcevic	UNIGE		
Luca Geretti	UNIUD		
Lorena de Celis	AT		
Ester Artieda Puyal	ISL		
Roberto Uribeetxeberria	MGEP		
Iñaki Eguia Elejabarrieta	TECNALIA		
Christian German	SICS		
Hans Thorsen	T2DATA		
Eszter Viszlai	S-LAB		
Eva Vázquez de Prada Fernández	ISL		
Harry Manifavas	TUC		
Carlo Pompili	TELC		
Andrea Fiaschetti	UNIROMA1		
Antonio Abramo	UNIUD		
Mariana Esposito	ASTS		
Paolo Azzoni	ETH		
John Giaelis	ATHENA		
Spase Drakul	THYIA		
Tor Olav Steine	ALFA		
Reviewed by			
Name	**Company**		
Elisabetta	Campaiola		
Approved by			
Name	**Company**		
Josef Noll			

Modification History		
Issue	**Date**	**Description**
Draft A	2013-07-11	First issue for comments.
Final	2013-09-30	

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 Publishable summary

1.1 Overview

This document is the Periodic Annual Management Report of the activities carried out by the nSHIELD consortium within the nSHIELD project N. 269317 during the period from September 1st 2012 to August 31st 2013.

The document is structured as follows:

Chapter 2 - *Project Objectives for the period* is a summary of the progress made during the above mentioned period of activities, including a comparison between the activities planned in the Work program and the actual accomplishment of the period.

Chapter 3 - *Work progress achievements during the period* is the detailed description of the consolidated results for each Work Package, including progress towards objectives, supported by indicators and details for each task and each partner. This section is ordered according to the Work Packages as defined in the Technical Annex.

Chapter 4 - *Project Beneficiary grouped by country* is the detailed description of the activities carried out during the period to reach specific objectives within the task/WP by each partner. Effort planned and effort actual spent in this period are also indicated for each task.

Chapter 5 - *Deliverables and milestones tables* includes the list of deliverables due in the period with the delivery date and comments or justification. The achievement of the milestones of the period is showed.

Chapter 6 – *Project Management* is the description of the management activities of the period, including encountered problems, impact on the project schedule and mitigation action.

Chapter 7 - *Explanation of the use of the resources* Person-Month status and cost tables are reported for each partner.

1.2 Major findings

In the second year of the project many important activities have been executed in the framework of metrics, prototypes and demonstrators. A “demonstrator” (or scenario) is defined as composed by a group of prototypes.

In nSHIELD we had two approaches for address SPD functionality through metrics: (a) the multi-metrics approach and (b) the single metrics approach. Both approaches have their advantages and disadvantages, and we were not in the stage of deciding on one solution for nSHIELD. Thus both approaches have been developed in parallel, and explained during the meeting of Stockholm in order to evaluate the applicability of the approaches to our nSHIELD scenarios and the explanation through guidelines on how to use the approaches. All the nSHIELD partners have been actively involved on the metrics approach evaluation because this subject is strictly connected to the final system requirements definition and, consequently, to the demonstrators integration and validation plan definition. The results of this activity is included in D2.8 - SPD Metrics specifications. This document is not part of the deliverables of the second year, but has been prepared in parallel to the second year activities, because it could be considered essential for the project.

Additional important activities have been executed on WP5 “SPD Middleware & Overlay”. In particular additional studies have been carried out to find the adequate models and methodologies that represent the official SHIELD Formal Model. The tangible results provided by WP3, WP4 and WP5 is a set of prototypal SPD modules ready to be integrated (D3.2, D4.2, D5.2) provided with the required documentation (D3.3, D4.3, D5.3). The possible strategic impact in the process of realization of nSHIELD as a standard of new element “Middleware Protection Profile” has been evaluated in order to be defined and developed in D5.2 and D5.3.

The complete list of prototypes developed in the framework of the nSHIELD project has been identified.
The list includes 38 highly heterogeneous prototypes from 19 different partners. Some of them are software components, some are hardware components and some others are algorithms or models. The prototypes have been split depending on the layer, from node to overlay layer. For this reason, a common methodology for validation and verification activities is not provided, giving the choice of the most suitable mean of verification to the experts of the different layers. Some prototypes have be selected for integration in the common platform or in the final demonstrators.
The process of integrating the large number of different prototypes in a unified framework is a challenging task due to their heterogeneity and the complexity which is increased as the number of technologies increases. As overall approach, the first step of the system integration is to analyse the application requirements and crosscheck them with the repository of system requirements to find the degree of fulfilment of both application and SPD requirements.
Numerous prototypes of node, network and middleware layers are in an advanced or less mature stage of development, whereas the 4 application domains and correspondent scenarios are being built. All these activities come to synchronize efforts in the integration roadmap, finalized to construct a framework able to compose systems using different SPD components while addressing functional and SPD application requirements.

The plan and the methodologies driving the integration, the validation and verification activities for Railway Security scenario, Voice/Facial Recognition demonstrator and Dependable Avionic scenario have been described. Each scenario has been proposed in order to address the real-world issues related to the SPD requirements for each reference application. For sake off full, the technologies needed to be integrated to satisfy requirements set for Railway security, Voice/Facial Recognition and Reliable Avionic have been identified.

2 Project objectives for the period (1/9/2012-31/8/2013)

Within the second reporting period of the nSHIELD project (01.09.2012-31.08.2013) some intermediate objectives for the project were planned as described within the Technical Annex. Here below we are listing objectives and achievements for the related period.

WP2 Objectives and Achievements summary

"SPD Metric, requirements and system design" is the topic of this work package.
2nd year deliverables: D2.6
The deliverable is available at:

- D2.6 Final system Requirements and specifications http://nshield.unik.no/wiki/D2.6

All the following outcomes, of the 2nd year, have been achieved:

- Final SPD specification has been developed taking into account prototypes identified in WP6 and use case definitions of WP7.
- Metrics have been determined in a quantitative and formal way. During year 2, two ways for having an holistic measurement have been followed, Single metric approach (attack surface metric) and Multi metric approach (function analysis, fuzzy logic and genetic algorithms). There results will be described in D2.8 (M26)
- Definition of a heterogeneous and distributed architecture which aims to link the dissimilar components of nSHIELD System.

Note for WP2
The new leader of WP2 is TECNALIA.

At M23, no delays and not negative impact on future planned project activities

WP3 Objectives and Achievements summary

"SPD Node" is the topic of this work package.
2nd year deliverables: D3.2, D3.3
The deliverables are available at

- D3.2 Preliminary SPD node technologies prototype http://nshield.unik.no/wiki/3.2
- D3.3 Preliminary SPD node technologies prototype Report http://nshield.unik.no/wiki/D3.3

WP3 aims to create an Intelligent ES HW/SW Platform that consists of three different kinds of Intelligent ES Nodes: nano node, micro/personal node and power node. These three categories of embedded systems will represent the basic components of the lower part of an SPD Pervasive System that will cover the possible requirements of several market areas: from field data acquisition, to transportation, to personal space, to home environment, to public infrastructures, etc.

The activity of this year has been focused on the detailed description of the node technologies that are currently under development in work package 3, conforming to the preliminary architecture and the composability requirements specified during the first year.

Clearly significant and tangible results are:

- design and prototype implementation (see WP3 description for details)

- some prototypes available for demonstration have already been completed

At M23, no delays and not negative impact on future planned project activities

WP4 Objectives and Achievements summary

"SPD Network" is the topic of this work package.
2nd year deliverables: D4.2, D4.3
The deliverables are available at

- D4.2 Preliminary SPD network technologies prototype http://nshield.unik.no/wiki/D4.2
- D4.3 Preliminary SPD network technologies prototype Report http://nshield.unik.no/wiki/D4.3

This WP follows an approach similar to the WP3; in particular, in the layered architecture, building on top of the node functionalities defined in the WP3, Work Package 4 deals with implementation of the SPD functionalities at the network layer.

The activities of the second year of the project have been mainly focused on prototype design and implementation activities, as well as integration with WP7 (common demonstrators). They have been focused on the detailed description of the network technologies that are currently under development in work package 4, conforming to the preliminary architecture and the composability requirements specified in deliverables D2.4 and D2.5.
Clearly significant and tangible results are:

- Definition of technical perspective on the developed Network prototypes, focusing on the development platforms and technologies
- Overview of the prototypes operational characteristics
- Definition of interfaces to the upper layers (Middleware and Overlay)
- Creation of the "SPD level – node class" matrix in order to demonstrate applicability of each of the algorithms under development to different nSHIELD node classes and different levels of SPD controlled by the Overlay
- Usage of the pseudo-codes for presenting the algorithm functionality in a clear, readable way
- Decision on types of commercially available embedded nodes that may be commonly used for porting and testing of the developed algorithms

Note for WP4
Each of the partners involved in the WP4 – coming from different backgrounds - brings to the table their own expertise and work style, often resulting in usage of different technologies for algorithm development.

At M23, no delays and not negative impact on future planned project activities

WP5 Objectives and Achievements:

SPD Middleware & Overlay" is the topic of this work package. This WP defines a common semantic to describe the SPD interfaces and functionalities; Improve SPD middleware technologies;
2nd year deliverables: 5.2, D5.3
The deliverables are available at

- D5.2 Preliminary SPD middleware and overlay technologies prototype http://nshield.unik.no/wiki/D5.2
- D5.3 Preliminary SPD middleware & Overlay technologies prototype Report
- http://nshield.unik.no/wiki/D5.3

WP5 objectives for the 2nd year are the listed below:

- Definition of the semantic data structures necessary to make the SHIELD framework work
- Definition of the basic middleware services that represent the core of the SHIELD platform
- Design and development of a SPD-middleware policy-based management for ensuring a high level of security, privacy and dependability in systems composed by Intelligent ES Nodes
- Development of a control algorithms able to drive the composability of Embedded System for Security purposes.

The major achievements are:

- Identification and refining of the methodology to build the "knowledge base" used by the SHIELD Middleware to compose SPD functionalities, based on the decoupling between "domain information" and "security information"
- Production and formalization of peliminary models of the SHIELD components (in a language close to the demonstrator needs)
- Confirmation of the OSGI platform
- Intrusion detection systems (a set of different scanners that monitor the activities of an information system looking for malicious actions), has been identified as the first safety barrier for possible attacks against the system, warning of possible attacks to maintain reliability and availability of the network
- a secure overlay solution transparent to end "application*, regarding the multi-layered Overlay Security, has been designed and built. This solution does not require any modification to the current end device applications.
- A Protection Profile for the Middleware layer has been edited in order to address security, privacy and dependability (SPD) in the context of ESs as "built in" functionalities, with the long term objective of promoting the SPD certification for future ESs. Details on SPD core service are in WP5 activities description
- common understanding about the solution and the mechanisms chosen (e.g. operating system, infrastructure, interfaces) to ensure the required interoperability among stakeholders
- The architecture of the Security Agent has been preliminarily translated into code at Middleware level and the harmonization of the decision making process (metrics vs policies vs control algorithms) has been preserved in this first implementation.

Note for WP5

The D5.2 and D5.3 were delayed from M18 to M22. The reason for not being right on schedule (mainly in terms of contribution in WP5 deliverables) is the delay in the finalization of some necessary inputs (also from other tasks), which has introduced a delay in the formalization of some key concepts in WP5. This is mainly due to metrics and demonstrators definition. However the delay will be recovered in the last year of the project, since good basis in the above mentioned critical fields have been put.

At M23, no significant delays and not negative impact on future planned project activities

WP6 Objectives and Achievements summary

"Platform integration, validation & demonstration" is the topic of this work package.
2nd year deliverables: D6.1, D6.2, D6.3
The deliverables are available at

- D6.1 Lifecycle and SPD Support Plan http://nshield.unik.no/wiki/D6.1
- D6.2 Prototype validation and verification http://nshield.unik.no/wiki/D6.2
- D6.3 Prototype integration report http://nshield.unik.no/wiki/D6.3

Summarising, the WP has 3 major objectives distributed correspondingly in 3 tasks. The reporting period under examination concerns the following:

- Aims at integrating components and prototypes developed in WP3, WP4 and WP5
- Plans and conducts the validation and verification of the implemented solution
- Aims at guaranteeing the proposed architecture to be future-proof, to support the installation, download and upgrade cycle and to address the security and integrity issues involved

The achievements of the 2nd year WP6 are summarized below:

- SPD lifecycle principles in nSHIELD
- Planning methodology and phases of system's lifecycle
- Validation and verification methodology
- Validation and verification of prototypes
- Integration methodology
- Components per application
- Initial integrated systems per application

Note for WP6
Tasks and duties allocated to partner THYIA have been re-distributed among other partners.

At M23, no delays and not negative impact on future planned project activities

WP7 Objectives and Achievements summary

""SPD Applications" is the topic of this work package.
2nd year deliverables: D7.1, D7.2, D7.3, D7.4
The deliverables are available at

- D7.1 Railways security demonstrator - integration and validation plan http://nshield.unik.no/wiki/D7.1
- D7.2 Voice/Facial Recognition demonstrator - integration and validation plan http://nshield.unik.no/wiki/D7.2
- D7.3 Dependable Avionic System demonstrator - integration and validation plan http://nshield.unik.no/wiki/D7.3

The main objective of WP7 is the definition of each **application** scenarios in terms of Integration and validation plan.

The outcomes can be summarized as in the following for three of the four proposed scenaios:

- Definition of the demonstrator in terms of prototypes involved and architecture
- Analysis of the internal interfaces among the different prototypes being part of each demonstrator
- Description of the integration and validation activities approach.

Note for WP7
The official starting date of WP7 is with Milestone M3 at 1. March 2013. Most of the partners have started activities in advance to ensure that the envisaged applications are in line with the technology developments in nSHIELD.
As defined during the face to face meeting in Barcelona, a common Table of Contest for the Integration and Validation plan has been agreed and distributed to partners involved in T7.x. In addition to the planning of integration and validation, the document aims to define, in a detailed manner, the demonstrator main scheme, its architecture, the SHIELD technologies involved and the interface among the different subcomponents.

The identified use cases cover a wide variety of applications for «measurable security». Two of the use cases «Railway» and «UAV» clearly address the complexity of System of Systems, while the «facial recognition» addresses the embedded systems, and «Social mobility» the privacy related issues.
Though three out of four use cases are on track, the fourth use case on "social mobility" is hampered by the withdrawal of partners in Norway and the reduction of man months in Slovenia.

WP8 Objectives and Achievements summary

"Knowledge exchange and industrial validation" is the topic of this work package.
1st year deliverable: D8.4
2nd Year deliverables: D8.6, D8.5
The deliverable are available at:

- D8.5Preliminary Exploitation plan http://nshield.unik.no/wiki/D8.5

The WP8 objectives for the period are:

- The management of the nShield project public website http://www.newshield.eu.
- The elaboration of the exploitation plan in order to evaluate and explore the impact of the results on each scenarios
- Dissemination activities

The major achievements are:

- The identification and the analysis of the market reality within which the nSHIELD project could operate
- Participation to workshop and industrial dissemination. Details are provided in the description of WP8 activities.

Note for WP8
The major deviation is related to the deliverable D8.4: "SHIELD run-through" (previously known as D8.4: "Operational Manual v1"). For consequence also the elaboration
The elaboration of deliverables D8.4 and D8.6 has also been coordinated by MGEP. It must be mentioned that the delivery of these documents suffered considerable delay.

3 Work progress and achievements during the period

3.1 WP2

WP 2- Leader TECNALIA	
Period: 1 September 2012- 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner* The convergence to objectives is in line with the project and WP objectives. Summarising, the WP aims to: - Define SPD requirements and specifications for each layer and the overall system - Describe SPD metrics for overall system measurement - Define the overall architecture responding to a common architectural approach. During year 2 the following outcomes have been achieved. 1) Final SPD specification has been developed taking into account prototypes identified in WP6 and use case definitions of WP7. This task is finished but it should be open to new reviews further in project. 2) Metrics have been determined in a quantitative and formal way. During year 2, two ways for having an holistic measurement have been followed: a. Single metric approach – attack surface metric b. Multi metric approach – function analysis, fuzzy logic and genetic algorithms 3) Definition of a heterogeneous and distributed architecture which aims to link the dissimilar components of nSHIELD System – formalising structure
2	*Highlight clearly significant and tangible results* The following deliverables have been delivered and approved in the last review: 1) D2.6 SPD Final Specification is finished 2) D2.7 and D2.8 are being developed. 2.8 is developed in 80% while 2.7 will be ended by M26 Significant results are: 3) Requirements described in a standardized way to ensure a common understanding and to facilitate later exploration and usage for implementation and their close interpretation of use case and integration needs of WP6 and WP7 • Definition of SPD requirements for each layer, alignment with the architecture and convergence with different use cases described; • Description of requirements in a standardized way to ensure a common understanding and to facilitate later exploration and usage for implementation; • Preparation of a rationale for each identified requirement; • Final Requirements definition through the mapping between the requirements identified in the definitions phase and those actually achieved by the prototypes identified in Midlleware and Overlay layer definition (WP5) 4) SPD Metrics quantification and formalisation: nSHIELD full domain metrics have been identified and quantified. Composition methods have been analyzed, identified and new 2 approaches have been identified. SPD concepts are not linearly addressed but in different functional manners (logarithmic, exponentially…) <u>Single metric approach:</u> • Contribution (for the Common Criteria related aspects) to determination of metrics in a quantitative and formal way. The formalisation comes from three points of view: • Mathematical approach for measuring each of the metrics identified • Formal alignment towards specification and standards (Common Criteria) • Compositional approaches identified but not prioritised yet.

- Identification and quantification of nSHIELD full domain metrics
- Composition method derivation towards an incremental certification scope and view
- Identification of a formal model for SPD metrics
- Definition of a metric composition methodology able to produce a single SPD level for a nSHIELD compliant system.
- Definition of specifications data sheet that must be provided with each component that must be used within a system nSHILED compliant.
- Definition of a spreadsheet to determine the SPD level of an nSHIELD compliant system from the data provided by the manufacturers with each components that constitute it (data sheet)

Multi metric approach:

- Mathematically described each metric
- Functional description
- Expert system trhough fuzzy logic
- Learning system through genetic algorithms.

5) WP2 effort linking to WP6 new architectures based on prototypes: due to diversity of components and subsystems, the integration architecture of WP6 is being seen as an input for final nSHIELD Architecture. Both WPs are being working together as a task force for finalising the architecture in M26.
   - Contribution to finalization of nSHIELD Reference System Architecture;
   - verification of the conformity of the identified prototypes with the proposed nSHIELD System Architecture Definition of a heterogeneous and distributed reference architecture which aims to link the dissimilar components of nSHIELD System

3 *If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning*

No Applicable. Remarkable: a task force between WP2 and WP6 is being done so that final architecture deliverable would be

4 *If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)*

No applicable

5 *a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

WP2 Involvement and effort during the reporting period (MM)							
Partner	**MM**	**T2.1**		**T2.2**		**T2.3**	
		Plan.	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**
ASTS	11	1	1	2,82	2,83		
AT	8					1,24	1,3
TECNALIA	12	1	4,4	2	10	1	3
ETH	2		0		0		0
HAI	22	2	2	**1**	2	2	2,5
S-LAB	10	0,33	0,31	2	1,96		
SICS	6	1	1			1	1
T2D	10	1	1			2	2

	THYIA	13	0,167	0,167	0,167	0,167	0,167	0,167	
	TUC	10	1,2	1,2			1,3	1,3	
	SES	23	**1**	0	3	4,5	1	3	
6	*A statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*								
	An information flow towards RISC project of DG_HOME has been archieved as Tecnalia is participating in both project. RISC project aims at using part of public knowledge generated by nSHIELD in the challenge of Security and Dependability Measures.								
7	*A statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*								
	N.A.								
8	*If applicable, propose corrective actions*								
	N.A.								

Table 1: WP2 Management Report

3.2 **WP3**

WP 3 - Leader ISD	
Period: 1 September 2012- 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner* The activities of the second year of the project have been mainly focused on design and development activities. The results of these activities are described in detail in the deliverable D3.2 "Preliminary SPD node technologies prototype", that has been submitted as planned. This deliverable will be extended and finalized in the second part of the project based on the finalization of the requirements arising from the application scenarios and the overall SHIELD architecture. In some cases, prototypes available for demonstration have already been completed, as a result of this work. These demonstrators are described in detail in the deliverable D3.3 "Preliminary SPD node technologies prototype report". This deliverable will also be extended and finalized in the second part of the project. The research and designed activities have been focused on the following topics: - AT: Two main topics have been analysed and reported in the framework of this WP. The power supply protections of SDR/Cognitive enabled nodes and the anti-tamper modules. AT has designed a prototype to validate the studies performed in the fields of power supply protection and physical barriers for anti-tampering. - ATHENA: Prototype set of DDoS defense mechanisms; Novel cryptographic key exchange algorithm (Controlled Randomness). - ETH: Prototype of the face recognition system that will be used for demonstrations. Prototype of the embedded camera conceived for real environments (i.e. stadium scenario). - ISD: Development of an audio based surveillance/anti-tampering system. - SES: OMBRA architecture compatibility to the maximum extent with the nSHIELD node functionalities evaluation. Analysis of the node requirements and architectures focusing on the FPGA available on the prototype board. - S-LAB: Work on security evaluation methodology for partners' contributions (Hypervisor for Trusted Execution Environment and Secure Boot) - SESM: The nS-ESD-GW development process has been triggered exploiting the Xilinx Zynq ecosystem. This platform, being a hybrid device composed by a dual core ARM A9 and a 7-series Xilinx FPGA, provides tools and hardware for the development and the integration of firmware modules with software applications. To foster the diffusion of the SHIELD results across fervent Open Hardware and Open Software communities the ZebBoard has been exploited. - SICS: Secure hypervisor for security development with focus on Global Platform support and Linux porting. Secure boot design and development. - T2D: Secure boot integration with SICS. - TECNALIA: Analysis of inserting digital certificates for M2M in order to preserve privacy putting PKI infrastructure serving M2M (node to node). - TELC: For year 2, Telcred's work was initially planned to focus on evaluation of cryptographic schemes in collaboration with UNIGE. After discussion with the involved parties, we have instead shifted focus to implement such the form of a "secure lock controller" in collaboration with AT.

	- TUC: Smartcard authentication protocol, compact crypto library for resource-constrained devices, location anonymity component, implementation of the Gossamer protocol for automatic access control, ID-based key exchange protocol, GPU accelerated hashing lookup implementation. - UNIGE: Release of a prototype of scalable node according to the nShield three node typology, in the context of task 3.4. Development of a software library designed to support Elliptic Curve Cryptography in low-cost, low power programmable processors in the context of task 3.5. - UNIUD: Selection of reference architectures (real and emulated). Porting of a reference operating system (linux 3.4.4) on the target platforms. Development of a kernel driver for password management of protected SD memory cards. Initial development of user and kernel level power management, and of activity profiler. - HAI: research on TinyOS based nodes (IRIS, TelosB, MicaZ), on sensor resources (memory, CPU processing power), RF capabilities and different levels of node security (e.g. security in 802.15.4).
2	*Highlight clearly significant and tangible results* Both project deliverables for this period (D3.2 and D3.3) have been completed on time. The following results in terms of research, design and development have been achieved during this reporting period: - AT: AT participates in three tasks in the scope of the work package. Two main topics have been analysed and reported in the framework of this WP. The power supply protections of SDR/Cognitive enabled nodes and the anti-tamper modules. These analysis and design have been summarized in the internal deliverable D3.2 and the public one D3.3. In order to build a prototype to validate the technologies analysed, and taking into account that BeagleBone board has been considered one of the reference platform, AT, together with two other partners TELC and TUC, has designed a BeagleBone cape including different technologies studied in the scope of the project: Smart power unit + anti tamper solution + Smart Card (TELC) + ZigBee Module (TUC). During this reporting time the first design has been finalized and future steps are the manufacturing and testing phase. (Results: First design of a custom BeagleBone Cape.) - ATHENA: o Design and prototype implementation of the node reporting functions to support DDoS attacks mitigation mechanisms. In conjunction with task 4.2, those mechanisms have been simulated in OMNET++ environment and are currently in the process of integration with the prototype. o Design and prototype implementation for the controlled randomness protocol for cryptographic key exchange on the micro and power nodes. There is a partial implementation of the protocol in Beaglebone platform and is in the process of integration with the prototype. - ETH: o Design and implementation of the prototype of the face recognition system that has been conceived specifically to illustrate the functionalities of the SPD recognition process during demonstrations. This prototype is used also for development and test purposes. o Design of the prototype of the embedded camera that will provide the recognition functionalities in a real environment (i.e. the stadium scenario). - ISD: ISD has completed the design of a novel audio based surveillance system in accordance to the technical annex and has initiated its implementation. The system consists of three types of boards. The first of which has already been manufactured and debugged and the second one .has been manufactured and is under debugging. - SES: Prototypes, matching with WP2 requirements, specification and interface design. Inputs to

	the deliverables D3.2 and D3.3 and coordinator activities. - SESM: The technologies (SW, HW, Tool and BSP) necessary to support the development of the nS-ESD-GW have been firmly identified and acquired. The nS-ESD-GW development process, based on the WP2 requirements, has been triggered. In particular, several nS-ESD-GW sub modules have been developed such as the Coordination Module, Encryption Module and Data Integrity module. Currently the development process is completed at 80%, and there are two modules left to be implemented. We envision to deploy in the next year, a new custom version of the nS-ESD-GW, that will be specifically tailored on the avionic scenario. At same time activities of test and verification will be performed on the nS-ESD-GW. The modular architecture adopted improves the isolation of components fostering the requirements coverage. In particular, the activities achieved regard: o The definition and the design of the hardware and software architectures; o The definition of the communication policies and the development of the coordination module that is in charge to control and coordinate interrogations and messages; o The implementation and the integration of a custom FPGA-based IP module to perform data encryption and decryption with the aim to ensure the long-term secure storage of private information; o The development of a data integrity module to assure accuracy and consistency of data exchanged among the nSHIELD middleware and legacy nodes. - SICS: Almost finalized a complete Linux port of the hypervisor for security on Beaglebone. Global platform design ready and implementation almost completed during the period. Secure boot design agreed and verified together with T2Data. - T2D: A secure boot design developed together with SICS and we successfully showed secure boot of the SICS hypervisor and FreeRTOS on Beaglbone. - TECNALIA: Performed work in the analysis of inserting digital certificates for M2M in order to preserve privacy putting PKI infrastructure serving M2M (node to node). - TELC: An approach to a framework for delegation of access rights has been developed through a M.Sc. thesis. - TUC: o Task 3.1: Design of a smartcard authentication protocol based on symmetric keys, able to work on any TPM. The scheme has been implemented and tested in a LAN. We have looked into integrating the smart card module into BeagleBones, so as to integrate it in the TUN interface described in WP5. o Task 3.2: Implementation of a compact crypto library in C, for a subset of lightweight ciphers and compact implementations of standard ciphers. o Task 3.4: ▪ An anonymizer component based on the k-anonymity concept has been developed for nSHIELD applications, where personal location privacy is to be preserved, while enabling the system to provide location monitoring services. ▪ Implementation of the Gossamer protocol for automatic access control functionality. ▪ Contribution to D3.1 (SPD node technologies assessment) in Section 6 (Dependable self-x Technologies). o Task 3.5: ▪ Investigated secure protocols and methods for establishing cryptographic keys among communicating parties, using Identity Based Cryptography. One such scheme has partially been implemented.

- Contribution to D3.2 in section 6.4 (An Identity-Based Encryption scheme).
- Contribution to D3.3 in section 6.3 (Identity-Based Encryption).
- Development of a lightweight, efficient, GPU accelerated hashing and hash lookup mechanism utilizing the CUDA GPGPU toolkit. Significant speed-ups have been achieved.

- UNIGE: In the context of task 3.4 a demo has already been released: the Elliptic Curve Cryptography running in the node prototype with a comparison of running time with a standard PC. In the context of task 3.5 a prototype of the software library designed to support Elliptic Curve Cryptography in low-cost, low power programmable processors has already been released.
- UNIUD: Finalized port of the target operating systems on all the target platforms. Demo of the features related to the SD cards memory management
- THYIA followed the project, no active participation.

3 *If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning*

N/A

4 *If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)*

N/A

5 *a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

The following table summarizes the use of resources for every partner:

WP3 Involvement and effort during the reporting period (MM)											
Partner	**MM**	**T3.1**		**T3.2**		**T3.3**		**T3.4**		**T3.5**	
		Plan.	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**
AT	22	0	2	2.5	5.7	2.5	0			2.7	2
ATHENA	8							1	1	2	2
TECNALIA	6							2	3.1	1	2
ETH	25			6	6						
HAI	4							2	2		
ISD	58					24	26				
S-Lab	12							1.85	1.45	2	1.5
SESM	15					8	8				
SICS	20	1	1	4	12	2	2				
T2D	26	1	1	6	10	2	2				
TELC	6									3	0.6
THYIA	7	0,2	0,1	0,2	0,1	0,2	0,1	0,2	0,1	0,2	0,1
TUC	30	2.4	2.4	2.4	2.4			2.4	2.4	5.6	5.6
UNIGE	30							6.5	6.5	7	7
UNIUD	12	4	4								
SES	24	2,1	0,6	2,1	1,4	3	1,2	0,5	0,5	0	0

	For Telcred in T3.5: Behind schedule due to a) shift of focus from evaluating cryptographic schemes in collaboration with UNIGE to implementing such in collaboration with AT, and b) now waiting for input from AT
6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*
	N/A
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*
	TUC: • Lightweight Cryptography for Embedded Systems – A Comparative Analysis Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Rantos, K. 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), Egham, U.K., 12-13 Sep. 2013. Accepted for publication. • CasperCommunity: A Lightweight Anonymity & Location Privacy Service Fysarakis, K.; Adamopoulos, A.; Manifavas, C.; Papaefstathiou, I. IEEE International Conference on Communications (ICC), Sydney, Australia, 10-14 June 2014. Submitted. • Integrated Hardware Implementation of PRESENT and SPONGENT Hatzivasilis, G.; Floros, G.; Manifavas, C.; Papaefstathiou, I. IEEE International Conference on Communications (ICC 2014), Communications and Information Systems Security Symposium (CISS), Sydney Australia, 10-14 June 2014. Submitted. UNIGE: • C. Peretti, P. Gastaldo, M. Stramezzi and R. Zunino. "Embedded implementation of Edwards curve- and extended Jacobi quartic curve-based cryptosystems" submitted to the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)
8	*If applicable, propose corrective actions*
	N/A

Table 2: WP3 Management Report

3.3 WP4

WP 4- Leader SES	
Period: 1 September 2012- 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner*
	The activities of the fourth semester of the project have been mainly focused on prototype design and implementation activities, as well as integration with WP7 (common demonstrators). The results of these activities are described in detail in deliverables D4.2 and D4.3. The final versions of deliverables D4.2 and D4.3 were submitted in month M22. Future validation and verification mechanisms for the prototypes developed in WP4 were described in deliverable D6.2. The aforementioned activities have encompassed the following topics: • ATHENA: Algorithms for recognizing & modelling denial-of-service attacks • HAI: Development of a trusted routing prototype based both on direct evidence and reputation for wireless sensor networks. • ISL: Development of a secure channel for the communication of the nSHIELD nodes, based on cc2420 hardware security, providing CTR, CBC-MAC and CCM algorithms. • MGEP: Focus placed on the design and implementation of reputation based intrusion detection system for wireless sensor networks prototype • SES: WP4 coordination; participation of development of Smart Transmission Layer • TECNALIA: Development of QoS for DLMS Network converging with nSHIELD requirements. • TUC: A prototype of a novel modular and configurable reputation and trust-based system for secure routing and intrusion detection was designed and implemented. Also, an IPsec scheme able to provide both confidentiality and message authentication by utilising only ESP with AES-CCM* was developed. Both schemes have been designed for deployment on embedded system devices. • UNIGE: Focus was placed on deployment of the SPD-driven Smart Transmission Layer prototype • UNIUD: Theoretical framework for dependable computation; preliminary software implementation of the framework
2	*Highlight clearly significant and tangible results*
	Both project deliverables for this period (D4.2 and D4.3) have been submitted in M22. The following results in terms of research, design and development have been achieved during this reporting period: - ATHENA: A methodology to recognize and model denial-of-service attacks based on network traffic, power consumption and signal strength traffic was developed. This methodology comprises the parallel operation of two algorithms, one based on real time statistical analysis and one on pattern identification. Algorithms are being simulated in the OMNET++ platform and porting to real hardware (beaglebones) is imminent. - HAI: Implementation and evaluation of Trusted Greedy Perimeter Stateless Routing (T-GPSR) for TinyOS-based motes. This routing protocol using both direct evidence and reputation messages

is able to counteract against several network layer attacks ensuring undisrupted routing operation.

- ISL: Implementation and evaluation of different algorithms to provide link layer security based on tinyOS motes. Study of the energy consumption and validation of authenticity and confidentiality in the communication.
- MGEP: Initial implementation of the reputation based IDS on Zolertia Z1 hardware.
- SES: WP4 coordination; setting up the Smart Transmission Layer (with UNIGE)
- TECNALIA: SPD functionality implementation in DLMSCosem network: towards defining an industrial trusted and dependable connectivity.
- TUC: A prototype of a novel modular and configurable reputation and trust-based system for secure routing and intrusion detection was designed and implemented. The prototype was implemented in ns-2 simulator, in C++ language. The system extends the routing protocol DSR. Furthermore, a protocol that secures nSHIELD exchanged messages at the network layer, extending the standardized IPSEC protocol and adapting it to the restricted environment of sensor nodes, was finalized and developed for specific platform (Contiki). The corresponding measures taken demonstrate that this solution is a strong candidate for protecting communications, while providing additional benefits compared to other mechanisms working at other layers of the TCP/IP communication stack.
- UNIGE: Setting up the SPD-driven Smart Transmission Layer test bed; its initial testing and validation. Further validation of the performance of developed anti-jamming algorithms through the developed C++ simulator.
- UNIUD: Completed theoretical framework for model-based distributed computation; completed implementation of the deployment routines; identified proper technologies for the implementation of synchronization/persistence layers

3

If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning

Final versions of deliverables D4.2 and D4.3 submitted with 4 month delay, as – compared to the previous versions – they were supplemented with most up-to-date results from each of the partners.

4

If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)

UNIUD: due to a delay in the definition of the application scenario and of the corresponding requirements, the theoretical framework had to be partially redesigned; as a consequence, greater effort was required within WP6, and a working preliminary prototype could not be developed by the end of this period

5

a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)

The following table summarizes the use of resources for every partner during the 2nd year (3rd and 4th semester):

WP4 Involvement and effort 2nd year (3rd + 4th semester) (MM)									
Partner	**MM (whole project)**	**T4.1**		**T4.2**		**T4.3**		**T4.4**	
		Plan.	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**	**Plan.**	**Eff.**
ATHENA	10	0	0	5	5	0	0	0	0
TECNALIA	14	0	0	3	4	0	0	4	5,8
HAI	15	0	0	0	0	5,5	9	2	2
ISL	34	0	0	0	0	6	6	11	11

MGEP	20	0	0	0	0	6	6,1	2	1,9
THYIA	3,5	0,167	0,167	0	0	0,167	0,167	0,167	0,167
TUC	14	0	0	0	0	2,4	2,4	3,2	3,2
UNIGE	25	7	9	5	6,5	0	0	0	0
UNIUD	12	0	0	6	4	0	0	0	0
SES (SE+SG)	84+10	20	18	12	13	1	1	3	2

Partners' statements on the use of resources is as follows:

- HAI: HAI used more than planned of its allocated T4.3 resources (9 pm instead of 5,5). Among the reasons are: less than planned effort was consumed during the previous periods and resource demanding trusted routing was implemented during second year (TinyOS code on sensors).
- SES: additional resources were put forward into development of the hardware components necessary for realization of the SPD-driven Smart Transmission Layer (T4.1)
- TECNALIA: Due to cost changes during in proposal phase and execution phase, TECNALIA is spending more effort for this period in WP4
- UNIGE: had additional efforts invested in collaboration with other partners (namely SES) for defining final demonstrators and scenarios and adapting developed algorithms to them
- UNIUD: some planned effort for this period had to be held back in order to focus on integration issues in WP6

6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*
	N.A.
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*
	The following academic dissemination activities (publications) were performed during the 2nd year of the project: • Dabcevic, K.; Marcenaro, L.; Regazzoni, C. S. "Security in Cognitive Radio Networks" - book chapter for "Evolution of Cognitive Networks and Self-Adaptive Communication Systems", IGI Global, 2013 • Mughal, M. O.; Razi, A.; Alam, S. S.; Marcenaro, L.; Regazzoni, C. S. "Analysis of Energy Detector in Cooperative Relay Networks for Cognitive Radios", Proceedings of the 7th International Conference on Next Generation Mobile Apps, Services and Technologies, NGMAST 2013 • Rantos, K.; Papanikolaou, A.; Manifavas, C.; Papaefstathiou, I. "IPv6 Security for Low Power and Lossy Networks", IEEE/IFIP Wireless Days 2013, Valencia, Spain, 13-15 Nov. 2013. – ACCEPTED FOR PUBLICATION • Rantos, K.; Papanikolaou, A.; Manifavas, C. "IPsec over IEEE 802.15.4 for Low Power and Lossy Networks", ACM 11th Int. Symposium on Mobility Management and Wireless Access (MOBIWAC 2013), Barcelona, Spain, 3-8 Nov. 2013. - ACCEPTED FOR PUBLICATION • Hatzivasilis, G.; Papaefstathiou, I.; Manifavas, C. "ModConTR: A modular and configurable trust and reputation-based system for secure routing in ad hoc networks", IEEE International Conference on Communications (ICC 2014), Ad Hoc and Sensor Networking Symposium (AHSNS), Sydney Australia, 10-14 June 2014. – SUBMITTED • Hatzivasilis, G.; Manifavas, C. "Building Trust in Ad hoc Distributed Resource-sharing Networks Using Reputation-based Systems", 16th Panhellenic Conference on Informatics with international participation (PCI 2012), University of Piraeus, Greece, 5-7 October, 2012.
8	*If applicable, propose corrective actions*
	UNIUD: the software implementation of the final prototype will be completed on schedule by moving the unassigned MMs to Y3

Table 3: WP4 Management Report

3.4 WP5

WP 5- Leader Selex-ES	
Period: 1 September 2012 - 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner*
	Task 5.1 SPD driven Semantics The objective of this task is to define the semantic data structures necessary to make the SHIELD framework work. Following the guidelines declared in Deliverable 5.1, UNIROMA1 and SES spent the second year of the project to derive the new SHIELD models, in close collaboration with the people involved in the definition of the SHIELD metric (mainly TECNALIA and SES) as well as with the demonstrator teams, since both metrics and application scenarios are the key drivers for the semantic model design. With respect to the identified challenges, taking into account i) the inputs from the pSHIELD final review and ii) the scenarios definition, additional studies have been carried out to find the adequate models and methodologies that represent the official SHIELD Formal Model. The methodology identified to build the "knowledge base" used by the SHIELD Middleware to compose SPD functionalities, is based on the decoupling between "domain information" and "security information", and has been refined and tailored to the middleware architecture (liaison with Task 5.2). The candidate set of semantic technologies has been reduced, mainly focusing on semantic representations that allows: i) a technological abstraction of components and ii) the deployment of a connector algebra to identify potential relation, leaving to the domain data bases the task of specifying them in detail. Preliminary models of the SHIELD components have been produced and formalized (in a language close to the demonstrator needs). These models represent one of the WP5 prototypes. Analysis on semantic parsers in Java language, to be integrated in the OSGI platform, have been performed at design level. However, preloaded models are being prepared as first solution for the prosecution of integration phases. Preliminary Analysis about the integration between policies representation and semantic representation have been started Some additional work has been performed in liaison with WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve semantic technologies and their implementation HAI conducted an assessment on UML diagrams, candidates for the nSHIELD semantic model As an additional topic, Intrusion detection systems have been examined. Intrusion detection systems can be defined as a set of different scanners that monitor the activities of an information system looking for malicious actions. In the scope of the project, the IDS will be the first safety barrier for possible attacks against the system, warning of possible attacks to maintain reliability and availability of the network. From the point view of ontologies, intrusion detection can be considered as possessing several characteristics and classifications and it needs a language that describes instances of that ontology. MGEP has participated in the assessment of several proposed ontologies for intrusion detection. MGEP has proposed an ontology from the literature and has created an extension of pSHIELD ontology that includes some IDS properties.

Task 5.2 Core SPD services (ex T5.2+T5.4)

The objective of this task is to define the basic middleware services that represent the core of the SHIELD platform.

Following the guidelines declared in Deliverable 5.1, UNIROMA1 has stated the design and development of the new SHIELD Middleware Core services, in order to meet the new project needs (dynamic composability and more security functions). As first step, an architectural refinement has been performed to introduce the new bundles representing the new middleware components (Secure Discovery, Security agent and interfaces with Intrusion Detection Bundle) and the OSGI platform has been confirmed also for the nSHIELD project, arising the need of aligning the new partner to the use of such kind of platform. With respect to this, significant effort has been put in place to enable the new partners to seamless integrate with the OSGI heritage from pSHIELD (UNIROMA1 is the owner of the software platform).

Then, intensive studies have been carried out to select the most suitable solution to implement the innovative SHIELD Secure Discovery. The corresponding bundle has been preliminarily developed in the OSGI framework and represents one of the WP5 prototypes. In particular, extensive analysis has been performed to define the architecture of the SHIELD Security Agent (see also Task 5.4) and the corresponding bundles have been preliminarily developed in the OSGI framework, thus representing another WP5 prototypes.

Some work has been done on the implementation of the OSGi-DPWS interface, to allow interoperability between the nSHIELD architecture and the DPWS-compliant policy-based management infrastructure developed by TUC in T5.3. Appropriate technologies have been identified and, after successful setup of existing nSHIELD OSGi framework (Knopflerfish), will be integrated.

Interoperability issues between interfaces and between interfaces and the nSHIELD platform have been identified and addressed, mainly with the objective of identifying a common ground and facilitate cooperation at later stages (namely integration and demonstration).

Regarding the multi-layered Overlay Security: a secure overlay solution has been designed and built, that is transparent to end “application”. This means that this solution do not require any modification to the current end device applications. The current version implements a threshold DoS detection mechanism. The current code basis will be provided as open source in order to be re-used as open source solution. We discuss with other partners opportunities for integrating this approach with the OSGi framework.

With respect to the Intrusion Detection Bundle, in the first half of the period SLAB developed a preliminary version of technologies for middleware core and innovative SPD services and a prototype of Intrusion Detection Bundle. In the second half of the period, in frame of D5.2, SLAB developed Preliminary SPD middleware and overlay technologies prototype. Moreover SLAB:

- developed and interfaced a preliminary DDOS protection,
- collected and edited the Middleware Interface report,

In order to address security, privacy and dependability (SPD) in the context of ESs as "built in" functionalities, with the long term objective of promoting the SPD certification for future ESs, SES edited a Protection Profile for the Middleware layer. This must be seen as a first step to define a security problem definition and security objectives for embedded systems (ESs) which aim to be SHIELD compliant.

In the scope of the Adaptation of Legacy Systems, ATHENA developed a specific solution:

i) ad-hoc software on the server side, i.e. bundles that register to R-OSGi the nSHIELD services in order to make them visible outside.

ii) ad-hoc software on the client side, i.e. bundles that connect to a GW and get the service.

For demonstration purposes, a simple scenario has been set-up. On one hand a very simple service Nservice (Echo Service) runs in server side and registers itself to R-OSGi. On the other hand the client side runs a LeNoReSer (Legacy Node Service) that connects remotely to the nSHIELD server and gets the Remote nSHIELD

service (Echo Service).

As a result of the above a local proxy for the remote service is created. The service proxy is registered with the local service registry and can also be retrieved like a normal OSGi service.

In the performed test the Echo service is running on a machine and the ad hoc software bundle registers it in R-OSGi.When the ad hoc LeNoReSer runs on another machine on the network gets the Echo service from the remote machine and displays a message.

A scenario that makes use of nSHIELD services by Legacy Systems is applicable.

Task 5.3 Policy-based Management

This task aims at designing and developing a SPD-middleware policy-based management for ensuring a high level of security, privacy and dependability in systems composed by Intelligent ES Nodes (developed in WP3) and based on Smart Transmissions (developed in WP4) on the base of the metrics identified in task 2.2. In order to build specific management functionalities and procedures for accomplishing these objectives, several aspects will be investigated and analysed.

In this task ISL is studying what kind of policies can be proposed, among all, ISL has identified the following kind:

- Power policy-based: change the roles of the nodes in function of the battery or power life of them. For instance:
  - If Nodei.getremaingBattery() <= threshold then REDUCE the routing capabilities of the node and turn it into a “leaf node”.

  Thus in this study we have to perform an analysis of different thresholds in order to propose proper values for different kind of nodes and roles.
  - If Nodei.getremaingBattery() <= threshold then CHANGE the routing capabilities of the node.

  Thus in this study we have to perform an analysis of different thresholds in order to propose proper values for different kind of nodes and roles. Moreover, in this case we have to propose (in conjunction) with WP4 different routing schemes.

- Security policy-based: change the roles of the nodes in function of the certificates of nodes. For instance:
  - If Nodei.getFQDN().equal(“STRING”) decide what kind of functionalities, permissions, roles or responsabilities this node has.
  - If Nodei.getOrganizationalUnit().equal(“STRING”) decide what kind of functionalities, permissions, roles or responsabilities this node has.

Summarizing use the nodes’ certificates to apply policies in the middleware or application layer.

HAI coordinates the work that has to be undertaken for the development of the corresponding components for a working prototype to demonstrate a policy-based management solution on embedded systems. Emphasis has been given on the achievement of a common understanding about the solution and the mechanisms chosen (e.g. operating system, infrastructure, interfaces) to ensure the required interoperability among stakeholders

HAI contributes to the finalization of the description of a policy-based management solution and the mechanisms that comprise it

HAI collaborates with other partners regarding the platforms chosen to demonstrate this solution

TUC elaborated further on the proposed framework by narrowing down the alternatives based on published findings and research undertaken on the field. Also collaborated with other partners for a common agreement on the proposed model and the work that needs to be undertaken for a prototype both on the

technical level, regarding the format of the exchanged policy messages and their protection, as well as on policies' definition.

TUC conducted further research and hands-on testing in order to finalize the heterogeneous hardware platforms, operating systems and application environments to be used. This preliminary work, which involved consideration of the computational and power needs of the corresponding policy management components, will provide the basis for the development of the prototype of the chosen mechanisms.

TUC worked on finalizing the aim and outline of the demonstration scenario for the proposed framework. SES defined a policy classification and hierarchy so to have a common model to policy definition in nSHIELD project. This model aim to be valid for:

- Those policies to be used as input to a Policy-based management which aim to ensure a defined level of security, privacy and dependability
- Those policies that serve as the governing reference for any required adaptation a particular scenario may require.

Task 5.4 Overlay monitoring and reacting system by security agents (ex T5.5)

The aim of this task is to develop control algorithms that could drive the composability of Embedded System for Security purposes.

Following the guidelines declared in Deliverable 5.1, UNIROMA1 has stated the design and development of the new SHIELD Overlay and control algorithms, in order to meet the new project needs. Extensive investigations have been performed to confirm the theoretical framework for SPD composability, and two candidate technologies have been selected: Petri Nets and Coloured Petri Nets.

The first formal model for theoretical composability of SPD functionalities have been developed based on Coloured Petri Nets. Intensive simulations have been performed to validate this model in a significant scenario in line with the SHIELD requirements. These models and simulations represents one of the UNIROMA1 prototype.

A second formal model have been identified, in strict liaison with the definition of the SHIELD metric. This approach is based on the translation of the "attack surface" concept into an optimization problem and in the application of optimization algorithms to find candidate solutions. Preliminary analysis are being performed.

Liaisons between the modelling of SPD functionalities for control purposes, and their semantic representation (Task 5.1) have been maintained and enriched.

The architecture of the Security Agent has been preliminarily translated into code at Middleware level (see also Task 5.2) and the harmonization of the decision making process (metrics vs policies vs control algorithms) has been preserved in this first implementation.

Some preliminary studies on the interaction of several security agents (either at architectural or theoretical framework level) have been performed in order to identify potential solutions to drive architecture and control algorithms refinement.

HAI has started working on the multi-layered Overlay Security Agent, in the direction of the design of abstracted and open user services

Transversal WP activities and remarks:

Support to WP5 coordination activities has been provided by UNIROMA1 (in particular it is T5.4 leader)
Preliminary investigations to the demonstrator architecture definition for WP6
Maintenance of a repository server to improve WP5 participants awareness and collaborative work
The outcomes of the above mentioned activities, performed in the scope of WP5, will be used as inputs by WP2 with respect to requirement and architecture, thus resulting in additional contributions to WP2

	deliverables.
2	*Highlight clearly significant and tangible results*
	Deliverables: The above mentioned results have been used mainly as major inputs for -Deliverable 5.3 in terms of report of designed solutions and -Deliverable 5.2 with respect to the development of prototypes. Additional input have been provided to Deliverable 2.X (requirements and architecture refinement) **Prototypes:** - MGEP has created a sample ontology for Intrusion Detection Systems that extends the ontology delivered in pSHIELD. A suitable candidate ontology has been also proposed. - UNIROMA1 has created simple models to support the SHIELD semantic - UNIROMA1 has developed the SHIELD Secure Discovery bundle - UNIROMA1 has developed the SHIELD Security Agent bundle - UNIROMA1 has created a Coloured Petri Net model for the SHIELD System - SES has created a Protection Profile for the SHIELD Middleware - SES has identified criteria to Policy Definition and classification - S-LAB has developed a prototype of Intrusion Detection Bundle - ATHENA has developed a sample scenario to demonstrate Adaptation of Legacy Systems - TUC has proposed a Policy Based Access Control code - TUC has proposed an Overlay Agent Solution
3	*If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning*
	Not applicable
4	*If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)*
	Since UNIROMA1 was the main contributor and owner of the OSGI platform, on which also the nSHIELD prototypes will be developed, a time-consuming effort was needed to allow the new partners to integrate their new prototypes into a consolidated software code. The reason for not being right on schedule (mainly in terms of contribution in WP5 deliverables) is the delay in the finalization of some necessary inputs (also from other tasks), which has introduced a delay in the formalization of some key concepts in WP5. This is mainly due to metrics and demonstrators definition. However the delay will be recovered in the last year of the project, since good basis in the above mentioned critical fields have been put.
5	*a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

WP5 Involvement and effort Y2 (MM)

Partner	MM	T5.1		T5.2		T5.3		T5.4	
		Plan.	Eff.	Plan.	Eff.	Plan.	Eff.	Plan.	Eff.
ATHENA	14			4	4				
TECNALIA	20	2	3	3	3,4				

	HAI	27	2	1,5			5	6	2	1,5
	ISL	18					12	12		
	MGEP	8	7,5	7,5						
	S-LAB	28			11,06	12,33				
	THYIA	4,5	0,125	0,125	0,125	0,125	0,125	0,125	0,125	0,125
	TUC	18			4	4	3,2	3,2		
	UNIROMA1	41	4,3	4	6,7	6,3			8,7	8,1
	SES	53	7	6,5	4	4	6	6,5	4	4,5
6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*									
	Not applicable									
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*									
	A press release has been published few months ago in ISL. Organization and chairing of the Embedded System Security Session in the XII Spanish Meeting on Cryptology and Information Security (RECSI 2012), Donostia-San Sebastián (Spain), 4-7 September 2012. Post in the Mondragon University ICT blog: http://mukom.mondragon.edu/ict/mu-at-artemis-and-itea-2-co-summit/									
8	*If applicable, propose corrective actions*									
	Increasing the number of meetings (skype, telephone) in order to coordinate the different proposals of partners involved in WP5.									

Table 4: WP5 Management Report

3.5 WP6

WP 6- Leader HAI	
Period: 1 September 2012- 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner* The convergence to WP6 objectives has been in progress during the 2nd nSHIELD year. Summarising, the WP has 3 major objectives distributed correspondingly in 3 tasks. The tasks are divided in two periods, delivering two versions of 3 documents. The reporting period under examination concerns the first stage of this process: 4) T6.1: Aims at integrating components and prototypes developed in WP3, WP4 and WP5. 5) T6.2: Plans and conducts the validation and verification of the implemented solution. 6) T6.3: Aims at guaranteeing the proposed architecture to be future-proof, to support the installation, download and upgrade cycle and to address the security and integrity issues involved. The integration methodology incorporates input from and establishes interactions with the main topics of nSHIELD work, including requirements, metrics, architecture, layers, scenarios and developing technologies. A consortium's common decision organizes component integration based on the scenarios in which these components participate. The integrated components have to be verified and validated, initially as individual units and subsequently as a common platform. The latter has to be tailored and refined to reflect the specific needs of application scenarios. The guidelines and the plan for ensuring the future viability and reliability of nSHIELD SPD architecture are described. The engineering life cycle is supported by the phases of installation, operation and upgrading, while in parallel the security and integrity issues involved are addressed. The aforementioned activities were distributed between partners as follows: • HAI: Coordination of D6.3; Definition of integration methodology and framework (T6.1); Contribution in Network verification covering requirements-prototypes-verification; Verification procedure and tests validating the proposed Reputation-based schemes (T6.2); Forming SPD lifecycle procedures for nSHIELD, based mainly on the international standard ISO/IEC 12207 (T6.3). • ASTS: Definition of prototype to be integrated in the railway scenario; Analysis of Validation and Verification process for each prototype. • AT: Within the scope of the project, Acorde (AT), Telcred (TELC), and SICS are collaborating on developing a secure micro node, which can be used as a lock controller. A custom "cape" for a standard BeagleBone low end Linux computer has been developed. This cape will provide features such as tamper detection, backup power, secure storage of cryptographic keys, and a real time clock. This prototype will worked as an offline access control and it has been included in the list of nSHIELD prototypes. • ATHENA: Definition of and validation methodology for the following nSHIELD prototypes; Recognizing DoS attack prototype, Key Exchange Protocol prototype and Adaptation of Legacy System prototype. • SES: Definition of and validation methodology for the nSHIELD prototypes; Contribution to Validation and Verification procedure of Middleware Protection Profile; Coordination of D6.2. • TECNALIA: Development of the plan for lifecycle and SPD support. Tecnalia has led this deliverable that develops SPD lifecycle methodology (D6.1). • ISL: Preliminary validation and verification tests of the link layer security prototype have been

	done in order to integrate the prototype on the different scenarios. • MAS: Established new partnership with Seek and Find (SknFnd) to establish the prototype for the SHIELD Social Mobility Use case. Review and evaluation work on the use case. Implementation work on motorbike for policy-based access to information. • ALFATROLL: Ongoing implementation of the IQEngine as part of the UAV use case. • SknFnd: Delivery of prototypes to the Social Mobility use case. Requirement work on the use case, development of policy-based access for the prototype and work on the service interface are ongoing activities. • S-LAB: Security Evaluation methodology supplementing Validation and Verification of secure technologies; validation of node prototypes (Hypervisor and Secure Boot) supplemented by the methodology; description and validation of Intrusion Detection System for Middleware. • UNIUD: Preliminary integration to the Voice/Facial recognition scenario; redesign of some features of the proposed distributed computation framework to accommodate scenarios requirements: the framework has shifted from a cellular-automata model to a higher-granularity dataflow model. • UNIROMA1: has supported the definition of the SHIELD common platform architecture as well as the demonstrators' architecture with respect to Middleware and Overlay technologies. In addition it has started all the activities necessary to integrate the OSGI Middleware and Overlay prototypes into the Avionic and Railways demonstrators. Last, but not least, a validation plan has been identified for the above mentioned prototypes. • MGEP: has collaborated in the definition of the integration scenarios • THYIA followed the project, no active participation.
2	*Highlight clearly significant and tangible results* The results of the three 2nd year WP6 deliverables (D6.1, D6.2, D6.3) are summarized below: • SPD lifecycle principles in nSHIELD • Planning methodology and phases of system's lifecycle • Validation and verification methodology • Validation and verification of prototypes • Integration methodology • Components per application • Initial integrated systems per application Some of partners' activities that produced the aforementioned results are listed below: • HAI: Structure of integration methodology, based on the involvement of individual prototypes in each scenario; Tests for trusted routing, proposal of testing format and techniques; Finalization of D6.1. • ATHENA: Contribution to prototype descriptions. • SES: produced input to Middleware deliverables (D5.2, D5.3) • TECNALIA: D6.1 was finalized under the coordination of TECNALIA. Next document (D6.4) has been initiated. • MAS: contribution to prototype description. • ALFATROLL: IQEngine prototype description. • SknFnd:Social Mobility prototype description.
3	*If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning* The three deliverables have due dates inside the period M18-M22. Although D6.1 was finalized on time, all three deliveries are foreseen for the period prior to the second year review. This is due to the fact that D6.2 and D6.3 have to follow the developments (and therefore also the delivery dates) of all the other "technical" documents. This combines with the general shift of the temporal milestone of deliverables that were due for the second year, from their actual submission date to a prior to review plausible date.

4	*If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)*
	Reasons for delays in the achievement of critical objectives include: • SES: Unable to contact partner THYIA

5 — *a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

Partners' statements concerning the use of resources in the reference period are provided below:

- UNIUD: some planned effort for Y3 had to be shifted into Y2 in order to better integrate the prototype into the chosen scenario; no issues are expected due to the reduced MMs available for Y3.
- SES (ED): Resources have been temporarily diverted from WP6 to WP2 in order to overcome the problems arising from THYIA poor contribution during the period. For this reason within WP2 an effort greater than the planned one has been spent while with regard to WP6 the actual effort was reduced (in the first six months).
- TECNALIA: Due to cost changes during in proposal phase and execution phase Tecnalia is spending more effort for this period in WP6 for task 6.3.

The following table summarizes the use of resources for every partner during the 2nd year:

WP6 Involvement and effort Y2 (MM)

Partner	MM (whole project)	T6.1		T6.2		T6.3		Total (Y2)	
		Plan.	Eff.	Plan.	Eff.	Plan.	Eff.	Plan.	Eff.
HAI	32	9	9	4	4	3,5	3		16
TECNALIA	15					7	12,8	7	12,8
ASTS	8	2	2	1,54	1,54			3,54	3,54
AT	19	6	6.7	3.5	3.5	0	0	9.5	10.2
ATHENA	21	3	3	3	3			6	6
ISL	14	11,5	11,5	0	0	0	0	11,5	11,5
MAS	7	1	1	2	2			3	3
MGEP	3	0,2	0,2	0	0	0	0	0,2	0,2
THYIA	2	0,167	0,167	0,167	0,167	0,167	0,167	0,167	0,167
ALFATROLL	5			4	4			4	4
SknFnd	0			1	1			0	2
S-LAB	29	3	1,15	5	4	4	1,7	12	6,85
UNIROMA1	4	2	2					2	2
UNIUD	6	0	0	2	3	0	0	2	3
SES	36	7	2	3	1	2	1,3	12	4,3

6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*
	N.A
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*
	S-LAB: Planned dissemination activity - conference paper in preparation for PECCS2014 about Security Evaluation methodology supplementing Validation and Verification of secure technologies SES: No dissemination activities.
8	*If applicable, propose corrective actions*
	Corrective actions proposed by partners include: • SES: Tasks and duties allocated to partner THYIA have been re-distributed among other partners

Table 5: WP6 Management Report6

3.6 WP7

WP 7- Leader Movation	
Period: 3 – September 2012 - August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner*
	The main objective of WP7 is to validate the nSHIELD approach on real application demonstrators, and by that contributing *(i)* to the feasibility of the nSHIELD approach and *(ii)* creating applications to form the basis for successful industrial dissemination and exploitation. The identified use cases cover a wide variety of applications for «measurable security». Two of the use cases «Railway» and «UAV» clearly address the complexity of System of Systems, while the «facial recognition» addresses the embedded systems, and «Social mobility» the privacy related issues. The official starting date of WP7 is with Milestone M3 at 1. March 2013. Most of the partners have started activities to ensure that the envisaged applications are in line with the technology developments in nSHIELD. WP7 is organised in four tasks, each of them representing one of the use case scenarios. Each task focusses on one application scenario, resulting in the respective deliverables D7.1, D7.2, D7.3 and D7.4 with focus "Integration and Validation Plan" for the desired application.
2	*Highlight clearly significant and tangible results*
	The identified use cases cover a wide variety of applications for «measurable security». Two of the use cases «Railway» and «UAV» clearly address the complexity of System of Systems, while the «facial recognition» addresses the embedded systems, and «Social mobility» the privacy related issues. ***Alfatroll:*** One important field to be covered is the "Reliable Avionic Systems" field. Alfatroll has contributed with its unique technology, and intends to demonstrate how even complex solutions involving unmanned systems can be solved in a non-complex manner and with high reliability. In addition to the clarification in the bullet point above, Alfatroll did not start from zero, and introducing its already proven technology in the project is a major contribution. All necessary components for the solution has been identified and are now in place. Suitable and efficient developers are also in place, and the specification of the work to be done is 75% finished. The remaining part will be specified as the activity progresses. The development work proceeds according to the plan, and this seems to be the case also for the next phases. **ASTS** had the focus on definition and analysis of a Reference architecture for the scenario demonstration, including a preliminary Analysis of threat scenarios and related risk analysis. From this analysis the follow on steps were the definition of application scenarios, the definition of SHIELD prototypes to be integrated in the architecture of railway and the preliminary analysis of Validation and Verification process for the scenario. ***IPS Sistemi Programmabili*** (ETH) is responsible for the "Face and voice recognition scenario". During the reporting period ETH has been involved in the definition of this scenario and of the related uses cases. In this context, ETH coordinated the plan of the integration, validation and testing activities. It is responsible for deliverable D7.2 "Voice/Facial Recognition demonstrator - integration and validation plan". During the

reporting period ETH focused on the implementation of the prototype for face recognition and on the implementation of the hardware of the final embedded camera. The prototype that will be used for demonstrations is currently available, while for the embedded camera the OS, drivers and recognition software are still under development.

Movation had the focus on bringing SHIELD-based methodology to the market. Movation used its network to establish communications with research organisations (FFI, Sintef) with companies (ABB, Witelcom, Telenor) and interest organisations (Business network: Internet-of-things, IFEA, Norwegian Oil and Gas). Goal of the talks is to pave the way for SHIELD-empowered applications in the various segments. In short, most of the actors see SHIELD as "too ambitious".

Due to the changes of partners a reconsideration of the "Social Mobility" scenario took place, resulting in the invitation to Seek and Find (SknFnd) to join the consortium. Together with SknFnd we worked on integration of the embedded SIM platform on vehicles, and looked for harmonisation with the SHIELD approach.

Seek and Find joined nSHIELD in August 2013, bringing the expertise of an embedded SIM as core of a sensor system into the project. The SIM-module enables communication, but even more the capability of security updates ("composability") on the sensor platform in a *secured* way. Though task T7.4 is foreseen as a feasibility study, we expect to enlarge it with a real demonstration covering parts of the SHIELD architecture.

SES as leader of the Dependable Avionic Scenario has coordinated the activities finalized to defined and design the preliminary structure of an innovative Avionic Dependable Architecture according to the nSHIELD framework. SES The main effort was given to include Dependability and Composability concept in the demonstrator, under the context of the OMNIA platform architecture. SES, with the support of the partners involved on the Task, has prepared the D7.3. This deliverable incudes the requested preliminary integration and validation plan together with a technology overview of each component involved on the Avionic Demonstrator. The prototypes involved on the Avionic Scenario and included in the complete set of prototypes provided by nSHIELD partners, have been selected. A Preliminary Interface Control Document is prepared and included in D7.3. Support has been provided to SESM in order to finalize the nS-ESD-GW customization needed to foster the communications between legacy power Node and SHIELD components.

SESM is actively participating on the WP7, giving its contribution on the project definition and on the scenario definition as well. The main effort was given to the coordination and to the scheduling of activities regarding the task T7.3. Moreover, SESM has prepared and distributed a preliminary interface control document in order to foster the integration process of components involved into the avionic scenario. The customization of the nS-ESD-GW has been started to adapt the Gateway developed by SESM to the Integrated modular avionics (IMA) architecture provided by SES.

In particular the following pivotal tasks project organization, cooperative tools, components integration, and SW/HW component consolidation have been tackled. Project organization: the project schedule along with the roles and responsibilities have been defined and agreed among partners. Cooperative tools: best practise and cooperative tools have been identified and agreed among partners, in particular to facilitate the exchange of document we are using a cloud storage service. Components Integration: Interface Control Document (ICD) has been prepared and shared among the partners to firmly define the interface of each components involved into the scenario. Consolidation of the Software and Hardware component to employ into nS-ESD-GW; in particular, have been identified modules that will be integrated as they are coming from the WP3 prototype and modules that will require some changes according to the scenario needs.

SLAB prepared a preliminary validation and verification plan for the Railway Security system, and described the IDS prototype validation and verification. This methodology could be adaptable for the other 3 scenarios also (continuous work ongoing). As the work included adaptability for the three other

scenarios, the workforce needed to be extended by almost 6 PM.

The activities of this WP have been starting during this reporting time. **AT** collaborates in one of the four scenarios proposed to validate the nSHIELD prototypes, in task 7.1.

AT +TELC + SICS prototype has been included in the Railways security demonstrator as an Offline Access Control**.** First results have been included in deliverable *D7.1 Railways security demonstrator – integration and validation plan*

THYIA followed the project, no active participation

3	*If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning*
	The change of partners in Slovenia and Norway caused us to reconsider the contributions to the use-cases. Through Alfatroll (NO) the focus on UAV was enhanced. The project has searched for partners being able to enhance the «Social Mobility» use case, and discussed the possibility of participation based on the research vision of the envisaged partner. A final selection was performed, having the focus on «Social Mobility». As a result Movation reduced the participation in the project to give room for the technology provider Seek and Find.
4	*If applicable, explain the reasons for failing to achieve critical objectives and/or not being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)*
	Though three out of four use cases are on track, the fourth use case on "social mobility" is hampered by the withdrawal of partners in Norway and the reduction of man months in Slovenia.
5	*a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

WP7 Involvement and effort Y2 (MM)

Partner	MM	T7.1		T7.2		T7.3		T7.4	
		Plan.	Eff.	Plan.	Eff.	Plan.	Eff.	Plan.	Eff.
MAS	8	5	0			0	0,5	3	1,5
ASTS	21	18,87	18,87						
AT	2	0,6	0,6						
TECNALIA	8	0	**1**	2	1,2			2	1
ALFA	13					0	4		
ETH	18			6	6				
HAI	23	3	5			1	0,5	3	3
THYIA	3							0,5	0,5
SknFnd	1							1	0
S-LAB*	24	4,5	2			4	0,53		
SESM	16					8	8		
TUC	9			1,2	1,2			1,2	1,2
UNIGE	5					1	1		
SES	40					13	3,7		

* Due to applicability work for the other scenarios

6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research*

	Programmes)
	The use cases are further developed to enlarge the visibility of the topic «measurable security»
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*
	Our goal is to demonstrate the applicability of the SHIELD approach through developing SHIELD-based applications. Market impact is a major focus in nSHIELD, including targeted dissemination, and addressing networks for collaboration in the domain. nSHIELD partners have partly established these networks, and are in collaboration with selected players in the market. Alfatroll will fulfil its role in the project, and will be able to demonstrate a dependable avionics system, envisaged through the agreed scenario. It is the hope of the company that more participants in the nSHIELD project considers evaluating Alfatroll's technology for their other avionics systems. Alfatroll intends to demonstrate how even extremely advanced systems can be implemented with simple and efficient on-board avionics systems, given that Alfatroll's Knowledge Based System is used. ETH expects that the facial recognition system will be ready for a prototypical demonstration is going to be demonstrated as a SHIELD application in year 3.

Table 6: WP7 Management Report

3.7 WP8

WP 8- Leader MGEP	
Period: 1 September 2012- 31 August 2013	
1	*A summary progress towards objectives, supported by measurable indicators and details for each task and each partner* The objectives of WP8 are: 1. Industrial Dissemination 2. Industrial Standardization of innovative solutions; 3. Industrial Exploitation of results. 1. - Dissemination This task aims at disseminating the project results and at influencing new standards. A dissemination plan has been internally delivered in the previous period (D8.2). Dissemination activities will consist in the publication of all important results in well-known conferences and journals as well as organization of special sessions in conferences and workshop (listed in section 7 of this document and in the project's website http://www.newshield.eu/dissemination-activities/). 2. - Standardization The standardization task is a key component to increase the impact in the SPD sector. Close interaction with standardization groups to monitor ongoing activities and the preparation of documents and proposals for standardization groups are planned. A standardization plan was internally delivered (D8.3). 3. - Exploitation The target of this task is to promote and facilitate the exploitation of the achieved results. The partners, and, in particular, the large industrial companies will elaborate business plans to evaluate and explore the impact of the results on their business scenarios. During this period, deliverable D8.5 Preliminary Exploitation Plan has been released. **Movation (MAS)** concentrated in this period on the business challenges in bringing measurable security to the industrial community. Movation used its network to establish communications with research organisations (FFI, Sintef) with companies (ABB, Witelcom, Telenor) and interest organisations (Business network: Internet-of-things, IFEA, Norwegian Oil and Gas). Goal of the talks is to pave the way for SHIELD-empowered applications in the various segments. Though "security" as such is both seen as a necessity to be able to deploy wireless sensors in an industrial environment, the way on how to achieve "security" is not clear. Typical challenges being addressed are "retrofitting of security" and "design for a long time horizon". The SHIELD approach is seen as being highly ambitious, though necessary for the future of the wireless industry. Recent discussions with the oil and gas industry indicates that the SHIELD approach will be taken up the the Security working group of the ISO 15926 "Global Integration Project" for the Norwegian shelf. See more at: http://nshield.unik.no/wiki/NSHIELD_Dissemination **Alfatroll** co-organised the Nordic UAV conference in Oslo, collecting the main European players

	and representatives from the USA. The need for certification of software and co-operation in a joined air space are the major challenges. Alfatroll expects that their IQEngine can contribute to a sustainable way of certification of UAV software, and is in discussion with certification organisations on that topic. However, details of the process are delayed until a suitable prototype of the IQEngine is in place. **ASTS** has contributed to Planning of dissemination activities and standardisation strategies and Publication (see dissemination activities) **AT**: During this period of time the nSHIELD project has been included in the company profile presentations. The nSHIELD project has been shown in several customer presentations and public conferences where ACORDE has participated. Finally, the exploitation plan of the company in the scope of the project has been updated, with a contribution to deliverable D8.5: Preliminary Exploitation Plan. **SES** has contributed on providing information for the nSHIELD website. Minor coordination activities. The exploitation plan of the company in the scope of the project has been updated, with a contribution to deliverable D8.5: Preliminary Exploitation Plan. **TECNALIA** Dissemination activities carried out in cross European projects (nSHIELD presentation in RISC project kick off (DG_HOME)) and developing paper in SPD metric area. Tecnalia is now member of M490-SGIS ETSI/CENELEC security group and aims to incorporate nSHIELD results as inputs for industrial cybersecurity standards **ETH** during the reporting period, dissemination activities have been focused on internal dissemination, both at company level and at group level. During the second semester, ETH started planning the exploitation of project results from an industrial point of view. The prototype of the embedded camera for people identification is the candidate for a future engineering revision that will produce a new smart security camera with SPD intrinsic functionalities. ETH plans to include this new product in its portfolio, in order to enrich the commercial offer in the security market. **HAI** activities has been focused on disseminating nSHIELD results through all available channels. Additionally, HAI contributed to forming and describing the verification and testing plan for the first version of nSHIELD operational manual. **ISL**: ISL has been involved in Deliverable D.8.5 Preliminary exploitation plan. Regarding the dissemination and exploitation plan Indra has been working on: • Preparing and releasing a press release, which was published in many relevant newspapers, media agencies, and technology web portals. Moreover, Indra uploaded all the mentions of nSHIELd project derived from the press release in the wiki and webpage of nSHIELD project. • Promoting nSHIELD project to the frontpage of the “Boletín Global de Noticias”. A company magazine available internal and externally. • Contact teams of the company involved in interesting projects such as Atenea (http://www.indracompany.com/en/noticia/indra-designs-an-urban-platform-for-smart-city-government) in order to exploit the developments of the nSHIELD in other projects. **MGEP**: During this period year, MGEP, as leader of WP8 has managed nShield project public website http://www.newshield.eu. The elaboration of deliverables D8.4 and D8.6 has also been coordinated by MGEP. It must be mentioned that the delivery of these documents suffered considerable delay. MGEP organised and chaired Embedded System Security Sessions also promoted nSHIELD internally in Mondragon University.

	SknFnd has joined SHIELD in August 2013, and concentrated so far on the implementation work. Dissemination/Exploitation will come at a later stage. **SLAB** contributed to Task 8.1 with content sections in D8.2 dissemination plan. S-LAB also planned dissemination activities related to internal project meeting organized by S-LAB in Budapest, 10-11.09.2012. **THYIA** No activities in this period **TUC** Has published one paper in conference proceedings (PCI 2012) and another three have been accepted for inclusion in conference proceedings (MobiWac 2013, SETOP 2013, Wireless Days 2013). Four more papers have been submitted to the IEEE International Conference on Communications (ICC 2014) and one paper has been submitted for journal publication (ACM TECS).
2	*Highlight clearly significant and tangible results* During this period the following **dissemination** activities have been carried out: • PhD and Master thesis: 0 • Book chapters: 1 • Journal papers: 2 • Conference proceedings: 13 • Workshops, Exhibitions & Presentations: 4 • Industrial Dissemination: 1 • Organization of special sessions: 1 • In the press: 32 For detailed information, please see section 7 of this document or go to http://www.newshield.eu/dissemination-activities/ Regarding **exploitation**, during this period, deliverable D8.5 Preliminary Exploitation Plan has been released. Finally, some activities towards **industrial standardization of innovative solutions** have been carried out. Please see section 7 of this document for details.
3	*If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning* The major deviation is related to the deliverable D8.4: "SHIELD run-through" (previously known as D8.4: "Operational Manual v1"). o This deliverable has caused considerable controversy within the consortium as it is considered a key deliverable for dissemination but also for a common understanding of the project and objectives. It is planned to be a short and direct document aiming non-technical audience where the necessity of security in embedded systems must be clear and also how adopting the SHIELD approach can help designing SPD compliant embedded systems. o Due to this internal discussion, the deliverable has been delayed but this had no impact in other tasks. To solve this issue a general agreement is needed and a Task Force team has been created to manage it. Although first Task Force meetings were inconclusive a final decision was made during the plenary meeting in Barcelona (March 2013) concluding with the structure of the deliverable
4	*If applicable, explain the reasons for failing to achieve critical objectives and/or not*

	being on schedule and explain the impact on other tasks as well as on available resources and planning (the explanations should be coherent with the declaration by the project coordinator)
	Not applicable
5	*a statement on the use of resources, in particular highlighting and explaining deviations between actual and planned person-months per work package and per beneficiary in Annex 1 (Description of Work)*

WP8 Involvement and effort 2nd year (MM)

Partner	MM (whole project)	T8.1		T8.2		T8.3	
		Plan.	Eff.	Plan.	Eff.	Plan.	Eff.
Movation	3	2	2	0	0,5	0	0
ASTS	6	0.5	0.5	0	0	0	0
AT	4	0,7	0,6	0,68	0,5		
TECNALIA	8	1,9	1,9				
ETH	1	0,3	0,3	0	0	0,4	0,4
Alfatroll	0	0	0	0	0	0	0
HAI	6	1	1			2	2
THYIA	2	0,5	0	0,5	0	0	0
ISL	14	2	2	3.1	3.1	0.7	0.7
MGEP	11	3	3	0	0	0	0
SknFnd	1	0	0	0	0	0	0
SLAB	5	0	0	0	0	0	0
TUC	5	1.9	1.9	0	0	0	0
SES	13	1,2	0.7	1,2	0.7	0	0

6	*a statement on the information flow between the Project and other related Project(s) part-financed under the ARTEMIS JU, the Community Frame Work Programme, and/or National Research Programmes)*
	ISL has contacted teams of the company involved in interesting projects such as Atenea (http://www.indracompany.com/en/noticia/indra-designs-an-urban-platform-for-smart-city-government) in order to exploit the developments of the nSHIELD in other projects.
7	*a statement on the dissemination activities and exploitation perspectives including an updated positioning with respect to the competitive situation in the field addressed by the Project and to other Projects (inside and outside ARTEMIS JU)*
	1. Industrial Dissemination Book Chapters: Title of chapter: Security in Cognitive Radio Networks Book: Evolution of Cognitive Networks and Self-Adaptive Communication Systems Author(s): Krešimir Dabcevic (University of Genova, Italy), Lucio Marcenaro (University of Genova, Italy)

and Carlo S. Regazzoni (University of Genova, Italy)
Year of publication: 2013
Editor: IGI Globa

Journal Papers:

Embedded Systems Security: A Survey of Research Efforts in the EU
Manifavas, C.; Fysarakis, K.; Papanikolaou, A.; Papaefstathiou, I.
ACM Transactions on Embedded Computing Systems (TECS)
Submitted.
The New SHIELD Architectural Framework
M. Esposito, F. Flammini, A. Fiaschetti. In: ERCIM News No. 93, April'13, Special Issue on Mobile Computing: pp. 53 (ERCIM EEIG, Sophia Antipolis Cedex, France, ISSN: 0926-4981)

Conference Proceedings:

Policy-based Access Control for Body Sensor Nodes
Manifavas, C.; Rantos, K.; Fysarakis, K.; Papaefstathiou, I.
IEEE International Conference on Communications (ICC), Sydney, Australia, 10-14 June 2014. Submitted.

CasperCommunity: A Lightweight Anonymity & Location Privacy Service
Fysarakis, K.; Adamopoulos, A.; Manifavas, C.; Papaefstathiou, I.
IEEE International Conference on Communications (ICC), Sydney, Australia, 10-14 June 2014. Submitted.

Integrated Hardware Implementation of PRESENT and SPONGENT
Hatzivasilis, G.; Floros, G.; Manifavas, C.; Papaefstathiou, I.
IEEE International Conference on Communications (ICC 2014), Communications and Information Systems Security Symposium (CISS), Sydney Australia, 10-14 June 2014. Submitted.

ModConTR: A modular and configurable trust and reputation-based system for secure routing in ad hoc networks
Hatzivasilis, G.; Papaefstathiou, I.; Manifavas, C.
IEEE International Conference on Communications (ICC 2014), Ad Hoc and Sensor Networking Symposium (AHSNS), Sydney Australia, 10-14 June 2014. Submitted.

nSHIELD-Gateway: A hybrid FPGA-Microprocessor based architecture to foster the interconnection of embedded systems
Antonio Di Marzo, Michele Paragliola and Marco Aiello
4th international conference on pervasive and embedded computing and communication systems, PECCS 2014, Lisbon, Portugal, 7-9 January, 2014
Submitted

Machine Assisted Proof of ARMv7 Instruction Level Isolation Properties
Khakpour N., O. Schwarz O. and Dam M.,
3rd International Conference on Certified Programs and Proofs, Melbourne, Australia, December, 2013.
Accepted for publication.

Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel
Dam M., Guanciale R., N. Khakpour, Nemati H., Schwarz O.,
20th ACM Conference on Computer and Communications Security, Berlin, Germany, November, 2013.
Accepted for publication.

IPsec over IEEE 802.15.4 for Low Power and Lossy Networks
Rantos, K.; Papanikolaou, A.; Manifavas, C.
ACM 11th Int. Symposium on Mobility Management and Wireless Access (MOBIWAC 2013), Barcelona,

	Spain, 3-8 Nov. 2013. Accepted for publication. IPv6 Security for Low Power and Lossy Networks Rantos, K.; Papanikolaou, A.; Manifavas, C.; Papaefstathiou, I. IEEE/IFIP Wireless Days 2013, Valencia, Spain, 13-15 Nov. 2013. Accepted for publication. Analysis of Energy Detector in Cooperative Relay Networks for Cognitive Radios Muhammad Ozair Mughal, Adeel Razi, Sk. Shariful Alam, Lucio Marcenaro, Carlo Regazzoni 7th International Conference on Next Generation Mobile Apps, Services and Technologies, NGMAST 2013 September 2013 Accepted for publication Secure RPC in embedded systems – Evaluation of some GlobalPlatform implementation alternatives Vahidi A., Jämthagen C. 8th Workshop on Embedded Systems Security, Montreal, Canada, September, 2013. Accepted for publication. Lightweight Cryptography for Embedded Systems – A Comparative Analysis Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Rantos, K. 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), Egham, U.K., 12-13 Sep. 2013. Accepted for publication. Lightweight Cryptography for Embedded Systems – A Comparative Analysis Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Rantos, K. 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), Egham, U.K., 12-13 Sep. 2013. Accepted for publication. Building Trust in Ad hoc Distributed Resource-sharing Networks Using Reputation-based Systems Hatzivasilis, G.; Manifavas, C. In 16th Panhellenic Conference on Informatics with international participation (PCI 2012), University of Piraeus, Greece, 5-7 October, 2012. Digital Object Identifier: 10.1109/PCi.2012.28 Publication Year: 2012, Page(s): 416 – 421 <u>Industrial dissemination:</u> 2013.04.11 Sics Security Seminar 2013: Future Trustworthy It Systems. For the third consecutive year, SICS arranges a seminar on future IT Security. This time the event will take place in Lund, where SICS has opened a new lab, led by Associate Professor Christian Gehrmann. <u>Workshops, Exhibitions & Presentations:</u> 2013.09.05-06 Workshop ISO 15926 and Semantic Technologies 2013 Josef Noll, Zahid Iqbal, Martin Folkestad, “Attribute based access to industrial life-cycle data, the semantic dimension“, Workshop ISO 15926 and Semantic Technologies 2013, 5.-6. September 2013, Sogndal, Norway 2013.05.29-30 Semantic Days 2013 J. Noll, “Measurable Security for the Internet of Things“, Semantic Days 2013, 29-30. May 2013, Stavanger 2013.05.21-23 7th Strategic Workshop

J. Noll, Measurable Security for the Internet of Things, 7. Strategic Workshop, 21.-23.May 2013, Marbella, Spain

2013.04.24-25 FFI Seminar on Advances in ICT
Measurable Security – a discussion of potential approaches, Josef Noll at FFI Seminar on Advances in ICT, 24.-25.Apr. 2013, Jeløya

Workshops, Exhibitions & Presentations:

2013.09.05-06 Workshop ISO 15926 and Semantic Technologies 2013
Josef Noll, Zahid Iqbal, Martin Folkestad, "Attribute based access to industrial life-cycle data, the semantic dimension", Workshop ISO 15926 and Semantic Technologies 2013, 5.-6. September 2013, Sogndal, Norway

2013.05.29-30 Semantic Days 2013
J. Noll, "Measurable Security for the Internet of Things", Semantic Days 2013, 29-30. May 2013, Stavanger

2013.05.21-23 7th Strategic Workshop
J. Noll, Measurable Security for the Internet of Things, 7. Strategic Workshop, 21.-23.May 2013, Marbella, Spain

2013.04.24-25 FFI Seminar on Advances in ICT
Measurable Security – a discussion of potential approaches, Josef Noll at FFI Seminar on Advances in ICT, 24.-25.Apr. 2013, Jeløya

Organization Of Special Sessions:
International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014)
Organization and chairing of the Special session on Measurable security for Embedded Computing and Communication Systems – MeSeCCS 2014, 7 – 9 January, 2014 – Lisbon, Portugal.

In The Press:

Partners also promoted nSHIELD activities and results in press releases, both electronic and paper versions. To see those, please refer to the nSHIELD website: http://www.newshield.eu/in-the-press/

2. Industrial standardization of innovative solutions

Activities related to standardisation:

Standards Norway is a founding member of the Internet of Things Value Network (http://internet-of-things.no), and within Norway partners of nSHIELD discuss on the focus in standardisation in CEN, CENELEC and ETSI.

NORSIS (http://www.norsis.no) is the Norwegian Center for Information Security, and covers all aspects of information security, both on the corporate and the national level. On 16 Oct 2012 Josef Noll and Tone Hoddø Bakås (NOR) had a meeting discussing activities on measurable security. As of today, these topics are not that emphasised in NORSIS, and thus we agreed to focus on awareness.
SKOS Simple Knowledge Organization System: SKOS is an area of work developing specifications and standards to support the use of knowledge organization systems (KOS) such as thesauri, classification schemes, subject heading lists and taxonomies within the framework of the Semantic Web.

- Foreseen for standardisation of security ontologies
- Web link at w3.org .

	SO 15926 for Norwegian Oil and Gas - Standardisation in Oil and Gas for the Norwegian Shelf. EPIM, the Exploration and production information management association, has the focus on IT solutions to promote the best possible flow of information between authorities and licensees on the Norwegian continental shelf. The EPIM Information Management Association has established a project activity named ILAP, Integrated Lifecycle Assets Planning. This new ILAP standard bases on the Generic Information Modeling (GIM) standard (ISO 15926), and is extended into various aspects of oil and gas operations. The two standards being mostly related to the SHIELD security work are ISO 27000+ on Information Security Management and ISO 31000+ on Risk management. The first exchange of knowledge between SHIELD and ILAP has taken place, focussing on the identification of applicability.
8	*If applicable, propose corrective actions*
	Not applicable

Table 7 WP8 Management Report

4 Project Beneficiary (Grouped by Country)

4.1 Italy

The activities done by Selex Elsag and Selex Galileo before their merge have been considered completed. Selex ES, the merging company,

4.1.1 Ansaldo

Beneficiary[5]:	ASTS		
Work Package(s)	WP 1- **Project Management** WP 2- **SPD metrics, requirements and system design** WP 6- **Platform integration, validation and demonstration** WP 7- **SPD Applications** WP 8 - **Knowledge exchange and industrial validation**		
Task(s)	Task 1.1 Project management Task 2.1 Multi-technology requirements & specification Task 2.2 Multi-technology SPD metrics Task 6.1 Multi-Technology System Integration Task 6.2 Multi-Technology Validation & Verification Task 7.1 Railways security Task 8.1 Dissemination		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1 Task 2.1 Task 2.2 Task 6.1 Task 6.2 Task 7.1 Task 8.1	0.5 PM 1 PM 2.82 PM 2 PM 1.54 PM 10.87 PM 0.5 PM	0.5 PM 1 PM 2.82 PM 2 PM 1.54 PM 10.87 PM 0.5 PM	100% 100% 100% 100% 100% 100% 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP: Task 1.1 Project management: ➢ Report of progress and resource expenditure; Task 2.1 Multi-technology requirements & specification: ➢ Definition of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration. ➢ Drafting of the section in charge of ASTS. ➢ Contribution to the definition of SPD requirements and specification , in particular focusing on the dependability and security Task 2.2 Multi-technology SPD metrics: ➢ Identification and definition of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration.			

[5] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

- Drafting of the section in charge of ASTS.
- Study focused on dependability and security metrics for Railway Scenario.
- Application of method to calculate the SPD level with the different techniques

Task 6.1 Multi-Technology System Integration:

- Definition of prototype to be integrated in the railway scenario
- Drafting of the section in charge of ASTS.
- Revision of the document

Task 6.2 Multi-Technology Validation & Verification:

- Analysis of the document

Task 7.1 Railway Security

- Definition and analysis of a Reference architecture for the scenario demonstration
- Preliminary Analysis of threat scenarios and related risk analysis
- Definition of application scenarios
- Definition of SHIELD prototypes to be integrated in the architecture of railway
- Preliminary analysis of Validation and Verification process for the scenario

Task 8.1 Dissemination:

- Planning of dissemination activities and standardisation strategies
- Drafting of the section in charge of ASTS.
- Publication (see dissemination activities)

Description of criticalities met during the period:

- NTR

Corrective actions:

- NTR

Meetings performed during the period:

- Pre-review meeting in Budapest September 11-12 2012
- Review meeting in Rome October 17-18 2012
- Phone Call on WP 6, February 14 2013
- Project Meeting Stockholm, June 12-13 2013
- Phone Call on Document Status, June 27 2013
- Phone Call on WP 2, July 10 2013
- Phone Call on deliverable demonstrator, July 12 2013

Deviations between actual and planned person-months:

- During the first semester, the resources have been redistributed in different manner from to the Annex. Some activities regarding WP2 and WP7 have been anticipated in order to favor the company internal research plan and to increase the added value of the research performed. In particular regarding to the WP7, it's been possible to do a preliminary analysis of ASTS case study, in order to align it with the activities proposed in the previous WPs. The deviation in PM will not influence the budget and next activities to complete.

Dissemination activities and exploitation perspectives:

Publication on ERCIM magazine

- M. Esposito, F. Flammini, A. Fiaschetti: "The New SHIELD Architectural Framework ". In: ERCIM News No. 93, April'13, Special Issue on Mobile Computing: pp. 53 (ERCIM EEIG, Sophia Antipolis Cedex, France, ISSN: 0926-4981)

4.1.2 ETH I.P.S Sistemi Programmabili - Eurotech Security

Beneficiary[6]:	ETH		
Work Package(s)	WP1 – Project Management WP3 – SPD Node WP7 – SPD Applications WP8 – Knowledge exchange and industrial validation		
Task(s)	Task 1.1 Project management Task 3.2 Micro/Personal node Task 7.2 Voice/Facial recognition Task 8.1 Dissemination Task 8.3 Exploitation		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	0,4 PM	0,4 PM	70%
Task 3.2	6 PM	6 PM	96%
Task 7.2	6 PM	6 PM	33%
Task 8.1	0,3 PM	0,3 PM	80%
Task 8.3	0,4 PM	0,4 PM	80%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

During the second year the activities have been performed in the following tasks:

- Task 1.1
  - Management activities required by the project: financial and technical planning, management of research activities, review meeting preparation.
- Task 3.2
  - The analysis of the "Face and Voice recognition scenario" has been finalized and the architecture of the scenario has been defined.
  - Study of new face recognition algorithms suitable for embedded systems. Finalization of the architecture of the face recognition software. Implementation of the first set of tests for the recognition software that represents a proof of concept for the selected approach and constitutes the starting point for the implementation of the related prototype (planned to start in the next semester).
  - Study of new voice verification algorithms for low resources embedded systems. Finalization of the architecture of the voice verification software. Implementation of the first set of tests for the voice verification software that represents a proof of concept for the selected approach and constitutes the starting point for the implementation of the related prototype (planned to start in the first semester of the third year of the project).
  - Design of the architecture of the SPD application that will provide the functionalities of face recognition and voice verification.
  - Preliminary identification of the embedded hardware that will be adopted in the "Face and Voice recognition scenario".
  - Contribution to D3.2 and D3.3.
  - Design and implementation of the prototype of the face recognition system that has been conceived specifically to illustrate the functionalities of the SPD recognition process during demonstrations. This prototype is used also for development and test purposes.

[6] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

- Design of the prototype of the embedded camera that will provide the recognition functionalities in a real environment (i.e. the stadium scenario).

- Task 7.2
  - ETH is responsible for the "Face and voice recognition scenario". During the reporting period ETH has been involved in the definition of this scenario and of the related uses cases. In this context, ETH coordinated the plan of the integration, validation and testing activities. It is responsible for deliverable D7.2 "Voice/Facial Recognition demonstrator - integration and validation plan". During the reporting period ETH focused on the implementation of the prototype for face recognition and on the implementation of the hardware of the final embedded camera. The prototype that will be used for demonstrations is currently available, while for the embedded camera the OS, drivers and recognition software are still under development.
  - A new scenario for face recognition technologies has been identified: people identification for security purposes at the stadium. This scenario has been inspired by customer requests and therefore has an important value from the market point of view. For this reason, the activities related to voice recognition have been momentarily postponed, in order to give more space to the design and development of this scenario.
- Task 8.1
  - Participation to conferences and events on security.
  - Contribution to publication related to security.
  - During the second semester, dissemination activities have been focused on internal dissemination, both at company level and at group level.
- Task 8.3
  - During the second semester, ETH started planning the exploitation of project results from an industrial point of view. The prototype of the embedded camera for people identification is the candidate for a future engineering revision that will produce a new smart security camera with SPD intrinsic functionalities. ETH plans to include this new product in its portfolio, in order to enrich the commercial offer in the security market.

Description of criticalities met during the period:

- No deviations from planned activities during reporting the period.

Corrective actions:

- N.A.

Meetings performed during the period:

- nSHIELD pre-review meeting in Rome, October 17, 2012.
- nSHIELD review meeting in Rome, October 18, 2012.
- Phone calls on project management, task force, WP2, WP3, WP6 and WP7.
- nSHIELD project meeting in Barcelona, March 5-7, 2013.
- nSHIELD project meeting in Stockholm, June 11-13, 2013.

Deviations between actual and planned person-months:

- There are no deviations between actual and planned efforts in the active tasks during the period.

Dissemination activities and exploitation perspectives:

- Participation to ViS ("Vivere in sicurezza") conference, 12/11/2012, Udine, Italy.
- Contribution to the book "Misure di sicurezza", Bancaria Editrice, 2012.
- Participation to the conference "Banche e sicurezza 2012", ogarinzed by OSSIF and ABI.

4.1.3 SESM scarl SESM

Beneficiary[7]:	SESM		
Work Package(s)	WP3 -SPD Node WP7 - Application		
Task(s)	Task 3.3 Power Node Task 7.3 Dependable Avionic		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.3 Task 7.3	8 PM (out of total 15) 8 PM (out of total 16)	8 PM 8 PM	100% 100%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

Task3.2

During this period all the technologies (SW,HW, Tool) necessary to support the development of the nS-ESD-GW have been firmly defined and acquired. A subset of node architectures have been assessed and consequently a node architecture has been selected to be developed. Thus, the development process based on the WP2 requirements has been triggered, and several nS-ESD-GW sub module have been developed such as the Coordination Module, Encryption Module and Data Integrity module. Currently the development process is completed at 80%, and there are two modules left to be developed. We envision to deploy in the next year, a new release of the nS-ESD-GW, that custom version will be specifically tailored to the avionic scenario. At same time activities of test and verification will be performed on the nS-ESD-GW.

Task7.3

Several steps towards the definition of the avionic scenario and towards the integration of the ns-ESD-GW into it have been performed. In particular during this period the following aspects have been tackled:

- 7.3 Schedule, roles and responsibilities have been constituted and agree among partners;
- 7.3 best practise and cooperative tools have been identified and agreed among partners;
- Process of nS-ESD-GW integration with other components;
- Definition and consolidation of the nS-ESD-GW interface;
- Consolidation of the Software and Hardware component to employ into nS-ESD-GW;
- A process to adapt the generic scheme of the nS-ESD-GW to the scenario has been triggered.

Description of criticalities met during the period:

We had some difficulties to start up the task 7.3, mainly due to the complexity of the project itself, and, due to the partners different perception of the scenario.

Corrective actions:

No any corrective actions have been performed.

Meetings performed during the period:

- Face to Face meeting Barcelona 6 -7 March 2013

[7] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

- WebEx 3 April 2013 (SES, SESM, UNIGE,SLAB)
- WebEx 11 April 2013 (SES, SESM, ALFATROL, UNIGE,SLAB)
- Face to Face meeting STOCKHOLM 12-13 June 2013
- WebEx 24 June 2013
- WebEx 27 June 2013
- WebEx 12 July 2013
- WebEx 23 July 2013
- Internal Meeting Rome WP7.3 16 January 2013 (SES,SESM)
- Internal Meeting Rome WP7.3 2 March 2013 (SES,SESM)
- Internal Meeting Rome WP7.3 22-23 April 2013 (SES,SESM, UNIROMA,UNIGE)

Deviations between actual and planned person-months:

- …

Dissemination activities and exploitation perspectives:

- ….

4.1.4 Università degli Studi di Genova UNIGE

Beneficiary[8]:	UNIGE		
Work Package(s)	WP3 - SPD Node		
Task(s)	Task 3.4 Dependable self-x technologies Task 3.5 Cryptographic technologies		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.4 Task 3.5	6.5 PM 7 PM	6.5 PM 7 PM	75% 80 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Task 3.4
  - Consolidation of the node prototype (OMBRA)
    - Satisfying the node scalability
    - Satisfying the four scenarios requirements
    - Satisfying the metrics that outcome in D2.5 deliverable
  - Demo implementation on the prototype:
    - Point multiplication on an elliptic curve (developed in task 3.5)
    - Comparing results with standard PC
- Task 3.5

  Implementation on embedded microprocessors of a public-key authentication algorithm based on Elliptic Curve Cryptography (ECC)
  - Final development of the basic module supporting prime finite field arithmetic
  - Final development of the fundamental functionalities supporting ECC
    - conversion of elliptic curve points from affine representation to projective representation;
    - point addition
    - point doubling
    - point multiplication
  - Implementation of the libraries on embedded microprocessors (ARM)
  - Testing

Description of criticalities met during the period:

- N.A.

Corrective actions:

- **N.A.**

Meetings performed during the period:

- Project Meeting: September, 11-12, 2012
  Review Meeting: October, 17-18, 2012
  Project Meeting: March, 6-7, 2013
  Project Meeting: June, 12-13, 2013

Deviations between actual and planned person-months:

- N.A.

Dissemination activities and exploitation perspectives:

- C. Peretti, P. Gastaldo, M. Stramezzi and R. Zunino. "Embedded implementation of Edwards curve- and extended Jacobi quartic curve-based cryptosystems" submitted to the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)

[8] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary[9]:	UNIGE		
Work Package(s)	WP4 - SPD Network WP7 - Applications		
Task(s)	Task 4.1 Smart SPD driven transmission Task 4.2 Distributed self-x models Task 7.3 Dependable Avionic System		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 4.1 Task 4.2 Task 7.3	7 PM 5 PM 1 PM	9 PM 6,5 PM 1 PM	50% 50% 20%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Task 4.1
  - Final goal
    - Design and development of SPD-based transmissions methodologies among nSHIELD node levels
  - Activities and results
    - Finalizing the proprietary C++ based cognitive radio simulator used to demonstrate the effectiveness of the proposed defense schemes related to Cognitive Radio and Software Defined Radio security (3rd semester). Simulation results for the Smart Jamming Attacks and the corresponding anti-jam system were shown (4th semester).
    - A detailed technical proposal of the Smart Transmission Layer (in collaboration with SelexElsag), proposing the means of implementation of the technology (hardware and software components), its enablers and the expected functionality(3rd semester). Assembly of the SPD-driven Smart Transmission Layer (in collaboration with Selex ES), initial results achieved using the completed prototype (4th semester).
- Task 4.2
  - Final goal:
    - Design of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks
  - Completed activities:
    - Self-x has been defined as an inherent concept of the Security-Aware framework, developed within the task T4.1. The proposed Security-Aware framework as the property of the SPD-driven Smart Transmission Layer, incorporates the self-management and self-reconfigurability potentials of the SDR-based and CR-based nodes. Several self-x functionalities are currently in-development within the SPD-driven Smart Transmission Layer, namely self-awareness and self-protection (more details in D4.2 and D4.3)
- Task 7.3
  - Final goal:
    - Applying functionalities-of-interest of SPD-driven Smart Transmission Layer (SPD-enabled communication in harsh and hostile channel conditions) to the Dependable Avionic System Demonstrator
  - Completed activities:
    - Creating the demonstrator's structure. Defining interfaces to other nSHIELD prototypes used in the demonstrator. Programming the software interface for STL for achieving 2-way communication with upper nSHIELD layers (Middleware and Overlay).

Description of criticalities met during the period:

[9] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

- N.A.

Corrective actions:

- **N.A.**

Meetings performed during the period:

- nSHIELD Project meeting Budapest, 11.9.2012.
- nSHIELD 1st annual review meeting Rome, 17.10.2012.-18.10.2012.
- TaskForce Skype meeting (TaskForce establishment), 9.1.2013.
- TaskForce Skype meeting (realizing D8.4; status of THYIA), 23.1.2013.
- TaskForce Skype meeting (Security metrics), 13.2.2013.
- TaskForce Skype meeting (towards the Barcelona project meeting), 27.2.2013.
- nSHIELD Project meeting Barcelona, 6.3.2013.-7.3.2013.
- T7.3 Webex meeting (Avionic Scenario consolidation), 3.4.2013.
- T7.3 Webex meeting (Avionic Scenario WBS structure and initial contributions), 11.4.2013.
- WP4 Skype meeting (periodic group meeting), 13.5.2013.
- WP4 Skype meeting (T4.3 consolidation), 20.5.2013.
- T7.3 Webex meeting (Avionic Scenario interfaces definitions), 4.6.2013.
- nSHIELD Project meeting Stockholm, 12.6.2013.-13.6.2013.
- WP4 Skype meeting (finalizing D4.2 and D4.3), 17.9.2013.

Deviations between actual and planned person-months:

- Additional effort was invested in collaboration with other partners for defining final demonstrators and scenarios and adapting developed algorithms to them;

Dissemination activities and exploitation perspectives:

- Kresimir Dabcevic, Lucio Marcenaro, Carlo S. Regazzoni, “Security in Cognitive Radio Networks” - book chapter for “Evolution of Cognitive Networks and Self-Adaptive Communication Systems”, IGI Global, 2013
- Muhammad Ozair Mughal, Adeel Razi, Sk. Shariful Alam, Lucio Marcenaro, Carlo S. Regazzoni, “Analysis of Energy Detector in Cooperative Relay Networks for Cognitive Radios”, Proceedings of the 7th International Conference on Next Generation Mobile Apps, Services and Technologies, NGMAST 2013

4.1.5 Università degli Studi di Udine UNIUD

Beneficiary[10]:	UNIUD		
Work Package(s)	WP1 – Project Management WP2 – SPD metrics, requirements and system design WP3 – SPD node WP4 – SPD network WP6 – Platform integration, validation and demonstration		
Task(s)	Task 1.1 – Project management Task 1.2 – Liasons Task 2.1 – Multi-technology requirements & specifications Task 2.2 – Multi-technology SPD metrics Task 2.3 – Multi-technology architectural design Task 3.1 – SDR/Cognitive Enabled node Task 3.2 – Micro node Task 3.3 – Power node Task 3.4 – Dependable self-x Technologies Task 3.5 – Cryptographic technologies Task 4.1 – Smart SPD driven transmission Task 4.2 – Distributed self-x models Task 4.3 – Reputation-based resource management technologies Task 4.4 – Trusted and dependable connectivity Task 6.1 – Multi-technology system integration Task 6.2 – Multi-technology validation and verification Task 6.3 – Lifecycle SPD support		
Period:	1st September 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1 Task 3.1 Task 4.2 Task 6.2	0,5 4 6 2	0,5 4 5 3	100% 100% 83% 150%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

Activities within WP1

- The activity within the WP has been the usual management one, concerning meeting participation and report preparation and delivery, conference calls and mail correspondence.
- Task 1.1:

  Preparation of projects documents and coordination meetings; periodic conference calls; e.mail discussions.

[10] This report is p6er Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary 0

Activities within WP3

- The activity in WP3 followed the development as planned. Since the focus of UNIUD in this WP is focused on mobile nodes (nanonodes), we selected a commercial embedded system as a reference architecture, in order to perform preliminary evaluations and to have a development target. We selected an ARM based platform as reference board because the large spreading of such a CPU architecture and of its good power consumption figures. The selected platform is the "Beagleboard" embedded system, powered by the OMAP3530 SoC (built around the ARM Cortex A8 core), and equipped with USB interfaces to further extend its peripheral availability. Moreover, to avoid limiting the exploration to a single case study, we adopted a virtual platform, based on a customized variant of a software emulator ("qemu"), still based on the ARM architecture. Using a virtual platform is also beneficial for it allows a deep inspection of the hw/sw interaction (by analyzing the hardware behavior even in components which do not expose debug features, as JTAG probing and scan access). Furthermore, within the software emulator, also hardware components that are not yet developed can be taken into account, and faults in hardware can be modeled.
- Task 3.1:

  - Porting of a reference operating system on the target platforms: we chose the Linux kernel 3.4.4 as our reference operating system and we ported it on the real target system as well as on the virtual platform.

  - Development of a kernel driver to handle password protected SD memory cards: such a feature is missing on the reference operating system, but it should be considered essential because a node can use an SD card to store data. Since a nanonode is easily reachable by a physical attacker, such a memory must be secured or has to be considered not usable; the password protection, provided by the SD specifications, is a low cost and low overhead mechanism to be used in addiction or in replacement of data encryption.

  - Initial development of user level interface to kernel power management features: the operating system provides access to the ARM specific power management and to the voltage regulators that supply the whole system. However, a user level interface to those features is needed to allow applications to tune their computational requirements and their power consumption. In this task we are developing such an interface, based on virtual filesystem objects and on IOCTL calls.

  - Initial development of an activity profiler as a kernel scheduler augmentation: to select the most effective energy policy, information about the whole system behaviour is needed. Such data, as the number of running tasks and their resource requirements are available at kernel level and, in particular, in the scheduling sub-system. In this task we are augmenting the scheduler in order to expose such information to other kernel sub-systems and to user level applications. In this way the power manager can choose the most appropriate supply levels over time, eventually scheduling system shut down and resume events, that allows meeting the requirements still reducing the energy consumption.

Activities within WP4

- The activity in WP4 also followed the specifications derived at the Project level in WP1. The aim of the WP is to define proper strategies able to implement SPD at the network level as a whole. As a result of the activity performed within WP6 and after a more detailed definition of the scenarios has been obtained, a shift has been performed on the application model. After the development of self-assembling autonomous strategies for the deployment of generic applications in a Cellular-Automata-like infrastructure, it has emerged, given the application scenarios which, in the meantime, had been determined, that instead of relying on a fine-grained cellular automata paradigm, a coarser-grained dataflow paradigm was found more appropriate and has been designed. This resulted in an improved architecture, meant to address all the single-point-of-failure situations that would block the execution of a distributed application. It is also better suited to run a generic software routine and thus can accommodate the needs of all the scenarios, though the Voice/Face Recognition scenario is the specific one chosen for demonstrating the prototype.
- Task 4.2:

- Development and test of the cellular-automata based paradigm simulator.

- Redesign of the architecture and the application metamodel from the theoretical viewpoint, taking into account aspects of dependability (guarantee a reliable execution in presence of faults) and auditing (offer prompt and detailed information regarding the application state).
- Initial software implementation in Java: focus on the dependable deployment and loading of the application model, while the runtime is still a work-in-progress.

Activities within WP6

- The work package focuses on the integration, validation and verification steps of the platform. It is concerned with interoperation between prototypes, with particular attention to the requirements of scenarios. The activity performed in this period has been driven by the need for the WP4 prototype to properly satisfy network requirements from the scenarios, more specifically the Voice/Face Recognition scenario.
- Task 6.2:
  - Study of the preferred software technologies to guarantee dependability at the network level.
  - Identification of the critical SPD requirements involved in the scenario of choice for WP4.

Description of criticalities met during the period:

- The full definition of the scenarios made it apparent that the granularity of application models under the cellular automata paradigm is inadequate, i.e., too fine to apply to routines envisioned within such scenarios.

Corrective actions:

- A redesign has been performed within the planned PM for the project to improve the dependability of the deployment and runtime of applications. Implementation of the prototype within WP4 has started and will be completed within March 2014, followed by final integration efforts within WP6.

Meetings performed during the period:

- NONE

Deviations between actual and planned person-months:

- An amount of 1 PM had to be additionally spent within WP6 to fully study the integration requirements related to the scenarios. As a consequence, a corresponding 1 PM from WP4 had to be held back.

Dissemination activities and exploitation perspectives:

- NONE

4.1.6 Università degli studi di Roma "La Sapienza" UNIROMA1

Beneficiary[11]:		UNIROMA1	
Work Package(s)		WP1[12] - Project Management	
Task(s)		Task 1.1 Project Management	
Period:		1st Sept 2012 – 31th August 2013	
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	1.0	1.4	140% [13]:

Description of the activities carried out during the period to reach specific objectives within the task/WP:

In the second year of the project, UNIROMA1 worked as member of Technical Management Committee as well as member of the Task Force (established after the first year review) to assure that the key players could drive the project towards its objective (by means of dedicated meeting, document review and cross-contribution to D8.4).

In addition, UNIROMA1 strongly supported the coordinator in the preparation and execution of the first and second review meetings and, as Task Leader in WP5, performed additional management activities to set-up and manage WP5 participants.

Description of criticalities met during the period:

No criticality was met.

Corrective actions:

N/A

Meetings performed during the period:

- 14th June, 2013 Task Force Meeting – Stockholm (SICS)
- 12th 13th June, 2013 Consortium Meeting – Stockholm (SICS)
- 6th March, 2013 Task Force Meeting – Barcelona (ISL)
- 5th – 6th March, 2013 Consortium Meeting – Barcelona (ISL)
- 27th February, 2013 – Task Force Phone Call (MGEP)
- 13th February, 2013 – Task Force Phone Call (MGEP)
- 3rd February, 2013 – Task Force Phone Call (MGEP)
- 9th January, 2013 – Task Force Phone Call (MGEP)
- 19th December, 2012 – Task Force Phone Call (MGEP)
- 28th November, 2012 – Task Force Phone Call (MGEP)
- 18th October, 2012 – First Review Meeting – Rome (FINMECCANICA)
- 17th October, 2012 – Pre-Review Meeting – Rome (FINMECCANICA)
- 11th -12th September, 2012 – Consortium Meeting – Budapest (S-LAB)

Deviations between actual and planned person-months:

No significant deviation.

Dissemination activities and exploitation perspectives:

N/A

[11] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[12] x is 1, 2, 3, 4, 5, 6, and 7

[13] Z% = (PMs spent)/PMs planned x 100.

Beneficiary[14]:		UNIROMA1	
Work Package(s)		WP5[15] - SPD Middleware and Overlay	
Task(s)		Task 5.1 SPD driven Semantics Task 5.2 Core SPD services Adaptation of legacy systems (ex T5.2+T5.4) Task 5.4 Overlay monitoring and reacting system by security agents (ex T5.5)	
Period:		1st Sept 2012 – 31st August 2013	
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 5.1 Task 5.2 Task 5.4	4.3 PM 6.7 PM 8.7 PM	4.0 PM 6.3 PM 8.1 PM	93% 94% 93%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

Task 5.1 SPD driven Semantics

- Following the guidelines declared in Deliverable 5.1, UNIROMA1 has addressed the definition of the new SHIELD models, in order to meet the new project needs.
- With respect to the identified challenges, and taking into account the inputs from the pSHIELD final review, as well as the nSHIELD first review, additional studies have been carried out to find the adequate models and methodologies that represent the official SHIELD Formal Model.
- The Semantic Model scope has been enlarged to include the whole process of "data management" in the SHIELD framework: together with the semantic component, also a data base management structure is evaluated.
- The methodology identified to build the "knowledge base" used by the SHIELD Middleware to compose SPD functionalities, mainly based on the decoupling between "domain information" and "security information", has been refined and tailored to the middleware architecture (liaison with Task 5.2).
- The candidate set of semantic technologies has been reduced, mainly focusing on semantic representations that allows: i) a technological abstraction of components and ii) the deployment of a connector algebra.
- The first set of models of the SHIELD components have been produced and formalized (in a language close to the demonstrator needs). The key design driver of this first delivery was the correct translation of metrics into the abstract description of the individual SPD component, in strict cooperation with task 2.2. These models, together with the structure of the SHIELD DB for the domain knowledge representation, constitute the UNIROMA1 prototypes.
- Potential liaisons between control algorithms and semantic model have been evaluated, in order to verify the feasibility of a modelling technique that could be immediately translated into a control algorithm. (Coloured) Petri nets were the first candidates.
- Analysis on semantic parsers in Java language, to be integrated in the OSGI platform, have been performed at design level. However, preloaded models are being prepared as first solution for the prosecution of integration phases.
- Preliminary Analysis about the integration between policies representation and semantic representation have been started, bringing to the definition of separate semantics to describe components or policies (in charge to T5.3).
- Significant additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve semantic technologies and their implementation.
- Some additional work has been carried out to support WP7 in the definition of the demonstrator architecture.
- Extensive advanced research has been carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

[14] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[15] x is 1, 2, 3, 4, 5, 6, and 7

Measurable Outcome: The above mentioned results have been presented in Deliverable 5.3 in terms of report of designed solutions and Deliverable 5.2 with respect to the development of prototypes.
Additional inputs have been provided to Deliverable 2.X (requirements refinement), as well as Deliverables D7.1, D7.2, D6.3.

Task 5.2 Core SPD services Adaptation of legacy systems (ex T5.2+T5.4)

- Following the guidelines declared in Deliverable 5.1, UNIROMA1 has designed and developed the first batch of the new SHIELD Middleware Core services, in order to meet the new project needs.
- An architectural refinement has been performed to introduce the new bundles representing the new middleware components (Secure Discovery, Security agent and interfaces with Intrusion Detection Bundle) and the OSGI platform has been adapted to be used in the nSHIELD project (as decided during the first year).
- Intensive studies have been carried out to select the most suitable solution to implement the innovative SHIELD Secure Discovery. The corresponding bundle has been developed in the OSGI framework and represents one of the UNIROMA1 prototypes.
- Extensive analysis has been performed to define the architecture of the SHIELD Security Agent (see also Task 5.4). The corresponding bundles have been developed in the OSGI framework and represent one of the UNIROMA1 prototypes. Control algorithms will be integrated in the second delivery.
- A more technology-focused work has been performed to identify components' interfaces to drive the development effort towards solutions that can be easily integrated into the avionic and railway demonstrator.
- With respect to the demonstrator, additional analyses have been performed to align Middleware with the HW and SW technologies available from other partners (see also Task 6.1 for integration effort)
- Significant effort has been put in place to enable the new partners to seamless integrate with the OSGI heritage from pSHIELD (UNIROMA1 is the owner of the software platform).
- Significant additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve middleware core services.
- Some additional work has been carried out to support WP7 in the definition of the demonstrator architecture.
- Extensive advanced research has been carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Measurable Outcome: The above mentioned results have been presented in Deliverable 5.3 in terms of report of designed solutions and Deliverable 5.2 with respect to the development of prototypes.
Additional inputs have been provided to Deliverable 2.X (requirements and architecture refinement), as well as Deliverables D7.1, D7.2, D6.3.

Task 5.4 Overlay monitoring and reacting system by security agents (ex T5.5)

- Following the guidelines declared in Deliverable 5.1, UNIROMA1 has designed and developed the new SHIELD Overlay and control algorithms, in order to meet the new project needs.
- Extensive investigations have been performed to confirm the theoretical framework for SPD composability, and two candidate technologies have been selected: Petri Nets and Coloured Petri Nets.
- The first formal model for theoretical composability of SPD functionalities has been developed based on Coloured Petri Nets. The control algorithm is "embedded" in the topology of the Petri Net itself.
- Intensive simulations have been performed to validate this model in a significant scenario in line with the SHIELD requirements. These models and simulations represent one of the UNIROMA1 prototype.
- Liaisons between the modelling of SPD functionalities for control purposes, and their semantic representation (Task 5.1) have been maintained and enriched.
- A second approach control based approach has been identified, on the grounds of the new results in metrics definition available at the end of second year. This approach is based on the formulation of the composability problem as an optimization problem, whose solution should drive the deterministic composition of individual functionalities to reduce the vulnerabilities of the "attack surface" (see Task 2.2)
- The architecture of the Security Agent has been translated into code at Middleware level (see also Task 5.2) and the harmonization of the decision making process (metrics vs policies vs control algorithms) has been preserved in this first implementation.
- Some studies on the interaction of several security agents (either at architectural or theoretical framework level) have been performed in order to identify potential solutions to drive architecture and control algorithms refinement. They will be better refined once the demonstrators architectures are frozen.

- Significant additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve overlay.
- Some additional work has been carried out to support WP7 in the definition of the demonstrator architecture.
- Extensive advanced research has been carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Measurable Outcome: The above mentioned results have been presented in Deliverable 5.3 in terms of report of designed solutions and Deliverable 5.2 with respect to the development of prototypes.
Additional inputs have been provided to Deliverable 2.X (requirements, architecture refinement and support to metrics definition), as well as Deliverables D7.1, D7.2, D6.3.

Transversal WP activities and remarks:

- Support to WP5 coordination activities has been provided (in particular, UNIROMA1 is T5.4 leader).
- Maintenance of a repository server to improve WP5 participants awareness and collaborative work.
- The outcomes of the above mentioned activities, performed in the scope of WP5, have been used as inputs by WP2 with respect to requirements and architecture, thus resulting in additional contributions to WP2 deliverables.

Description of criticalities met during the period:

- Since UNIROMA1 was the main contributor and owner of the pSHIELD concepts, on which also the nSHIELD prototypes will be developed, a significant time-consuming effort was needed i) to allow the new partners to integrate their new prototypes into the OSGI software code and ii) to review/align the concepts developed in other WPs (mainly WP2 and WP7). As a consequence, WP5 activities were slightly delayed, but only in terms of deliverable writing.
- In fact, D5.2 and D5.3 have been delivered with some month delays: however the information flow and sharing has not been interrupted (frequent phone calls have been set up), so this delay has not impacted the correct prosecution of activities, but only the material writing and editing of D5.3 and D5.2.

Corrective actions:

- No corrective actions are needed because the delay introduced by the above-mentioned criticality was only "editorial" with a minimum impact on the development phase

Meetings performed during the period:

- 12th 13th June, 2013 Consortium Meeting – Stockholm (SICS)
- 5th – 6th March, 2013 Consortium Meeting – Barcelona (ISL)
- 14th February, 2013 – Proxy of WP5 for WP6 Phone Call (HAI)
- 7th February, 2013 – WP5 Phone Call (SES)
- 16th January, 2013 – WP5 Phone Call (SES)
- 19th December, 2012 – WP5 Phone Call (SES)
- 18th October, 2012 – First Review Meeting – Rome (FINMECCANICA)
- 17th October, 2012 – Pre-Review Meeting – Rome (FINMECCANICA)
- 11th -12th September, 2012 – Consortium Meeting – Budapest (S-LAB)
- Periodic Joint meeting UNIROMA1-SES

Deviations between actual and planned person-months:

No significant deviation.

Dissemination activities and exploitation perspectives:

Most of WP5 results from UNIROMA1 have been carried out (and presented) in the scope of the following Ph.D Thesis: A. Fiaschetti, "Control Algorithms and Architectures for Resource Management in Multi-Layered Systems: Application to SatCom, Security and Manufacturing domains", Ph.D. Defence, March 2013.

Additional notes:

- The agreement of a formal model for the SHIELD framework requires the contribution from the whole consortium and especially from partners involved in demonstration scenarios and metrics. UNIROMA1 is providing a container and a methodology to represent the "consortium knowledge". For this reason the models derived in this phase are to be considered only one of the possible solutions and the ongoing discussions will lead to a more complete solution once the scenarios and the metrics are frozen. This is, however, already foreseen by the project planning, since D.5.2 and D.5.3 are 'preliminary' prototypes and reports.

Beneficiary[16]:		UNIROMA1	
Work Package(s)		WP6[17] - Platform integration, validation & demonstration	
Task(s)		Task 6.1 Multi-Technology System Integration	
Period:		1st Sept 2012 – 31st August 2013	
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
6.1	2 PM	2 PM	100%[18]

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- In the scope of prototype integration activities, UNIROMA1 has supported the definition of the SHIELD common platform architecture as well as the demonstrators' architecture with respect to Middleware and Overlay technologies.
- Once identified the building blocks of the platform, UNIROMA1 has elaborated the validation and verification plan for the Middleware and Overlay technologies previously described.
- In addition, it has started all the activities necessary to integrate the OSGI Middleware and Overlay prototypes into the Avionic and Railways demonstrators, with focused analysis on protocol stacks and software modules necessary to enable components communication.
- A significant effort has been put to support the WP6 leader in the assessment of all the available prototypes and their mapping on the SHIELD architecture, in order to define the demonstrators' shape. This activities have led to the production of the so called "prototype list", that is the basis of the whole WP6 and will drive the prosecution of activities in the last project year.

Measurable Outcome: The above mentioned results have been reported in Deliverable 6.2 with respect to validation and verification and D6.3 with respect to prototypes description.
Additional inputs have been provided to D7.1, D7.2 with respect to the demonstrator architecture.

Description of criticalities met during the period:

No criticality was met.

Corrective actions:

N/A

Meetings performed during the period:

- 12th 13th June, 2013 Consortium Meeting – Stockholm (SICS)

Deviations between actual and planned person-months:

No significant deviation.

Dissemination activities and exploitation perspectives:

N/A

[16] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[17] x is 1, 2, 3, 4, 5, 6, and 7

[18] Z% = (PMs spent)/PMs planned x 100.

4.1.7 Selex ES

This activities report will include the activities done by Selex Galileo and Selex Elsag during the first four months before the merging.

Beneficiary[19]:	SES		
Work Package(s)	WP1 – Project Management WP2 – SPD metrics, requirements and system design WP3 – SPD Node WP4 – SPD Network WP5 – SPD Middleware and Overlay WP6 – Platform integration, validation & demonstration WP7 – SPD Applications WP8 – Knowledge exchange and industrial validation		
Task(s)	Task 1.1 – Project management Task 1.2 - Liaisons Task 2.1 - Multi-technology requirements & specification Task 2.2 - Multi-technology SPD metrics Task 2.3 - Multi-technology architectural design Task 3.1 - SDR/Cognitive Enabled node Task 3.2 - Micro node Task 3.3 - Power node Task 3.4 - Dependable self-x Technologies Task 4.1 - Smart SPD driven transmission Task 4.2 - Distributed self-x models Task 4.3 - Reputation-based resource management technologies Task 4.4 - Trusted and dependable Connectivity Task 5.1 – SPD driven Semantics Task 5.2 – Core SPD services Task 5.3 – Policy-based management Task 5.4 – Adaptation of legacy systems Task 6.1 – Multi-Technology System Integration Task 6.2 – Multi-Technology Validation & Verification Task 6.3 - Lifecycle SPD support: Task 7.1 – Railways security Task 7.3 – Dependable Avionic Systems Task 7.4 – Social Mobility Task 8.1 – Dissemination Task 8.2 – Standardization Task 8.3 - Exploitation		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	18	14,2	64%
Task 1.2	5,75	2,7	50%
Task 2.1	1	0	79%
Task 2.2	3	4,5	96%
Task 2.3	1	3	100% (140% MM)

[19] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Task 3.1	2,1	0,6	51%
Task 3.2	2,1	1,4	63%
Task 3.3	3	1,2	39%
Task 3.4	0,5	0,5	50%
Task 4.1	20	18	69%
Task 4.2	12	13	63%
Task 4.3	1	1	60%
Task 4.4	3	2	55%
Task 5.1	7	6,5	85%
Task 5.2	4	4	67%
Task 5.3	6	6,5	59%
Task 5.4	4	4,5	45%
Task 6.1	7	2	13%
Task 6.2	3	1,1	6%
Task 6.3	2	1,3	43%
Task 7.3	13	3,7	11%
Task 8.1	1,2	0,7	28%
Task 8.2	1,2	0,7	41%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 1.1**
  - Management activities required by the project: financial and technical planning, internal review meeting preparation.
  - Contact with THYIA in order to re-arrange its involvement in the project and to avoid the compromising of the project objectives verification.
  - Several telephone conferences and meeting were held during those two months and several actions were taken in order to facilitate the work between partners.
  - nSHIELD Project meeting Stockholm coordination
  - TA updating.
- **Task 1.2**
  - Leading and preparing the definition of the "Quality Control Guidelines" deliverable.
  - Leading and preparing the report concerning the activities of Quality Control.

Objectives: Defining the quality control guidelines; application of the quality control guidelines to the activities done during the first year of the project.

Results: Preparation of the second issue of D1.2 and the first issue of D1.6.

- **Task 2.1**
  - Definition of SPD requirements for each layer, alignment with the architecture and convergence with different use cases described;
  - Description of requirements in a standardized way to ensure a common understanding and to facilitate later exploration and usage for implementation;
  - Preparation of a rationale for each identified requirement;
  - Final Requirements definition through the mapping between the requirements identified in the definitions phase and those actually achieved by the prototypes identified in Midlleware and Overlay layer definition (WP5)

Objectives: defining the requirement of the nSHIELD framework driven by the use case

Results: Preparation of D2.6 deliverable

- **Task 2.2**
  - Contribution (for the Common Criteria related aspects) to determination of metrics in a quantitative and formal way. The formalisation comes from three points of view:
    - Mathematical approach for measuring each of the metrics identified
    - Formal alignment towards specification and standards (Common Criteria)
    - Compositional approaches identified but not prioritised yet.
  - Identification and quantification of nSHIELD full domain metrics
  - Composition method derivation towards an incremental certification scope and view
  - Identification of a formal model for SPD metrics

- Definition of a metric composition methodology able to produce a single SPD level for a nSHIELD compliant system.
- Definition of specifications data sheet that must be provided with each component that must be used within a system nSHILED compliant.
- Definition of a spreadsheet to determine the SPD level of an nSHIELD compliant system from the data provided by the manufacturers with each components that constitute it (data sheet)

Objectives: defining the SPD metrics of the nSHIELD framework
Results: Preparation of D2.8 deliverable, inputs to Task 5.1 and Task 5.5

- **Task 2.3**
  - Definition of a heterogeneous and distributed reference architecture which aims to link the dissimilar components of nSHIELD System;
  - Contribution to finalization of nSHIELD Reference System Architecture;
  - verification of the conformity of the identified prototypes with the proposed nSHIELD System Architecture

Objectives: defining the nSHIELD framework architecture
Results: inputs to the D2.3 and D2.4 deliverables on overall high level and middleware/overlay architecture

- **Task 3.3**
  - Analysis of requirements to make OMBRA architecture compatible to the maximum extent with the nSHIELD node functionalities.
  - Contribution to D3.3 "Preliminary SPD node technologies prototype report"

Objectives: The main outcome of task 3.3 is prototypes, matching with WP2 requirements, specification and interface design.

- **Task 3.4**
  - Analysis of the node requirements and architectures that include the reprogrammability feature, focusing on the FPGA available on the prototype board.

Objectives: Develop prototypes following the composability criteria of the nSHIELD architecture design delivered by WP2.
Results: inputs to the deliverables D3.2 "Preliminary SPD node technologies prototype" and D3.3 "Preliminary SPD node technologies prototype report"

- **Task 4.1**
  - In-depth technical proposal of the Smart SPD-driven transmission layer

Objectives: establishing the means for the practical implementation and demonstration of the nSHIELD Smart SPD-driven transmission layer architecture
Results: inputs to the D4.2 and D4.3 deliverables "Preliminary SPD network technologies prototype" and ""Preliminary SPD network technologies prototype report"

- **Task 4.2**
  - Analysis of the distributed self-x models
  - Technical assessment on the distributed self-x models

Objectives: defining the nSHIELD distributed self-x models node architecture
Results: inputs to the D4.1 deliverable "Technical Assessment"

- **Task 4.3**
  - Analysis of the distributed self-x models
  - Technical assessment on the distributed self-x models

Objectives: defining the nSHIELD distributed self-x models node architecture
Results: inputs to the D4.1 deliverable "Technical Assessment"

- **Task 4.4**
  - Analysis of the distributed self-x models
  - Technical assessment on the distributed self-x models

Objectives: defining the nSHIELD distributed self-x models node architecture
Results: inputs to the D4.1 deliverable "Technical Assessment"

- **Task 5.1**
  - Taking into account the inputs from the pSHIELD final review, additional studies have been carried out to find the adequate models and methodologies that represent the official SHIELD Formal Model.
  - Refinement and tailoring to the middleware architecture (liason with Task 5.2) of the methodology identified to build the "knowledge base" used by the SHIELD Middleware to compose SPD functionalities, mainly based on the decoupling between "domain information" and "security information".

- Preliminary Analysis about the integration between policies representation and semantic representation have been started
- Some additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve semantic technologies and their implementation.

Objectives: defining the nSHIELD SPD driven Semantics paradigm
Results: inputs to the D5.1 deliverable "Technical Assessment"

- **Task 5.2**
  - Additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve middleware core services.
  - Collaboration with partners to identify and address interoperability issues between interfaces and between said interfaces and the nSHIELD platform. Also a collaboration with partners has been carried out to identify common ground and facilitate cooperation at later stages (namely integration and demonstration).
  - In order to address security, privacy and dependability (SPD) in the context of ESs as "built in" functionalities, proposing and perceiving with this strategy the first step towards SPD certification for future ESs, SES edited a Protection Profile for the Middleware layer. This must be seen as a first step to define a security problem definition and security objectives for embedded systems (ESs) which aim to be SHIELD compliant.

Objectives: defining the nSHIELD Core SPD services
Results: Preparation of D5.3 deliverable, definition of the CC Protection Profile for nSHIELD Middleware layer.

- **Task 5.3**
  - Definition of a policy classification and hierarchy so to have a common model to policy definition in nSHIELD project. This model aim to be valid for:
    • those policies to be used as input to a Policy-based management which aim to ensure a defined level of security, privacy and dependability
    • those policies that serve as the governing reference for any required adaptation a particular scenario may require.

Objectives: defining the nSHIELD Policy-based management paradigm
Results: inputs to the D5.1 and preparation of D5.2 deliverable

- **Task 5.4**
  - Liaisons between the modelling of SPD functionalities for control purposes, and their semantic representation (Task 5.1) have been maintained and enriched.
  - Some additional work has been performed in the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve overlay.

Objectives: defining the nSHIELD Policy-based management paradigm
Results: inputs to the D5.1 and reparation of D5.2 deliverable

- **Task 6.1**
  - Participation in call conferences with partners to discuss multi-technology system integration
- **Task 6.2**
  - Participation in call conferences with partners to address multi-technology validation and verification issues.
  - Definition of a verification and validation methodology for heterogeneous nSHIELD prototypes.
  - Contribution to Validation and Verification procedure of Middleware Protection Profile.
  - Integration of the contributions received by the various partners for the preparation of the deliverable D6.2

Objectives: development of prototypes ready to be integrated in the nSHIELD platform
Results: inputs to the D5.2 and D5.3 deliverable

- **Task 7.3**
  - Dependable Avionic Demonstrator Architecture definition (General description and SW & HW architecture outline)
  - Use of OMNIA prototype in nSHIELD finalized to the Avionic Demonstrator.
  - Evaluation concerning the integration of IQ_Engine in OMNIA
  - Definition of SHIELD prototypes to be integrated in the architecture of Avionic demonstrator
  - Preliminary analysis of Validation and Verification process for the scenario
  - Definition of the complete list of prototypes involved in the avionic Demonstrator Architecture including

I/F

Objectives: defining the avionic scenario demonstrator

Results: input to D7.3

- **Task 8.1**
  - Discussion on the subject of D8.4 and outcomes of project
  - Contribution on providing information for the nSHIELD website.
  - Contribution on providing information on nSHIELD Wiki.
- **Task 8.2**
  - Contribution on providing information for the nSHIELD website.

Description of criticalities met during the period:

- Some deliverables have a delay due to the following reasons: some partners started their activities later because of a delay in the signature of national contracts; some deliverables are considered as key deliverable for a common understanding of the project and objectives, so they need more time than planned.
- Change of Selex ES coordinator
- Merging between Selex Galileo and Selex Elsag in Selex ES
- Difficult to find Avionic SW engineering expertise due to the restructuring of Selex.
- The characteristics of the three node types (SDR/Cognitive, Micro and Power), as the main WP3 task, have still not been clearly defined, making it harder to typologize the SPD-driven networks and the corresponding security functionalities (since they heavily depend on the node capabilities)
- Unable to contact partner THYIA

Corrective actions:

- The delay of some deliverable does not impact the upcoming deliverables. However a recovery plan has been established and the project will be on track on month 24.
- Definitions of the node types as the output of the T3.1-T3.3 has been one of the topics of the Barcelona project meeting. The basic characteristics have now been decided upon, and these will be explained in detail in the upcoming deliverables D3.2 and D3.3.
- Tasks and duties allocated to partner THYIA have been re-distributed among other partners.
- Involvement of Selex ES Avionic capability department on the definition of the Avionic Scenario
- Support to the new coordinator by partners and colleagues.

- Meetings performed during the period:
- T7.1,T7.2, T7.3 Webex meeting (Demonstrators ToC definition) 12.07.2013
- Project plan status meeting 26.06.2013
- nSHIELD Project meeting Stockholm, 12.6.2013.-13.6.2013.
- T7.3 Webex meeting (Avionic Scenario interfaces definitions), 4.6.2013.
- T7.3 Webex meeting (Avionic Scenario WBS structure and initial contributions), 11.4.2013.
- T7.3 Webex meeting (Avionic Scenario consolidation), 3.4.2013.
- nSHIELD project meeting Barcelona, 06/03/2013 – 07/03/2013
- TMC meeting on 28/11/2012
- nSHIELD annual review Rome, 18/10/2012.
- nSHIELD project meeting Budapest, 11/09/2012
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis
- nSHIELD WP5 Skype/teleconference meetings, held on a monthly basis (on a bi-weekly basis in the first two months)

Deviations between actual and planned person-months:

- Resources have been temporarily diverted from WP6 to WP2 in order to overcome the problems arising from THYIA poor contribution during the period. For this reason within WP2 an effort greater than the planned one has been spent while with regard to WP6 the actual effort was reduced (in the first six months)
- Resources involved on T7.3 have been not totally used.

Dissemination activities and exploitation perspectives:

- nSHIELD has been presented at the ARTEMIS & ITEA Co-summit 2012 on October 2012 in Paris

4.2 Spain

4.2.1 Acorde Technologies AT

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP1 - Project management		
Task(s)	Task 1.1 Project management		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	3 PM	2.65 PM	69%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- During this reporting time the first review of the project has been performed. AT has contributed actively with the project coordinator with the management of the deliverables (format review, templating...).
- Four face to face meetings have been scheduled and AT has participated in three of them.

- Task 1.1 – Project Management
  - AT has contributed actively in the deliverables of this task, the Quality Control Guidelines and Report as well as the management reports.
  - Results: Deliverables D1.2, D1.6, D1.7 and D1.8

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

- Project meeting, 10th September 2012, Budapest
- First Review, 17th October (pre-review meeting) – 18th October (Review) 2012, Rome
- Project meeting, 6th March 2013, Barcelona

Deviations between actual and planned person-months:

- …

Dissemination activities and exploitation perspectives:

- References to the project have been added to the web site of the company and to the presentations of the company, and included within the R&D projects portfolio.

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP2 - Scenarios, requirements and system design		
Task(s)	Task 2.3 Multi-technology architectural design		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.3	1.24 PM	1.3 PM	83%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

In this WP AT is focused in the architecture definition, mainly in the node layer. In addition, some contribution to other tasks of the work package has been carried out.

- Task 2.3
  - In this task ACORDE has contributed with the architecture definition. Deliverable D2.4 has been finalized during this reporting time and the main work done by ACORDE has been focused in the node layer definition. Draft version of the main modules of the node layers has been defined as started point for WP3 implementations.
    Some contributions to D2.6, *Final System Requirements and Specifications,* has been sent.
  - Results: Deliverable D2.4 has been finalized during this period as an *intermediate* version of the "System Architecture Design".
    D2.6, *Final System Requirements and Specifications* has been finalized at the end of this reporting time.

Description of criticalities met during the period:

- None

Corrective actions:

- None

Meetings performed during the period:

- WP2 phone meeting: 10th July

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP3 - SPD node		
Task(s)	Task 3.1 SDR/Cognitive Enabled node Task 3.2 Micro Node Task 3.3 Power Node Task 3.5 Cryptographic technologies		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.1	0 PM	2 PM	80%
Task 3.2	2.5 PM	5.7 PM	80%
Task 3.3	2.5 PM	0 PM	-%
Task 3.5	2.7 PM	2 PM	80%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

Two main topics have been analysed and reported in the framework of this WP. The power supply protections of SDR/Cognitive enabled nodes and the anti-tamper modules. AT has designed a prototype to validate the studies performed in the fields of power supply protection and physical barriers for anti-tampering.

- Task 3.1
  - During this reporting time AT has proposed a design for a Smart Power Unit and presented it in the deliverables of the work package.
  - Results: These analysis and design have been summarized in the internal deliverable D3.2 and the public one D3.3
- Task 3.2
  - In order to build a prototype to validate the technologies analysed, and taking into account that BeagleBone board has been considered one of the reference platform, AT, together with two other partners TELC and TUC, has designed a BeagleBone cape including different technologies studied in the scope of the project: Smart power unit + anti tamper solution + Smart Card (TELC) + ZigBee Module (TUC). During this reporting time the first design has been finalized and future steps are the manufacturing and testing phase.
  - Results: First design of a custom BeagleBone Cape.
- Task 3.5
  - There are basically two kinds of anti-tamper measurements to protect the sensitive information of the node and prevent an easy access by an external attacker:
    - Measures that are typically implemented at manufacture level as passive physical barriers
    - Measures consisting of continuous monitoring and detection of tamper attacks.

    AT has investigated different solutions for the first option, encapsulation and physical barriers.
  - Results: These analysis and design have been summarized in the internal deliverable D3.2 and the public one D3.3

Description of criticalities met during the period:

Corrective actions:

Meetings performed during the period:

- All discussions about the prototype design has been perform by mail with the other partners, mainly TELC and TUC

Deviations between actual and planned person-months: None

Dissemination activities and exploitation perspectives: nona

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP6 - Platform Integration, validation & demonstration		
Task(s)	Task 6.1 Multi-technology System Integration Task 6.2 Multi-technology Validation & Verification		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 6.1 Task 6.2	6 PM 3.5 PM	6.7 PM 3.5 PM	50% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

These WP activities have been initialized during this period. A phone conference has been done in order to clarify and distribute the work that will be carried out in the following period.

Within the scope of the project, Telcred (TELC), Acorde (AT), and SICS are collaborating on developing a secure micro node, which can be used as a lock controller. A custom "cape" for a standard BeagleBone low end Linux computer has been developed. This cape will provide features such as tamper detection, backup power, secure storage of cryptographic keys, and a real time clock. This prototype will worked as an offline access control and it has been included in the list of nSHIELD prototypes.

- Task 6.1
  - First step in this task has been the elaboration of the list with all prototypes available in the project.
  - Results: contribution to *D6.3 Prototype Integration Report.*

- Task 6.2
  - In this task, one prototype has been added in the deliverable D6.2. The description, the SPD requirements covered, and the initial test cases to validate the prototype have been the sections included.
  - Results: contribution to *D6.2: Prototype Validation and Verification*

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

- WP6 phone meeting: 14th February 2013

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP7 - SDP Applications		
Task(s)	Task 7.1 Railways security		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 7.1	0.6 PM	0.6 PM	30%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

The activities of this WP have been starting during this reporting time. AT collaborates in one of the four scenarios proposed to validate the nSHIELD prototypes.

- Task 7.1
  - AT +TELC + SICS prototype has been included in the Railways security demonstrator as an Offline Access Control
  - Results: Contribution to deliverable *D7.1 Railways security demonstrator – integration and validation plan*

Description of criticalities met during the period:

- None

Corrective actions:

- **None**

Meetings performed during the period:

- None

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

Beneficiary:	ACORDE TECHNOLOGIES, AT		
Work Package(s)	WP8 - Knowledge exchange and industrial validation		
Task(s)	Task 8.1 Dissemination Task 8.2 Standardization		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 8.1	0.7 PM	0.6 PM	45%
Task 8.2	0.68 PM	0.5 PM	60%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

During this period of time the nSHIELD project has been included in the company profile presentations. The nSHIELD project has been shown in several customer presentations and public conferences where ACORDE has participated.

During this reporting time the exploitation plan of the company in the scope of the project has been updated, with a contribution to deliverable *D8.5: Preliminary Exploitation Plan*

Description of criticalities met during the period:

- None

Corrective actions:

- None

Meetings performed during the period:

- None

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- References to the project have been added to the web site of the company and to the presentations of the company, and included within the R&D projects portfolio.

4.2.2 Fundacíon Tecnalia Research & Innovation TECNALIA

Beneficiary[20]:	TECNALIA		
Work Package(s)	WP2[21] - SPD Metric, requirements and system design		
Task(s)	Task 2.1 - Multi-technology requirements & specification Task 2.2 - Multi-technology SPD metrics Task 2.3 - Multi-technology architectural design		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1 Task 2.2 Task 2.3	1 PM 2 PM 1 PM	4,4 PM 10 PM 3 PM	440 % 500 % 300 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 2.1**
  - Liaison between security specification and metrics
  - 2.6 document refinement and coordination
  - 2.6 requirements refinement for scenarios and prototypes

Objectives: defining the requirement of the nSHIELD framework driven by the use case and prototytpes
Results: Preparation of D2.6 deliverable

- **Task 2.2**
  - Definition of Multi-metric approach for quantitative solution
  - Liasons with WP7 use cases for defining multi metric approach
  - Mathematical and formal approaches including genetic algorithms

Objectives: defining the SPD metrics composition of the nSHIELD framework
Results: Preparation of D2.8 deliverable, inputs to Task 5.1, Task 5.5 and Task 7.1

- **Task 2.3**
  - Definition of a more formalised heterogenous architecture: formal refinement;
  - Contribution to finalization of nSHIELD Reference System Architecture;
  - verification of the conformity of the identified prototypes with the proposed nSHIELD System Architecture

Objectives: defining the nSHIELD framework architecture
- Results: preparation of deliverable 2.7

Description of criticalities met during the period:

- Metric composition approach is important in order to measure SPD functionality in a not linear way. Approach being addressed reflects composition in a not linear way
- Formalisation of the global specification

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- Due to cost changes during in proposal phase and execution phase and the amount of worlk overloaded because of the WP2 new leadership for Tecnalia, Tecnalia is spending more effort for this period.

Dissemination activities and exploitation perspectives:

- Tecnalia is activating the publication of metric oriented paper.

[20] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[21] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[22]:	TECNALIA		
Work Package(s)	WP3[23] - SPD Node		
Task(s)	Task 3.4 – Dependable self-x technologies Task 3.5 – Cryptographic technologies		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.4 Task 3.5	2PM 1 PM	3,1 PM 2 PM	155% 200 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 3.4**
  - Analysis of self-x technologies for M2M industrial scenarios

Objectives: refinement of described prototypes for D.3.2 and D3.3
Results: Preparation of D3.2 and D.3.3

- **Task 3.5**
  - Analyssi of SHA1 and MD5 based cryptography for light secure elements forming light M2M networks

Objectives: refinement of described prototypes for D.3.2 and D3.3
Results: Preparation of D3.2 and D.3.3

Description of criticalities met during the period:

- none

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

[22] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[23] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[24]:	TECNALIA		
Work Package(s)	WP4[25] - SPD Network		
Task(s)	Task 4.2 – Distributed self-x models Task 4.4 – Trusted and dependable connectivity		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 4.2 Task 4.4	3 PM 4 PM	4PM 5,8 PM	133,3% 145%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 4.2**
  - Development of QoS for DLMS Network converging with nSHIELD requirements

Objectives: refinement of described prototypes for D4.2 and D4.3
Results: Preparation of D4.2 and D4.3

- **Task 4.4**
  - SPD functionality implementation in DLMSCosem network: towards defining an industrial trusted and dependable connectivity.

Objectives: refinement of described prototypes for D4.2 and D4.3
Results: Preparation of D4.2 and D4.3

Description of criticalities met during the period:

- SPD functionality implementation feasibility in DLMS Cosem networks.

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- Due to cost changes during in proposal phase and execution phase Tecnalia is spending more effort for this period in WP4.

Dissemination activities and exploitation perspectives:

- None

Beneficiary[26]:	TECNALIA

[24] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[25] x is 1, 2, 3, 4, 5, 6, and 7

[26] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Work Package(s)	WP5[27] - SPD Middleware and Overlay		
Task(s)	Task 5.1 – SPD driven semantics Task 5.2 – Core SPD services		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 5.1 Task 5.2	2 PM 3 PM	3 PM 3,4 PM	150% 113,3%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 5.1**
  - Interfaces between metric approach and semantica driven development
  - Orchestration analysis

Objectives: refinement of described prototypes for D5.2 and D5.3
Results: Preparation of D5.2 and D5.3

- **Task 5.2**
  - Analysis of Core SPD services orchestration vs metrics compositional approach
  - Metric functionality analysis in middleware for core services

Objectives: refinement of described prototypes for D5.2 and D5.3
Results: Preparation of D5.2 and D5.3

Description of criticalities met during the period:

- Understand liaisons between metric composition and SPD core services composition and orchestration

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

[27] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[28]:	TECNALIA		
Work Package(s)	WP6[29] - Platform Integration, validation & demonstration		
Task(s)	Task 6.3 – Lifecycle SPD support		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 6.3	7 PM	12,8 PM	182,9%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 6.3**
  - Development of the plan for lifecycle and SPD support. Tecnalia leads this deliverable that develops SPD lifecycle methodology.

Objectives: develop a feasible plan supported in a credible methodology
Results: D6.1 ready and preparation of D6.4 which is the report

Description of criticalities met during the period:

- None

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- Due to cost changes during in proposal phase and execution phase Tecnalia is spending more effort for this period in WP6 for task 6.3.

Dissemination activities and exploitation perspectives:

- None

[28] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[29] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[30]:	TECNALIA		
Work Package(s)	WP7[31] - SPD Applications		
Task(s)	Task 7.1 – Railways security Task 7.2 – Voice/Facial Recognition Task 7.4 – Social mobility		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 7.1 Task 7.2 Task 7.4	0 PM 2 PM 2 PM	1 PM 1,2 PM 1 PM	100% 60% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 7.1**
  - Case study construction support
  - Liaison with WP2
  - Links to metrics composition

Objectives: develop a coherent railway scenario in order to prove nSHIELD prototypes
Results: Preparation of D7.1

- **Task 7.2**
  - Case study construction support
  - Liaison with WP2
  - Links to metrics composition

Objectives: develop a coherent voice/facial scenario in order to prove nSHIELD prototypes
Results: Preparation of D7.2

- **Task 7.4**
  - Case study construction support
  - Liaison with WP2
  - Links to metrics composition

Objectives: develop a coherent social mobility and networking scenario in order to prove nSHIELD prototypes
Results: Preparation of D7.4

Description of criticalities met during the period:

- None

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

[30] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[31] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[32]:	TECNALIA		
Work Package(s)	WP8[33] - Knowledge exchange and industrial validation		
Task(s)	Task 8.1 – Dissemination Task 8.2 – Standardisation		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 8.1 Task 8.2	1 PM 1PM	1 PM 1 PM	100% 100%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 8.1**
  - Dissemination activities carried out in cross European projects (nSHIELD presentation in RISC project kick off (DG_HOME))
  - Developing paper in SPD metric area

Objectives: construct TECNALIA's dissemination activities withing nSHIELD scope
Results: Execution of dissemination plan

- **Task 8.2**
  - Tecnalia is now member of M490-SGIS ETSI/CENELEC security group and aims to incorporate nSHIELD results as inputs for industrial cybersecurity standards

Objectives: improve current European security standards
Results: Execution of standardisation plan

Description of criticalities met during the period:

- None

Corrective actions:

- none

Meetings performed during the period:

- nSHIELD project meeting Kista Sweden, June 2013
- nSHIELD TaskForce Skype/teleconference meetings, held on a bi-weekly basis

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- Paper in SPD metrics scope

[32] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[33] x is 1, 2, 3, 4, 5, 6, and 7

4.2.3 Mondragon Goi Eskola Politeknikoa MGEP

Beneficiary[34]:	MGEP – Mondragon Goi Eskola Politeknikoa		
Work Package(s)	WP1[35]- Project Management WP4 - SPD Network WP5 - SPD Middleware & Overlay WP6 - Platform integration, validation & demonstration WP8 - Knowledge exchange and industrial validation		
Task(s)	Task 1.1 Project management Task 4.3 Reputation-based resource management technologies Task 4.4 Trusted and dependable Connectivity Task 5.1 SPD driven Semantics Task 6.1 Multi-Technology System Integration Task 8.1 Dissemination		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	1	1	66%
Task 4.3	6.0	6.1	65%
Task 4.4	2.0	1.9	65%
Task 5.1	7.5	7.5	100%
Task 6.1	0.2	0.2	6%
Task 8.1	3	3	55%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

During this period we have focused on two main aspects of nSHIELD. On the one hand the reputation and trust based Intrusion Detection Systems (IDS), for which we propose a new architecture and now are deploying the algorithm in a general purpose development platform for wireless sensor networks

On the other hand MGEP has participated in the assessment of the proposed ontologies for intrusion detection. Intrusion detection systems can be defined as a set of different scanners that monitor the activities of an information system looking for malicious actions. MGEP has created a sample ontology for Intrusion Detection Systems that extends the ontology delivered in pSHIELD.

- **Task 1.1 Project management**

Reporting of progress and resource expenditure, production of deliverables, attendance of technical meetings in Budapest, Barcelona and Stockholm, and the nSHIELD first year review in Rome as well as the Artemis-Itea2 co-summit in Paris and several technical and management teleconferences.

- **Task 4.3 Reputation-based resource management technologies**

During this period MGEP has been working on intrusion detection systems for Wireless Sensor Network (WSN) environments. The IDS proposed is a distributed anomaly detection based system, where each node will have an IDS agent that will monitor local activities. Focus has been placed on the design and implementation of reputation based intrusion detection system for wireless sensor networks prototype. An initial implementation of the reputation based IDS on Zolertia Z1 hardware has been produced.

[34] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[35] x is 1, 2, 3, 4, 5, 6, and 7

- **Task 4.4 Trusted and dependable connectivity**

One of the main concerns is the requirements definition for lightweight link-layer secure communication in wireless sensor network scenarios. This is taken into account in the architecture proposed and described in the previous paragraph (Task 4.3), as the agent based detection system minimises the communication needs.

- **Task 5.1 SPD driven Semantics**

From the point view of ontologies, intrusion detection can be considered as possessing several characteristics and classifications and it needs a language that describes instances of that ontology. MGEP has participated in the assessment of several proposed ontologies for intrusion detection. MGEP has proposed an ontology from the literature and has created an extension of pSHIELD ontology that includes some IDS properties. MGEP has created a sample ontology for Intrusion Detection Systems that extends the ontology delivered in pSHIELD. A suitable candidate ontology has been also proposed.

- **Task 6.1 Multi-Technology System Integration**

MGEP has collaborated in the definition of the integration scenarios

- **Task 8.1 Dissemination**

During this period, MGEP, as leader of WP8 has managed nShield project public website http://www.newshield.eu. The elaboration of deliverables D8.4 and D8.6 has also been coordinated by MGEP. It must be mentioned that the delivery of these documents suffered considerable delay. MGEP organised and chaired Embedded System Security Sessions also promoted nSHIELD internally in Mondragon University.

Description of criticalities met during the period:

The major deviation is related to the deliverable D8.4: "SHIELD run-through" (previously known as D8.4: "Operational Manual v1").

- This deliverable has caused considerable controversy within the consortium as it is considered a key deliverable for dissemination but also for a common understanding of the project and objectives. It is planned to be a short and direct document aiming non-technical audience where the necessity of security in embedded systems must be clear and also how adopting the SHIELD approach can help designing SPD compliant embedded systems.
- Due to this internal discussion, the deliverable has been delayed.

Corrective actions:

- Deliverables *D8.4, D8. 6 and D8.7 Operational Manual* (*v1, v2 and v3* respectively) coordinated by MGEP have been renamed to *D8.4, D8. 6 and D8.7 SHIELD run-through (v1, v2, and v3)*. There is no change in the description of the deliverable content described in the TA, just the name changes. The reason is, that this term fits better to what the reviewer suggested and the original term was somehow confusing as we saw in Brussels meeting.

- Content-wise, an agreement is needed and a Task Force team has been created to manage this issue. Although first Task Force meetings were inconclusive. A final decision was not made either in Barcelona or in Stockholm meetings what caused a further delay of the deliverables.

Meetings performed during the period:

Meetings:

- Project Meeting, 11-12 September 2012, Budapest
- Working meeting during Artemis-Itea2 co-summit, Paris, 30 & 31 October 2012 (informal)
- nSHIELD first year review in Rome 17-18 October 2012
- Project Meeting, 6-7 March 2013, Barcelona
- Project meeting, 12-13 June, Kista/Stockholm

Phone conferences:

- WP4-T4.3 meeting, 2013.05.20
- WP4 meeting 2013.05.13
- Task Force 27.02.2013
- Task Force 13.02.2013
- Task Force 2013.01.23
- WP5 meeting 2013.01.16
- Task Force 2013.01.09
- WP4 meeting 2013.01.23
- Task Force 2012.12.19
- WP5 Middleware 2012.12.19
- Task Force 2012.11.28
- WP4 meeting 2012.11.21

Deviations between actual and planned person-months:

- There are no major deviations in the planned effort (person-months) that need to be mentioned. The resources have been distributed according the schedule in the appendix

Dissemination activities and exploitation perspectives:

- Other dissemination actions carried out by MGEP:
  - Organization and chairing of the Embedded System Security Session in the XII Spanish Meeting on Cryptology and Information Security (RECSI 2012), Donostia-San Sebastián (Spain), 4-7 September 2012.
  - Organization and chairing of the Special session on Measurable security for Embedded Computing and Communication Systems (MeSeCCS 2014), within International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014, 7 – 9 January, 2014 – Lisbon, Portugal.
- Post in the Mondragon University ICT blog: http://mukom.mondragon.edu/ict/mu-at-artemis-and-itea-2-co-summit/

4.2.4 Indra Software Labs (ISL)

Beneficiary[36]:	Indra Software Labs (ISL)		
Work Package(s)	WP1 - Project Management		
Task(s)	Task 1.1 Project Management		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	3,7 PM	3,7 PM	60%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Overall financial and technical planning;
- Controlling project scheduling and achievements;
- Reporting of progress and resource expenditure;
- Organization of the meetings of the PA, TMC, plenary, and review meetings;
- Liaison with other projects (at a technical level, liaison will also be performed by WP leaders and individual partners);
- Handling the cost claim procedures and maintaining the financial budget status of each partner;
- Maintaining the technical description of the work and the Consortium Agreement;
- Approving and validating the visible outputs, such as deliverables, presentation material, papers, etc., thus adding a level of quality assurance to the project;
- Managing intellectual properties and patent requests;
- Supervising the website and e-mail lists;
- Contact point to the ARTEMIS JU including supervision of deliverable creation and in-time forwarding;
- Chairing processes to handle IPR on project results.
- As this task is mainly devoted to management, SG will take the lead. All other participants are included according to the described management structure.

-

Corrective actions:

- None

Meetings performed during the period:

- Rome meeting (October 2012)
- Barcelona meeting (March 2013)
- PL-phoneconf-1Jul2013

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

Explained below in WP8.

[36] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary[37]:	Indra Software Labs (ISL)		
Work Package(s)	WP4 - SPD Network		
Task(s)	**Task 4.3 Reputation-based resource management technologies** **Task 4.4 Trusted and dependable connectivity**		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 4.3 Task 4.4	6 PM 11 PM	6 PM 11 PM	100% 70%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 4.3 Trusted and dependable connectivity, 100% of work completed at the end of the period for the following specific tasks:**
  - Attending the WP conferences talks (skype) where WP issues are discusses.
  - Studying certification and authentication protocols
  - Contribute to D4.3 Preliminary SPD network technologies prototype Report

- **Task 4.4 Trusted and dependable connectivity, 70% of work completed at the end of the period for the following specific tasks:**
  - Defining an outline for Preliminary SDP Network Technologies Prototype Requirements for T4.4 as task coordinators.
  - Attending the WP conferences talks (skype) where WP issues are discusses.
  - Buying hardware to accomplish the tasks of this WP: RaspBerry Pi, Zolertia Z1, At-USB
  - Studying the security networks requirements for lightweight networks.
  - Studying several operative systems for motes
  - Test tinyOS + cc2420 security on motes (IEEE 802.15.4 compliant).
  - Implement CCM, CTR and CBC-MAC algorithms to provide confidentiality, integrity and authenticity to the transmitted data.
  - Contribute to T4.4 in the Preliminary SPD Network Technologies Prototype Requirements.
  - Contribute to T4.4 in the Preliminary SPD Network Technologies Prototype

Corrective actions:

- None

Meetings performed during the period:

- 4 WP4 skype conferences (December 2012, May 2013)

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

Explained below in WP8.

[37] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary[38]:	Indra Software Labs (ISL)		
Work Package(s)	WP5 - SPD Middleware & Overlay		
Task(s)	**Task 5.3 Policy-based management**		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 5.3	12 PM	12 PM	90%

- **Task 5.3 Policy-based Management, 90% of work completed at the end of the period for the following specific tasks:**

  - This task aims at designing and developing a SPD-middleware policy-based management for ensuring a high level of security, privacy and dependability in systems **composed by Intelligent ES Nodes (developed in WP3) and based on Smart Transmissions (developed in WP4) on the base of the metrics identified in task 2.2**. In order to build specific management functionalities and procedures for accomplishing these objectives, several aspects will be investigated and analyzed.

  - Studying what kind of policies can be proposed, among all, Indra has identified the following kind:
    - Power policy-based: change the roles of the nodes in function of the battery or power life of them. For instance:

    If Nodei.getremaingBattery() <= threshold then REDUCE the routing capabilities of the node and turn it into a "leaf node".
    Thus in this study we have to perform an analysis of different thresholds in order to propose proper values for different kind of nodes and roles.
    If Nodei.getremaingBattery() <= threshold then CHANGE the routing capabilities of the node.
    Thus in this study we have to perform an analysis of different thresholds in order to propose proper values for different kind of nodes and roles. Moreover, in this case we have to propose (in conjunction) with WP4 different routing schemes.

    - Security policy-based: change the roles of the nodes in function of the certificates of nodes. For instance:

    If Nodei.getFQDN().equal("STRING") decide what kind of functionalities, permissions, roles or responsabilities this node has.
    If Nodei.getOrganizationalUnit().equal("STRING") decide what kind of functionalities, permissions, roles or responsabilities this node has.
    Summarizing use the nodes' certificates to apply policies in the middleware or application layer.

Corrective actions:

- None

Meetings performed during the period:

- 5 WP5 skype conferences

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

Explained below in WP8.

[38] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary[39]:	Indra Software Labs (ISL)		
Work Package(s)	WP6 – Platform integration, validation and demostration		
Task(s)	**Task 6.1 Multi-Technology System Integration**		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 6.1	11,5 PM	11,5 PM	50%

- **Task 6.1 Multi-Technology System Integration, 50% of work completed at the end of the period for the following specific tasks:**
  - Prepare validation tests to check link layer security.
  - Attending the WP conferences talks (skype) where WP issues are discusses.
  - Contribute to D8.2 Prototype validation and verification.
-

Corrective actions:

- None

Meetings performed during the period:

- 1 WP6 phone conference
-

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

Explained below in WP8.

[39] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary:	Indra Software Labs (ISL)		
Work Package(s)	WP8 - Knowledge exchange and industrial validation		
Task(s)	**Task 8.1 Dissemination** **Task 8.2 Standardization** **Task 8.3 Exploitation**		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 8.1 Task 8.2 Task 8.3	2 PM 3,1 PM 0,7 PM	2 PM 3,1 PM 0,7 PM	58% 80% 20%

Task 8.1 Dissemination, 58% of work completed at the end of the period for the following specific tasks:

- Dissemination activities will consist in the publication of all important results in well-known conferences and journals. The research issues of the project will be promoted through the organization of special sessions in conferences and workshops on the research topics of the project. The universities will contribute to the dissemination of knowledge by producing scientific publications, by organizing and participating to dissemination events (international conferences and workshops) and by organizing an international journal special issue on the main research nSHIELD topics. Another important outcome of this task will be the annual delivery of the nSHIELD operational manual.
- Also we are involved in Deliverable D8.1.2 Dissemination Plan. Regarding the dissemination plan Indra is working on:
  - Prepare a press release for the media in Spain country that will make the punctual diffusion of the project's progress. In order to perform this task, we are expecting the next meeting in Budapest (September 2012) to coordinate the content of the press release with the rest of the partners.
    - Also, we are coordinating together with S-LAB an agreement with local or national media in order to publish the first press release about nSHIELD (the progress, partners involved, roadmap …).
    - Press Release has been published with a high media impact.
  - Following the same methodology, we are going to promote an nSHIELD Internet release for the Indra corporative web portal and also for the Indra' magazine called "Boletin Global de Noticias" (included in the D8.1.2 in subsection Brochures, flyers and posters).
  - We have contributed directly in the wiki and in the nSHIELD webpage in several sections such as:
  - http://nshield.unik.no/wiki/Project_Meeting_Barcelona_2013
  - http://nshield.unik.no/wiki/NSHIELD_Dissemination
  - http://www.newshield.eu/2012/01/in-the-press/
- Also we are involved in Deliverable D8.3 Standardization Plan, completing the following sections:
  - Interaction with other relevant standardization bodies and industrial for a, concretely subsection 2.6.3 of the deliverable where we include as a possible standardization body the European Network and Information Security Agency (ENISA), in order to develop advice and recommendations on good practice in information security.

Task 8.2 Standardization, 60% of work completed at the end of the period for the following specific tasks:

- Studying actual standards related to SPD network technologies in order to know the state of the art and be able to contribute to standardization institutions in the following period.

Task 8.3 Exploitation, 20% of work completed at the end of the period for the following specific tasks:

- Prepare Preliminary Exploitation Plan deliverable.
- Contact teams of INDRA involved in interesting projects such as Atenea (http://www.indracompany.com/en/noticia/indra-designs-an-urban-platform-for-smart-city-government) in order to exploit the developments of the nSHIELD in other projects

Meetings performed during the period:

- 1 WP8 phone conference

Deviations between actual and planned person-months:

- None

4.3 Slovenia

4.3.1 THYIA Tehnologije

Beneficiary[40]:	THYIA Tehnologije		
Work Package(s)	WP2 – SPD Node		
Task(s)	WP2 – SPD metrics, requirements and system design WP3 – SPD Node WP4 – SPD Network WP5 – SPD Middleware and Overlay WP6 – Platform integration, validation & demonstration WP7 – SPD Applications		
Period:	1st September 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1	0,167	0,167	90%
Task 2.2	0,167	0,167	90%
Task 2.3	0,167	0,167	90%
Task 3.1	0,2	0,1	60%
Task 3.2	0,2	0,1	60%
Task 3.3	0,2	0,1	60%
Task 3.4	0,2	0,1	60%
Task 3.5	0,2	0,1	60%
Task 4.1	0,167	0,167	80%
Task 4.3	0,167	0,167	80%
Task 4.4	0,167	0,167	80%
Task 5.1	0,125	0,125	80%
Task 5.2	0,125	0,125	80%
Task 5.3	0,125	0,125	80%
Task 5.4	0,125	0,125	80%
Task 6.1	0,167	0,167	25%
Task 6.2	0,167	0,167	25%
Task 6.3	0,167	0,167	25%
Task 7.4	0,5	0,5	20%
Description of the activities carried out during the period to reach specific objectives within the task/WP: ➢ THYIA in the second years only monitored R&D project activities and made a review of all final deliverables due for the second years. The reviews will be sent after the second review meeting with the reviewers. The reason for that is an intensive activity of the consortium in the last month with dynamic changes that required correction of the initial review reports prepared by THYIA.			
Description of criticalities met during the period: ➢ Due to company restructuring and some concerns with national funding authority, THYIA is no longer able to confirm its commitment for the prosecution of the SHIELD project, as originally declared in the technical annex.			
Corrective actions:			

[40] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

➢ A reduced involvement of THYIA, with a reduced amount of MM effort from M18 to M36, has been planned, as detailed in the Amendment #32.
Meetings performed during the period: ➢ None
Deviations between actual and planned person-months: ➢ None.
Dissemination activities and exploitation perspectives: ➢ None

4.4 Norway

The activities in Norway are collectively reported in the "Movation" report, while the effort tables are available in each chapter. Movation has a clear mandate from the Inner Circle partners to follow technological trends, and as such a high interest in the results of «measurable security». Noom had a vision on how to contribute, but had suffered from finding the way into the project, based on the minor budget. ESIS, the founder of the Socialtainment scenario, suffered most from the lack of academic support. Due to additional changes in the business environment, ESIS needed to reconsider the participation in nSHIELD. As a result, ESIS announced in Q1.2012 to leave the project.

The Norwegian participation is now stable with Movation, Alfatroll and Seek and Find. Focus is on demonstration and feasibility of the SHIELD approach in the "UAV" and the "Social Mobility" use case, as well as applicability of the approach to other sectors.

4.4.1 Movation AS (MAS), Alfatroll (ALFA) and Seek and Find (SknFnd)

Beneficiary[41]:		**Movation and Alfatroll**	
Work Package(s)		WP6 - Platform integration, validation & demonstration WP7 – SPD Applications WP8 – Support Activities	
Task(s)		Task 6.1 – Multi-technology System Integration Task 6.2 – Multi-Technology Validation & Verification Task 7.1 – Railroad Security Task 7.3 – Dependable Avionic Systems Task 7.4 – Social Mobility Task 8.1 – Dissemination Task 8.2 – Standardization Task 8.3 – Exploitation	
Period:		Sept 2012 - August 2013 Note: reporting numbers below are MAS + ALPHA + SknFnd	
Task(s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 6.1	3 + 4 + 0PM	3 + 4 + 1 PM	60%+60%
Task 6.2	0 PM	0 PM	0%
Task 7.1	5+ 0 + 0PM	0 PM	0%
Task 7.3	0.5 + 4 + 0 PM	0.5 + 4 + 0 PM	40%+50%
Task 7.4	1.5 + 0 + 1 PM	1.5 + 0 + 1 PM	40%+0+10%
Task 8.1	2 + 0 PM	2 PM	60%
Task 8.2	0 PM	0.5 PM	50%
Task 8.3	0 PM	0 PM	20%

This description of the activities contains the contribution from all partners (Movation, Alfatroll) of Norway in nSHIELD:

- Though coming late into the project, Alfatroll has successfully laid the way for integration of it's IQEngine prototype. The IQEngine is tailed for the UAV scenario, answering the needs from certification of unmanned aircrafts. The EuroHAWK disaster shows the need for a fundamentally new approach of software on a UAV. The EuroHAWK reports indicate that more than 500 MEuro have been used to get

[41] This report is for all Norwegian partners and contains reporting for all WPs

the American UAV converted into European airspace, but that the missing chance of certification cancelled the project. Our expectation is that the prototype development of the IQEngine, performed through nSHIELD, will demonstrate an option being certifiable.

- Movation concentrated in this period on the business challenges in bringing measurable security to the industrial community. Though "security" as such is both seen as a necessity to be able to deploy wireless sensors in an industrial environment, the way on how to achieve "security" is not clear. Typical challenges being addressed are "retrofitting of security" and "design for a long time horizon". The SHIELD approach is seen as being highly ambitious, though necessary for the future of the wireless industry. Recent discussions with the oil and gas industry indicates that the SHIELD approach will be taken up the Security working group of the ISO 15926 "Global Integration Project" for the Norwegian shelf.
- Movation also worked on getting the fourth use case, Social Mobility, back on track. Due to changes in partners, we did not have a core team with sustainable PM committed to the task 7.4 until August 2013, when Seek and Find joined the project..

Description of criticalities met during the period:

- The two main criticalities during this period are (i) selling measurable security and (ii) having a feasibility of the SHIELD approach demonstrated in the Social Mobility scenario.
- (i) "Selling" measurable security is a major challenge for SHIELD. Though the need for security is clearly visible, the SHIELD methodology of applying metrics is seen as a difficult approach in the market.
- (ii) Movation searched actively for a good partner from the embedded world to drive the Social Mobility scenario. During the first half of 2013 discussions and negotiations were going on focussing on two potential partners. SknFnd had a research focus which fitted best into the Social Mobility (T7.4) use case, and joined in Augst 2013.

Corrective actions:

- (i) The way to market for the SHIELD approach should focus on incremental steps. First step should be an indicative measure of security, and a second step can then be the focus on a set of metrics (or other methods).
- (ii) Seek and Find joined in Augst 2013, focussing on the Social Mobility use case.

Meetings performed during the period:

- All meetings are documented on the projects wiki: http://nshield.unik.no Examples of such meetings are:

	Date	Phone
PL-conf-1Mar2013	2013-03-01T13:30:00	office phone
TaskForce-27Feb2013	2013-02-27T14:00:00	see list ... 3948369#
WP6-phone-14Feb2013	2013-02-14T11:00:00	+39 010 9165954
TaskForce-13Feb2013	2013-02-13T14:00:00	see list ... 3948369#

- In addition to the project meetings Movation and Alfatroll participated in 10+ industrial face-to-face meetings or workshops discussing security for embedded systems.

Deviations between actual and planned person-months:

- Except the shift of focus from Social Mobility towards UAV the deviations between actual and planned person-months are minor.
- Movation reduced the involvement in nSHIELD to give space for the new partner Seek and Find.

Dissemination activities and exploitation perspectives:

- Movation and Alfatroll participated in 10+ industrial face-to-face meetings or workshops discussing security for embedded systems. Notably here are the Nordic UAV conference co-organized by Alfatroll, the Internet-of-things workshop co-organized by Movation, the industrial contacts to ABB and the Norwegian Oil and

Gass industry, as well as research contacts to the Research Department of the Norwegian Defence and the Norwegian Institute for Information Security (NorSIS).

- The need for certification of software and co-operation in a joined air space are the major challenges. Alfatroll expects that their IQEngine can contribute to a sustainable way of certification of UAV software, and is in discussion with certification organisations on that topic. However, details of the process are delayed until a suitable prototype of the IQEngine is in place.
- Amongst all dissemination activities being described on the wiki (http://nshield.unik.no/wiki/NSHIELD_Dissemination), we would like to focus on the information and knowledge exchange with the Norwegian Oil and Gas industry. EPIM, the Exploration and production information management association, has the focus on IT solutions to promote the best possible flow of information between authorities and licensees on the Norwegian continental shelf. The EPIM Information Management Association has established a project activity named ILAP, Integrated Lifecycle Assets Planning. This new ILAP standard bases on the Generic Information Modeling (GIM) standard (ISO 15926), and is extended into various aspects of oil and gas operations. The two standards being mostly related to the SHIELD security work are ISO 27000+ on Information Security Management and ISO 31000+ on Risk management. The first exchange of knowledge between SHIELD and ILAP has taken place, focussing on the identification of applicability.

4.5 Sweden

4.5.1 Swedish Institute of Computer Science SICS

Beneficiary[42]:	SICS		
Work Package(s)	WP2 - SPD metrics, requirements and system design		
Task(s)	Task 2.1 Multi-technology requirements & specification Task 2.3 Multi-technology architectural design		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1 Task 2.3	1 PM 1 PM	1 PM 1 PM	100% 100%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Before, at the Budapest meeting, and directly after the meeting we worked a lot with cleaning up the requirements handling and improve the structure and working approach.
- We have worked directly with the requirements document updating the content and improve the document structure.

- **Task 2.1**
  - New structure for the Preliminary System Requirements and Specifications suggested and adopted by the rest of the partners.
  - Review and rewrite of the system requirements according to the new structure.
  - Review and input to final requirement specification
- **Task 2.3**
  - Review of the old system architecture and suggestions for modifications/improvements.
  - Input to final architecture design.

Description of criticalities met during the period:

- The system requirements document quality secured and timely delivered before nSHIELD review meeting in October.
- Arranged nSHEILD face-to-face meeting at SICS in Stockholm area, June 12-13, 2013.
- The input to the updated final system requirements document done in August 2013.
- Input to final system architecture design according to time plan.

Corrective actions:

- The systems requirements document quality was not met when reviewed in September 2012 as identified during the nSHIELD internal review. We together with Selex managed to improve the quality by changing

[42] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

the requirement handling process and timely submit new collected requirements prior to the Rome review.
Meetings performed during the period: ➢ nSHIELD face-to-face meeting in Budapest, September 11&12, 2012. Participants from SICS: Christian Gehrmann. ➢ nSHIELD review meeting in Rome, October 17&18, 2012. Participants from SICS: Christian Gehrmann and Viktor Do. ➢ nSHIELD specification working meeting, December 4, 2012. Participants from SICS: Christian Gehrmann ➢ nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24, 2013. Participants from SICS: Christian Gehrmann ➢ nSHIELD face to face meeting, Barcelona, March 6-5, 2013. Participants from SICS: Christian Gehrmann and Viktor Do. ➢ SICS arranged the nSHIELD face-to-face meeting in Stockholm, June 12-13, 2013. Participants from SICS: Christian Gehrmann and Viktor Do.
Deviations between actual and planned person-months: ➢ **We had no deviations between actual and planned efforts in WP2 during the period.**
Dissemination activities and exploitation perspectives: ➢ **No dissemination activities was planned or performed during the period.**

Beneficiary[43]:	SICS		
Work Package(s)	WP3 - SPD Node		
Task(s)	Task 3.1 Nano node Task 3.2 Micro/Personal node Task 3.3 Power node		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.1 Task 3.3 Task 3.3	1 PM 4 PM 2 PM	1 PM 12 PM 2 PM	50% 100% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Hypervisor development using the selected target platform (nano and micro/personal node) has continued with focus on secure boot integration (with T2Data), Global Platform support and above all a Linux port for the hypervisor. We have changed our efforts slightly and will put the majority of our work into the nano and particular micro/persona node development.
- We have started a pre-study for hypervisor protection in nano nodes according to the nSHIELD architecture using the ARM Cortex M family.

- **Task 3.1**
  - We continued to work on a previously developed (in house SICS) hypervisor that runs both on simulated hardware and real ARM hardware platforms, i.e. Beagleboard and Beaglebone.
  - We have started to investigate a tiny ARM platform in the Cortex M family and providing a hypervisor security layer for this platform. Development hardware has been purchased and a pre-study has been launched. There will be additional focus on this part the final nSHIELD project year.
- **Task 3.2**
  - We continued to work on a previously developed (in house SICS) hypervisor that runs both on simulated hardware and real ARM hardware platforms, i.e. Beagleboard and Beaglebone.
  - A secure boot design developed together with T2Data and we successfully showed secure boot of the SICS hypervisor and FreeRTOS on Beaglbone.
  - Hypervisor performance figures were collected for running Free RTOS on the hypervisor.
  - We managed to successfully port Linux to our hypervisor protected development boards (Beaglboard and Bealbone) in March. Then we have gradually improved the impl. and design adding functionality and features.
  - In co-operation with the nSHIELD partner SearchLab the hypervisor design and impl. was evaluated. The evaluations lead to the detection of a couple of impl. mistakes. These were corrected and an improved updated impl. was resent to SearchLAB for re-evaluation.
  - We have evaluated and designed Global Platform support on the Beaglebone. Core part of Global Platform was implemented and evaluated from performance perspective and the results are accepted for publication.
  - Extensive input was written to the Preliminary SPD Node Technologies Prototype (D3.2) report in time.
  - Extensive input was written to the Preliminary SPD Node Technologies Prototype Report (D3.3) report in

[43] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

time.

- Although, we are not formally part of WP6, we gave considerable input to D6.2 together with SearchLAB,
- First steps toward formally verifying the hypervisor were taken in co-operation with another project.

- **Task 3.3**
  - We assisted with looking into the power node requirements and system architecture design together with the rest of the nSHIELD partners.
  - We have looked into the newly released TPM 2.0 from TCG and evaluated how it could potential fit into the nSHIELD architecture.

Description of criticalities met during the period:

- Full Linux port to the hypervisor protected ARM Cortex A8 platform
- FreeRTOS benchmark figures
- Global Platform support and benchmarks for the hypervisor protected platform
- Security evaluation and corrective actions

Corrective actions:

- We are according to plan except for that less efforts have been put into TPM integration as we have put full focus on the hypervisor development. We will put some more effort into it the last project year.

Meetings performed during the period:

- nSHIELD face-to-face meeting in Budapest, September 11&12, 2012. Participants from SICS: Christian Gehrmann.
- nSHIELD review meeting in Rome, October 17&18, 2012. Participants from SICS: Christian Gehrmann and Viktor Do.
- nSHIELD specification working meeting, December 4, 2012. Participants from SICS: Christian Gehrmann
- nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24, 2013. Participants from SICS: Christian Gehrmann
- nSHIELD face to face meeting, Barcelona, March 6-5, 2013. Participants from SICS: Christian Gehrmann and Viktor Do.
- SICS arranged the nSHIELD face-to-face meeting in Stockholm, June 12-13, 2013. Participants from SICS: Christian Gehrmann and Viktor Do.

Deviations between actual and planned person-months:

- We had no deviations between actual and planned efforts in WP3 during the period.

Dissemination activities and exploitation perspectives:

- The status of the hypervisor design and development for ARM was presented at the SICS Security seminar in Lund, April: http://www.sics.se/events/sics-security-seminar-2013-future-trustworthy-it-systems
- The following papers were accepted for publication (SICS security lab members in bold):
  - **A. Vahidi** and C. Jämthagen, "Secure RPC in embedded systems - Evaluation of some GlobalPlatform implementation alternatives", to appear in 8th Workshop on Embedded Systems Security, Montreal, Canada, September, 2013.
  - M. Dam, R. Guanciale, N. Khakpour, H. Nemati and **O. Schwarz**, "Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel", to appear in 20th ACM Conference on Computer and Communications Security, Berlin, Germany, November, 2013.
- N. Khakpour, **O. Schwarz** and M. Dam, "Machine Assisted Proof of ARMv7 Instruction Level Isolation Properties", to appear in 3rd International Conference on Certified Programs and Proofs, Melbourne, Australia, December, 2013.

4.5.2 T2 Data AB T2D

Beneficiary[44]:	T2D		
Work Package(s)	WP2 - SPD metrics, requirements and system design		
Task(s)	Task 2.1 Multi-technology requirements & specification Task 2.3 Multi-technology architectural design		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1 Task 2.3	1 PM 2 PM	1 PM 2 PM	100% 100%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Before and after face-to-face meeting in Budapest, we was involved in the improvement of requirements handling of application scenarios related to nSHIELD platform.
- **Task 2.1**
  - Review and input to final requirement specification
- **Task 2.3**
  - Input to final architecture design.

Description of criticalities met during the period:

- The system requirements document quality secured and timely delivered before nSHIELD review meeting in October.
- Contribute to system architecture design.

Corrective actions:

- Dialogue with SICS regarding improvements of requirements.

Meetings performed during the period:

- nSHIELD face-to-face meeting in Budapest, September 11&12, 2012. Participants from T2D: Hans Thorsen
- nSHIELD review meeting in Rome, October 17&18, 2012. Participants from T2D: Hans Thorsen
- nSHIELD specification working meeting, December 4, 2012. Participants from T2D: Hans Thorsen
- nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24, 2013. Participants from T2D: Hans Thorsen
- nSHIELD face to face meeting, Barcelona, March 6-5, 2013. Participants from T2D: Hans Thorsen.
- Meeting in Stockholm, June 12-13, 2013. Participants from T2D: Hans Thorsen

Deviations between actual and planned person-months:

- We had no deviations between actual and planned efforts in WP2 during the period.

Dissemination activities and exploitation perspectives:

- No dissemination activities was planned or performed during the period.

[44] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Beneficiary[45]:	T2D		
Work Package(s)	WP3 - SPD Node		
Task(s)	Task 3.1 Nano node Task 3.2 Micro/Personal node Task 3.3 Power node		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.1 Task 3.2 Task 3.3	1 PM 6 PM 2 PM	1 PM 10 PM 2 PM	50% 50% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Secure Boot development using the selected target platform (nano and micro/personal node) has continued with focus on secure boot integration (with SICS). Shift from design to implementation with focus on the demonstrator later this year.

- **Task 3.1**
  - The SRAM memory available at power on is only 64 kb in Beagle Board , the initial platform (Beagle Bone) has 128 kb. The code have been redesigned , re-implemented to support both platforms.

- **Task 3.2**
  - Ported software developed for target of class Micro Node to Power Node. Reusable components such as VFAT file system and signature verification tested on both X86 and ARM architectures.
  - In co-operation with the nSHIELD partner SearchLab the Secure Boot design and impl. was evaluated. The evaluations lead to the detection of a couple of issues.
  - Contributed to Preliminary SPD Node Technologies Prototype (D3.2).
  - Contributed to Preliminary SPD Node Technologies Prototype Report (D3.3).

- **Task 3.3**
  - Jointly worked with other partners regarding power node requirements and system architecture design.

Description of criticalities met during the period:

- Designed and implemented VFAT file system with very low memory footprint.
- Integrated Secure Boot with SICS Hypervisor
- Configured simulator with SecureBoot and Hypervisor for evaluation by Search-Lab

Corrective actions:

- Postponed TPM integration
- Support for both Beagleboard and Beaglebone resulted in new design and implementation of filesystem, due to memory constraints.

[45] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Meetings performed during the period: ➢ nSHIELD face-to-face meeting in Budapest, September 11&12, 2012. Participants from T2D: Hans Thorsen ➢ nSHIELD review meeting in Rome, October 17&18, 2012. Participants from SICS: Hans Thorsen ➢ nSHIELD specification working meeting, December 4, 2012. Participants from T2D: Hans Thorsen ➢ nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24, 2013. Participants from T2D: Christian Gehrmann ➢ nSHIELD face to face meeting, Barcelona, March 6-5, 2013. Participants from T2D: Hans Thorsen ➢ Meeting in Stockholm, June 12-13, 2013. Participants from T2D: Hans Thorsen
Deviations between actual and planned person-months: ➢ We have put slightly more effort than planned into WP3 during the period to compensate for the slightly lower effort spent during first project year. We are now well aligned with original plan.
Dissemination activities and exploitation perspectives: ➢ No dissemination activities was planned or performed during the period.

4.5.3 Telcred TELC

Beneficiary[46]:	TELC		
Work Package(s)	WP3 – SPD Node		
Task(s)	Task 3.2 Micro node Task 3.5 Cryptographic technologies		
Period:	1st September 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.2 Task 3.5	0 PM 3 PM	0 PM 0.6 PM	30%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Task 3.2
  - The M.Sc. thesis investigating a model for delegated authorization was 99% completed by the student, but not yet defended and approved by the University (KTH).
  - Results: M.Sc. thesis (document)
- Task 3.5
  - Discussion with the involved partners, resulting in a shift of our focus and effort from evaluating cryptographic schemes in collaboration with UNIGE to implementing such in collaboration with ACCORDE.
  - Providing input and requirements to ACCORDE for a secure offline lock controller.

Description of criticalities met during the period:

- The task in 3.2 may have been a bit too complex for a student so the results will not be applicable "out of the box". Impact on other tasks should be negligible.
- Behind schedule due to a) shift of focus from evaluating cryptographic schemes in collaboration with UNIGE to implementing such in collaboration with ACCORDE, and b) now waiting for input from ACCORDE

Corrective actions:

- Adjustment of our own time plan for completion of 3.5. No impact on other WPs or tasks is foreseen.

Meetings performed during the period:

- Feb 24th meeting with SICS and T2D
- June 12-13: project meeting in Stockholm.

Deviations between actual and planned person-months:

- Task 3.2 No deviation
- Task 3.5: 1.5 PM less than planned due to reasons explained above.

Dissemination activities and exploitation perspectives:

- M.Sc. thesis produced (but not yet published).

[46] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

4.6 Hungary

4.6.1 Security Evaluation Analysis and Research Lab. S-LAB

Beneficiary[47]:	S-LAB		
Work Package(s)	WP2 - SPD METRICS, REQUIREMENTS, AND SYSTEM DESIGN WP3 - SPD NODE WP5 - SPD MIDDLEWARE & OVERLAY WP6 - PLATFORM INTEGRATION, VALIDATION AND DEMONSTRATION WP7 – SPD APPLICATIONS		
Task(s)	2.1 - Multi-technology requirements & specification 2.2 - Multi-technology SPD metrics 3.4 - Dependable self-x Technologies 3.5 - Cryptographic technologies 5.2 - Core SPD services 6.1 - Multi-Technology System Integration 6.2 - Multi-Technology Validation & Verification 6.3 - Lifecycle SPD Support 7.1 – Railway transportation 7.2 – Voice/Facial recognition 7.3 – Dependable Avionic System		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
WP2: T2.1; T2.2	**2,33 PM**	**2,27 PM**	**92%**
T2.1	**0,33**	0,31	95%
T2.2	**2**	1,96	100%
WP3: T3.4, T3.5	**3,85 PM**	**2,95 PM**	**79%**
T3.4	1,85	1,45	80%
T3.5	2	1,5	78%
WP5: T5.2	**11,06 PM**	**12,33 PM**	**82%**
WP6: T6.1; T6.3; T6.4	**12 PM**	**6,85 PM**	**29%**
T6.1	3	1,15	80%
T6.2	5	4	90%
T6.3	4	1,7	13%
WP7: T7.1; T7.2; T7.3; T7.4	**8,5 PM**	**2,53 PM**	**13%**
T7.1	4,5	2	60%
T7.3	4	0,53	105

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Tasks 2.1 and 2.2
  - Requirements, specification, and SPD metrics development work

  Results in D2.5 Preliminary SPD metrics specifications; D2.6 Final System Requirements and Specifications
- Tasks 3.4 and 3.5
  - Security evaluation methodology for partners' technologies: Work on security evaluation methodology for partners' contributions (Hypervisor for Trusted Execution Environment and Secure Boot)

[47] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

- Results: in D3.2 and D3.3 - Preliminary SPD Node Technologies Prototype, and Preliminary SPD Node Technologies Prototype Report

- Task 5.2
  - preliminary version of technologies for middleware core and innovative SPD services
  - prototype of Intrusion Detection Bundle
  - Preliminary SPD middleware and overlay technologies prototype development. Developed and interfaced a preliminary DDOS protection, and collected and edited the Middleware Interface report, provided contribution for the D5.3 Preliminary SPD middleware and Overlay technologies prototype Report.
  - Results: D5.2 and D5.3

Task 6.3 Lifecycle SPD Support
- Revision of D6.1 Lifecycle SPD Support Plan deliverable
- Planning of integration / validation activities
- Results: deliverable D6.1 Lifecycle SPD Support Plan

Task 6.2 Multi-Technology Validation & Verification
- Prototype validation and verification:
- Definition of validation and verification plan, description of node evaluation
- Results: deliverable D6.2- Prototype validation and verification plan- contribution to validation and verification of the Secure Boot, the Hypervisor and Intrusion Detection System for Middleware

Task 6.1 Multi-Technology System Integration
- Integration planning of the prototypes:
- Results in deliverable D6.3 –Prototype integration report

• Task 7.1, 7.2, 7.3, 7.4

Preliminary integration and validation plan, security validation and verification plan for partner's components; railway, avionic, facial recognition and social mobility scenarios(continuous work in progress).

Description of criticalities met during the period:

-

Corrective actions:

- Overall efforts- overall planned efforts are higher than actual spent for WP5, WP6 WP7 and WP8. According to revised planning less than 108MM would be consumed for the foreseen work to be completed.
  Forecast for effort spending: around 82-85% of all efforts might be spent by SLAB during the whole project. This could vary on the volume of work in WP6, WP7, and dissemination activities for WP8.

Meetings performed during the period:

- Bi-weekly Task Force conferences
- 11-12 September, 2012, Budapest workshop
- 18 October 2012- Annual review, Rome
- 19 December, 2012 – WP5 teleconference
- 16 January, 2013 – WP5 teleconference
- 6 February, 2013 – WP5 teleconference
- 14 February, 2013 – WP6 teleconference
- 6, March, 2013- Project meeting, Barcelona
- 3, April, 2013- WP7 teleconference
- 11, April, 2013- WP7 teleconference
- 10 June, 2013 – WP2 teleconference
- 12-13 June, 2013- Project meeting, Stockholm (Kista)
- 9 July, 2013- WP5 teleconference

Deviations between actual and planned person-months:

- Delays in WP6, WP7 caused spending less efforts then planned

Dissemination activities and exploitation perspectives:

Dissemination: Planned dissemination and organized workshop in Budapest, 11-12,09-2012
Planned participation on PECCS 2013, Lisbon special session for Measurable security for Embedded Computing and Communication Systems
Exploitation: Security evaluation for further partner prototypes; further development of Intrusion Detection System (DDOS protection component)

4.7 Greece

4.7.1 ATHENA Research and Innovation Centre ATHENA

Beneficiary[48]:	ATHENA		
Work Package(s)	WP3 - SPD Node WP4 - SPD Network WP5 SPD Middleware & Overlay WP6 SPD Middleware & Overlay		
Task(s)	Task 3.4 : Dependable self-x Technologies Task 3.5 : Cryptographic technologies Task 4.2 Distributed self-x models Task 5.2: Core SPD services Task 6.1 Multi-Technology System Integration Task 6.2 Multi-Technology Validation & Verification		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.4	1 PM	1 PM	40 %
Task 3.5	2 PM	2 PM	70 %
Task 4.2	5 PM	5 PM	60 %
Task 5.2	4 PM	4 PM	60 %
Task 6.1	3 PM	3 PM	15 %
Task 6.2	3 PM	3 PM	15 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

WP3

With respect to WP3 activities, ATHENA / Industrial Systems Institute is intended to put effort on certain items as they are presented below per task:

- T3.4
  Design of DDoS attacks defence mechanisms for the micro and power nodes (Ingress/Egress filtering, Packet Marking and logging, Self reconfiguration and sustainability)
- T3.5
  Design of a novel cryptographic key exchange algorithm (Controlled Randomness)

The effort put per task during M13-18 is as follows:

- T3.4
  Design and prototype implementation of the node reporting functions to support DDoS attacks mitigation mechanisms.
- T3.5
  Design and prototype implementation for the controlled randomness protocol on the micro and power nodes.

Relative contribution was provided to deliverables D3.2 and 3.3

WP4

- Task 4.2
  - A methodology to recognize and model denial-of-service attacks based on network traffic, power consumption and signal strength traffic was developed and is being simulated.

The developed algorithms are being simulated in the OMNET++ environment in order for them to be adapted to

[48] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

the prototype under development.

- Task 5.2

Development of software adapters based on SLP protocol implementations, for discovering and registering legacy services. SW adapter was modelled and tested

WP5

- Task 5.2

Development of software adapters based on SLP protocol implementations, for discovering and registering legacy services. SW adapter was modelled and tested

WP6

- Task 6.1 Multi-Technology System Integration
  - Definition of integration requirements and basic interfaces.
- Task 6.2 Multi-Technology Validation & Verification
  - Definition of and validation methodology for the following nSHIELD prototypes; Recognizing DoS attack prototype, Key Exchange Protocol prototype and Adaptation of Legacy System prototype.

Description of criticalities met during the period:

- N.A

Corrective actions:

- **N.A**

Meetings performed during the period:

- Rome, Italy : October 2012 : Review Meeting
- Budapest, Hungary: September 2012 : Plenary Meeting
- Project Meeting Barcelona March 2013
- Project Meeting Stockholm, June 2013
- Skype conference meetings with Work Package leaders in December 2012 and January 2013.

Deviations between actual and planned person-months:

- N.A.

Dissemination activities and exploitation perspectives:

- N.A.

4.7.2 Hellenic Aerospace Industry

Beneficiary[49]:	HAI		
Work Package(s)	WP1[50] - Project Management		
Task(s)	Task 1.1 - Project Management Task 1.2 - Liaisons		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1 Task 1.2	4 PM 1 PM	5 PM 1 PM	54 % 67 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 1.1**
  - HAI dedicated the aforementioned effort in task coordination activities, participation in meetings and contribution in the coordination of deliverables and work

Objectives: collaborating with other coordinators to ensure effective workflow in the project
Results: achieving critical milestones, producing high quality deliverables

- **Task 1.2**
  - Liaisons with on going thematically relative projects are attempted

Objectives: to enhance nSHIED dissemination and benefit from collaborative activities
Results: widening nSHIELD's technical development in technologies and scenarios

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

- nSHIELD project meeting, Budapest, September 2012
- nSHIELD project meeting, Barcelona, March 2013
- nSHIELD project meeting, Kista Sweden, June 2013
- Coordination of WP6 phone conferences on a regular and ad-hoc basis

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[49] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[50] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[51]:	HAI		
Work Package(s)	WP2[52] - SPD Metric, requirements and system design		
Task(s)	Task 2.1 - Multi-technology requirements & specification Task 2.2 - Multi-technology SPD metrics Task 2.3 - Multi-technology architectural design		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1	2 PM	2 PM	100 %
Task 2.2	1 PM	2 PM	60 %
Task 2.3	2 PM	2,5 PM	88 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 2.1**
  - Participation in D2.6
  - D2.6 review
  - D2.6, addition of requirements in Social mobility scenario, Network, Node and Middleware layers

Objectives: finalizing the requirements of the nSHIELD framework
Results: finalization of D2.6

- **Task 2.2**
  - Assessment of candidate SPD Metrics
  - Review of D2.5

Objectives: defining the SPD metrics composition of the nSHIELD framework
Results: finalization of D2.5

- **Task 2.3**
  - Coordination of D2.4 (finalization)
  - Definition of the methodology and design process
  - Proposal of an overall Architecture scheme
  - Description of Network Layer, through its logical view and functionalities
  - Report of open issues and focus points for the determination of Interfaces
  - Development and Deployment views for all layers
  - Definition of three types of devices, used as reference nodes
  - List of Interfaces
  - Assessment on scenarios and realization of applications

Objectives: defining the nSHIELD reference architecture
Results: finalization of D2.4 and initialization of D2.7 preparation, towards a final nSHIELD Architecture

Description of criticalities met during the period:

- The finalization of nSHIELD reference Architecture, conducted in the beginning of the reference period, was an achievement with implications and interactions throughout the project

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

- HAI's slight effort overspending (6,5 instead of planned 5) is due to a corresponding underspending during the first nSHIELD year (12 instead of planned 14)

Dissemination activities and exploitation perspectives:

- N.A

[51] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[52] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[53]:	HAI		
Work Package(s)	WP3[54] - SPD Node		
Task(s)	Task 3.4 – Dependable self-x technologies		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 3.4	2 PM	2 PM	50 %

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 3.4**
  - Research on TinyOS based nodes (IRIS, TelosB, MicaZ), on sensor resources (memory, CPU processing power), RF capabilities and different levels of node security (e.g. security in 802.15.4)

Objectives: refinement of described prototypes for D.3.2 and D3.3
Results: Assessment on candidate nSHIELD platform nodes and preparation of HAI's contribution in D3.4, D3.5

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[53] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[54] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[55]:	HAI		
Work Package(s)	WP4[56] - SPD Network		
Task(s)	Task 4.3 – Reputation-based resource management technologies Task 4.4 – Trusted and dependable connectivity		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 4.3 Task 4.4	5,5 PM 2 PM	9 PM 2 PM	83% 67%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 4.3**
  - Development of a trusted routing prototype based both on direct evidence and reputation for wireless sensor networks

Objectives: implementation of a trusted routing protocol, suitable for nSHIELD framework
Results: Implementation and evaluation of Trusted Greedy Perimeter Stateless Routing (T-GPSR) for TinyOS-based motes. This routing protocol using both direct evidence and reputation messages is able to counteract against several network layer attacks ensuring undisrupted routing operation

- **Task 4.4**
  - Research on TinyOS based nodes (IRIS, TelosB, MicaZ), on sensor resources (memory, CPU processing power), RF capabilities and different levels of node security (e.g. security in 802.15.4)

Objectives: refinement of described prototypes for D4.2 and D4.3
Results: Review and refinement of D4.2 and D4.3

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

- HAI used more than planned of its allocated T4.3 resources (9 pm instead of 5,5). Among the reasons are: less than planned effort was consumed during the previous periods and resource demanding trusted routing was implemented during second year (TinyOS code on sensors)

Dissemination activities and exploitation perspectives:

-

[55] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[56] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[57]:	HAI		
Work Package(s)	WP5[58] - SPD Middleware and Overlay		
Task(s)	Task 5.1 – SPD driven semantics Task 5.3 – Policy-based management Task 5.4 – Overlay monitoring and reacting system by security agents		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 5.1 Task 5.3 Task 5.4	2 PM 5 PM 2 PM	1,5 PM 6 PM 1,5 PM	25% 43% 25%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 5.1**
  - HAI conducted an assessment on UML diagrams, candidates for the nSHIELD semantic model

Objectives: contribution in the design of nSHIELD semantic technologies
Results: work is in progress

- **Task 5.3**
  - HAI coordinated the work that has to be undertaken for the development of the corresponding components for a working prototype to demonstrate a policy-based management solution on embedded systems. Emphasis has been given on the achievement of a common understanding about the solution and the mechanisms chosen (e.g. operating system, infrastructure, interfaces) to ensure the required interoperability among stakeholders
  - HAI contributed to the finalization of the description of a policy-based management solution and the mechanisms that comprise it
  - HAI collaborated with other partners regarding the platforms chosen to demonstrate this solution

Objectives: planning of policy-based management solution
Results: outline of policy-based management scheme

- **Task 5.4**
  - HAI has started working on the multi-layered Overlay Security Agent, in the direction of the design of abstracted and open user services

Objectives: contribution in the design of Security Agents and Overlay monitoring system
Results: work is in progress

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[57] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[58] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[59]:	HAI		
Work Package(s)	WP6[60] - Platform Integration, validation & demonstration		
Task(s)	Task 6.1 – Multi-Technology System Integration Task 6.2 – Multi-Technology Validation & Verification Task 6.3 – Lifecycle SPD Support		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 6.1 Task 6.2 Task 6.3	9 PM 4 PM 3,5 PM	9 PM 4 PM 3 PM	50% 50% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 6.1**
  - Coordination of D6.3
  - Definition of integration methodology and framework

Objectives: integrating components and prototypes developed in WP3, WP4 and WP5
Results: structure of integration methodology, based on the involvement of individual prototypes in each scenario

- **Task 6.2**
  - Contribution in Network verification covering requirements-prototypes-verification
  - Verification procedure and tests validating the proposed Reputation-based schemes

Objectives: Plans and conducts the validation and verification of the implemented solution
Results: Tests for trusted routing, proposal of testing format and techniques

- **Task 6.3**
  - Forming SPD lifecycle procedures for nSHIELD, based mainly on the international standard ISO/IEC 12207

Objectives: developing a feasible lifecycle support plan
Results: finalization of D6.1

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

- nSHIELD project meeting, Budapest, September 2012
- nSHIELD project meeting, Barcelona, March 2013
- nSHIELD project meeting, Kista Sweden, June 2013
- Coordination of WP6 phone conferences on a regular and ad-hoc basis

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[59] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[60] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[61]:	HAI		
Work Package(s)	WP7[62] - SPD Applications		
Task(s)	Task 7.1 – Railways security Task 7.3 – Dependable Avionic System Task 7.4 – Social mobility		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 7.1 Task 7.3 Task 7.4	3 PM 1 PM 3 PM	5 PM 0,5 PM 3 PM	50% 17% 30%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 7.1**
  - Contribution in D7.1
  - Description of reputation-based secure routing, implemented on islands of smart sensors in the Railway scenario
  - HAI's team is working on a railway sub-scenario proposal, to complement one of the already described scenarios or to be a separate use case

Objectives: participation in developing a coherent railway scenario in order to prove nSHIELD prototypes
Results: participation in the finalization of D7.1

- **Task 7.3**
  - Following the development of Avionic scenario
  - Explore the integration aspects of the scenario (link with T6.1)

Objectives: participation to the work of developing a coherent avionic scenario in order to prove nSHIELD prototypes
Results: Reviewing D7.3

- **Task 7.4**
  - Smart city applications case study
  - Processing of application domains in social mobility framework (traffic control, energy management, security & safety)

Objectives: assisting in developing a coherent social mobility and networking scenario in order to prove nSHIELD prototypes
Results: Preparation of D7.4

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[61] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[62] x is 1, 2, 3, 4, 5, 6, and 7

Beneficiary[63]:	HAI		
Work Package(s)	WP8[64] - Knowledge exchange and industrial validation		
Task(s)	Task 8.1 – Dissemination Task 8.3 – Exploitation		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 8.1 Task 8.3	1 PM 2 PM	1 PM 2 PM	50% 50%

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- **Task 8.1**
  - Dissemination activities carried out in cross European projects

Objectives: disseminating nSHIELD results through all available channels

Results: Execution of dissemination plan

- **Task 8.3**
  - Forming and describing the verification and testing plan for the first version of nSHIELD operational manual

Objectives: contribute in nSHIELD operational manual

Results: First version of operational manual is delivered (D8.4)

Description of criticalities met during the period:

-

Corrective actions:

-

Meetings performed during the period:

-

Deviations between actual and planned person-months:

-

Dissemination activities and exploitation perspectives:

-

[63] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

[64] x is 1, 2, 3, 4, 5, 6, and 7

4.7.3 Integrated Systems Development ISD

Beneficiary[65]:	ISD		
Work Package(s)	WP1 - Project Management WP3 - SPD Node WP6 - Platform integration, validation & demonstration WP7 - SPD Applications		
Task(s)	Task 1.1 Project management Task 3.3 Power node Task 6.1 Multi-Technology System Integration Task 7.1 Railways security Task 7.2 Voice / facial recognition Task 7.4 Social mobility		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 1.1	1 PM	1 PM	50%
Task 3.3	24 PM	26 PM	55%
Task 6.1	0. PM	0. PM	0%
Task 7.1	0. PM	0. PM	0%
Task 7.2	0. PM	0. PM	0%
Task 7.4	0. PM	0. PM	0%
Description of the activities carried out during the period to reach specific objectives within the task/WP: ➢ ISD has completed the design of a novel audio based surveillance system in accordance to the technical annex and is proceeding with the implementation. The system consists of three types of boards, with the first one already manufactured and debugged and the second one manufactured and under debugging. More information can be found in the relevant section of D3.2.			
Description of criticalities met during the period: ➢ N/A			
Corrective actions: ➢ N/A			
Meetings performed during the period: ➢ 11/09 – 12/09 Project meeting in Budapest. ➢ 17/10 – 18/10 Annual project review in Rome. ➢ 05/12 Conference call regarding M18 deliverables. ➢ 23/01 Task force conference call. ➢ 13/02 Task force conference call. ➢ 27/02 Task force conference call. ➢ 27/06 Consortium conference call regarding deliverables.			
Deviations between actual and planned person-months: ➢ N/A			
Dissemination activities and exploitation perspectives: ➢ N/A			

[65] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

4.7.4 Technical University of Crete TUC

Beneficiary[66]:	TUC		
Work Package(s)	WP2 – SPD METRICS, REQUIREMENTS AND SYSTEM DESIGN WP3 – SPD NODE WP4 – SPD Network WP5 – SPD Middleware & Overlay WP7 – SPD Applications WP8 – Knowledge exchange and industrial validation		
Task(s)	Task 2.1 – Multi-technology requirements & specification Task 2.2 – Multi-technology SPD metrics Task 3.1 – Nano node Task 3.2 – Micro/Personal node Task 3.4 – Dependable self-x Technologies Task 3.5 – Cryptographic technologies Task 4.3 – Reputation-based resource management technologies Task 4.4 – Trusted and dependable Connectivity Task 5.2 – Core SPD services Task 5.3 – Policy-based management Task 7.2 – Voice/Facial recognition Task 7.4 – Social Mobility Networking Task 8.1 – Dissemination		
Period:	1st Sept 2012 – 31st August 2013		
Task (s)	**Effort planned in this period:**	**Effort actual or spent in this period:**	**% of work completed at the end of the period (indicative):**
Task 2.1	1.2 PM	1.2 PM	100 %
Task 2.2	1.3 PM	1.3 PM	100 %
Task 3.1	2.4 PM	2.4 PM	100 %
Task 3.2	2.4 PM	2.4 PM	100 %
Task 3.4	2.4 PM	2.4 PM	100 %
Task 3.5	5.6 PM	5.6 PM	100 %
Task 4.3	2.4 PM	2.4 PM	100 %
Task 4.4	3.2 PM	3.2 PM	100 %
Task 5.2	4.0 PM	4.0 PM	100 %
Task 5.3	3.2 PM	3.2 PM	100 %
Task 7.2	1.2 PM	1.2 PM	100 %
Task 7.4	1.2 PM	1.2 PM	100 %
Task 8.1	1.9 PM	1.9 PM	100 %

[66] This report is per Beneficiary, and has to be provided for each WP in which it is involved each Beneficiary

Description of the activities carried out during the period to reach specific objectives within the task/WP:

- Task 2.1
  - The system's requirements were revisited considering the peculiarities of the four scenarios and several enhancements were proposed. A mapping regarding the predefined requirements and the corresponding prototypes developed by TUC was also performed.
- Task 2.2
  - Proposal of a novel dynamic and applicable formal methodology for evaluating the SPD composed metric. The new approach supports a dynamic choreographed modelling scheme.
- Task 3.1
  - Design of a smartcard authentication protocol based on symmetric keys, able to work on any TPM. The scheme has been implemented and tested in a LAN. We have looked into integrating the smart card module into BeagleBones, so as to integrate it in the TUN interface described in WP5.
- Task 3.2
  - Implementation of a compact crypto library in C, for a subset of lightweight ciphers and compact implementations of standard ciphers.
- Task 3.4
  - An anonymizer component based on the k-anonymity concept has been developed for nSHIELD applications, where personal location privacy is to be preserved, while enabling the system to provide location monitoring services.
  - Implementation of the Gossamer protocol for automatic access control functionality.
  - Contribution to D3.1 (SPD node technologies assessment) in Section 6 (Dependable self-x Technologies).
- Task 3.5
  - Investigated secure protocols and methods for establishing cryptographic keys among communicating parties, using Identity Based Cryptography. One such scheme has partially been implemented.
  - Contribution to D3.2 in section 6.4 (An Identity-Based Encryption scheme)
  - Contribution to D3.3 in section 6.3 (Identity-Based Encryption)
  - Development of a lightweight, efficient, GPU accelerated hashing and hash lookup mechanism utilizing the CUDA GPGPU toolkit. Significant speed-ups have been achieved.
- Task 4.3
  - We design and implement a prototype of a novel modular and configurable reputation and trust-based system for secure routing and intrusion detection. The prototype was implemented in ns-2 simulator, in C++ language. The system extends the routing protocol DSR.
  - Contribution to D4.2 in sections 4.2 (Reputation based Secure Routing) and 4.3 (nSHIELD Reputation scheme)
  - Contribution to D4.3 in sections 4.2 (Reputation based Secure Routing) and 4.3 (nSHIELD Reputation scheme).
- Task 4.4
  - A protocol that secures nShield exchanged messages at the network layer, extending the standardized IPSEC protocol and adapting it to the restricted environment of sensor nodes, was finalized and developed for specific platform (Contiki). The performance results demonstrate that this solution is a strong candidate for protecting communications, while providing additional benefits compared to other mechanisms working at other layers of the TCP/IP communication stack.
  - Contribution to D4.2 in section 5.2 (Secure communication protocols on the network layer).
  - Contribution to D4.3 in section 5.2 (Secure communication protocols on the network layer).
- Task 5.2
  - Work on the implementation of the OSGi-DPWS interface, to allow interoperability between the nSHIELD architecture and the DPWS-compliant policy-based management infrastructure developed by TUC in T5.3. Appropriate technologies were identified and successfully integrated into existing nSHIELD OSGi framework (Knopflerfish).
  - Collaborated with partners to identify and address interoperability issues between interfaces and

between said interfaces and the nSHIELD platform. Also collaborated with partners to indentify common ground and facilitate cooperation at later stages (namely integration and demonstration).
    - Multi-layered Overlay Security: We design and build a secure overlay solution that is transparent to end "application". The current version implements a threshold DoS detection mechanism. The current code basis will be provided as open source in order to be re-used as open source solution. We discuss with other partners opportunities for integrating this approach with the OSGi framework.
- Task 5.3
    - The basic framework for controlling access to nShield's resources based on well-defined policies has been finalised and the prototype has been developed. It facilitates the deployment of a dynamic authorization model depending on the system's owner needs. Several enhancements are already undertaken to provide a robust solution. All the interfaces have been defined to deploy the distinct functional components on nShield nodes.
- Task 8.1
    - One paper has been published in conference proceedings (PCI 2012) and another three have been accepted for inclusion in conference proceedings (MobiWac 2013, SETOP 2013, Wireless Days 2013). Four more papers have been submitted to the IEEE International Conference on Communications (ICC 2014) and one paper has been submitted for journal publication (ACM TECS).

Description of criticalities met during the period:

➢

Corrective actions:

➢

Meetings performed during the period:

- 2012-09-03: Skype conference among TUC members
- 2012-09-17: Skype conference among TUC members
- 2012-09-25: Skype conference among TUC members
- 2012-10-22: Skype conference among TUC members
- 2012-11-21: WP4 PhC
- 2012-11-22: Skype conference among TUC members
- 2012-12-10: Skype conference among TUC members
- 2012-12-19: WP5 PhC
- 2012-01-16: WP5 PhC
- 2013-01-17: Skype conference among TUC members
- 2013-02-06: WP5 PhC, D5.2, D5.3
- 2013-02-14: Skype conference among TUC members
- 2013-04-12: WP5 PhC
- 2013-05-13: WP4 PhC (Part 1)
- 2013-05-14: WP4 PhC (Part 2)
- 2013-06-10: Skype conference among TUC members
- 2013-06-20: Skype conference about Train scenario – TUC, Francisco Flamminy, Mariana Esposito
- 2013-07-01: Skype conference about Voice Recognition scenario – TUC, Xilinx (Paolo Azzoni)
- 2013-07-08: WP5 PhC, D5.2, D5.3
- 2013-07-10: WP2 PhC

Deviations between actual and planned person-months:

➢

Dissemination activities and exploitation perspectives:

- Journal Articles:
    - Embedded Systems Security: A Survey of Research Efforts in the EU
      Manifavas, C.; Fysarakis, K.; Papanikolaou, A.; Papaefstathiou, I.
      ACM Transactions on Embedded Computing Systems (TECS)
      Submitted.
- Conference proceedings

- Policy-based Access Control for Body Sensor Nodes
  Manifavas, C.; Rantos, K.; Fysarakis, K.; Papaefstathiou, I.
  IEEE International Conference on Communications (ICC), Sydney, Australia, 10-14 June 2014.
  Submitted.

- CasperCommunity: A Lightweight Anonymity & Location Privacy Service
  Fysarakis, K.; Adamopoulos, A.; Manifavas, C.; Papaefstathiou, I.
  IEEE International Conference on Communications (ICC), Sydney, Australia, 10-14 June 2014.
  Submitted.

- Integrated Hardware Implementation of PRESENT and SPONGENT
  Hatzivasilis, G.; Floros, G.; Manifavas, C.; Papaefstathiou, I.
  IEEE International Conference on Communications (ICC 2014), Communications and Information Systems Security Symposium (CISS), Sydney Australia, 10-14 June 2014. Submitted.

- ModConTR: A modular and configurable trust and reputation-based system for secure routing in ad hoc networks
  Hatzivasilis, G.; Papaefstathiou, I.; Manifavas, C.
  IEEE International Conference on Communications (ICC 2014), Ad Hoc and Sensor Networking Symposium (AHSNS), Sydney Australia, 10-14 June 2014. Submitted.

- IPsec over IEEE 802.15.4 for Low Power and Lossy Networks
  Rantos, K.; Papanikolaou, A.; Manifavas, C.
  ACM 11th Int. Symposium on Mobility Management and Wireless Access (MOBIWAC 2013), Barcelona, Spain, 3-8 Nov. 2013.
  Accepted for publication.

- IPv6 Security for Low Power and Lossy Networks
  Rantos, K.; Papanikolaou, A.; Manifavas, C.; Papaefstathiou, I.
  IEEE/IFIP Wireless Days 2013, Valencia, Spain, 13-15 Nov. 2013.
  Accepted for publication.

- Lightweight Cryptography for Embedded Systems – A Comparative Analysis
  Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Rantos, K.
  6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), Egham, U.K., 12-13 Sep. 2013.
  Accepted for publication.

- Building Trust in Ad hoc Distributed Resource-sharing Networks Using Reputation-based Systems
  Hatzivasilis, G.; Manifavas, C.
  In 16th Panhellenic Conference on Informatics with international participation (PCI 2012), University of Piraeus, Greece, 5-7 October, 2012.
  Digital Object Identifier: 10.1109/PCi.2012.28
  Publication Year: 2012, Page(s): 416 – 421

5 Deliverables and milestones tables

5.1 Deliverables

TABLE 1. DELIVERABLES

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I (proj month)	Delivered Yes/No	Actual / Forecast delivery date	Comments
D1.2	Quality Control Guidelines	1	SES	R	R/PP	3	Yes	August 2013	The deliverable has been rejected by the reviewer. Second issue provided by the second year of activity.
D8.4	nSHIELD run-through v1	8	MGEP	R	PU	12	Not	December 2013	Delayed from Y1
D1.6	Quality Control Report 1	1	SES	R	PU	15	Yes	September 2013	The delay is due to the delay of D1.2
D1.7	Periodic Management Report	1	SES	R	PP	18	Yes	April 2013	
D3.2	Preliminary SPD node technologies prototype	3	ISD	P,O	RE	18	Yes	April 2013	
D3.3	Preliminary SPD node technologies prototype report	3	ISD	R	PU	18	Yes	April 2013	

D4.2	Preliminary SPD network technologies prototype	4	SES	P,O	RE	18	Yes	February 2013	
D4.3	Preliminary SPD network technologies prototype report	4	SES	R	PU	18	Yes	February 2013	
D5.2	Preliminary SPD middleware and overlay technologies prototype	5	UNIROMA1	P,O	RE	18	Yes	June 2013	
D5.3	Preliminary SPD middleware and overlay technologies prototype report	5	SES	R	PU	18	Yes	June 2013	
D6.1	Lifecycle and SPD Support Plan	6	TECNALIA	R	CO	18	Yes	March 2013	
D6.2	Prototype validation and verification	6	SES	R	RE	20	Yes	April 2013	
D6.3	Prototype integration report	6	HAI	R	RE	22	Yes	October 2013	Part of the delay is due the necessity to wait for the developments of all other “technical” documents.
D7.1	Railways security demonstrator – integration and validation plan	7	ASTS	R	CO	22	Yes	June 2013	
D7.2	Voice/Facial Recognition demonstrator – integration and	7	ETH	R	CO	22		June 2013	

	validation plan								
D7.3	Dependable Avionic Systems demonstrator – integration and validation plan	7	SES	R	CO	22		June 2013	
D7.4	Social Mobility and Networking - integration and validation plan	7	MAS	R	CO	22	Not	December 2013	Delayed
D1.8	Periodic annual Report	1	SES	R	PP	24	Yes	September 2013	
D2.6	Final System Requirements and Specifications	2	TECNALIA	R	PU	24	Yes	August 2013	
D8.5	Preliminary Exploitation Plan	8	ISL	R	PP	24	Yes	August 2013	
D8.6	nSHIELD run-through v2	8	MGEP	R	PU	24	Not	Delayed from Y2	As a consequence of the delay on D8.4, D8.6 has also been delayed as it should be an upgraded version of D8.4. Delivering them so close in time makes no sense.

Table 8 Deliverables

The D0.0 Acronym list is updated every time new acronyms need to be explained .

5.2 Milestones

TABLE 2. MILESTONES							
Milestone no.	**Milestone name**	**Work package no**	**Lead beneficiary**	**Delivery date from Annex I**	**Achieved Yes/No**	**Actual / Forecast achievement date**	**Comments**
M3	Preliminary composable SPD prototypes	WP3,WP4,WP5	ISD	M18	Yes		D3.3, D4.3, D5.3
M4	Preliminary Integrated Platform	WP6	SES	M22	Yes		D6.3
M5	Final System Requirements and Specification	WP2	SES	M24	Yes		D2.6

Table 9 Milestones

6 Project management

6.1 Consortium management tasks and achievements

The management structure and tasks are defined in details in the Consortium Agreement. All partners are included within that agreement according to the management structure described in the Technical Annex. In particular financial and technical actions were planned, the meetings and phone conferences (described below) of appropriate level were scheduled, the technical description of the work and the Consortium Agreement were maintained, the electronic media were maintained including website, collaborative tools, document repository and e-mail list. Contact and exchange of information between partners was provided on daily basis by means of email, phone calls and mail. In frame of consortium management tasks the role of project coordinator who is a contact point with JU was maintained.

6.2 Encountered problems

Selex ES role

Selex ES will continue taking care of the technical part of project coordination as Selex Galileo merging company.

All the actions necessary to manage the expiring of the two companies, Selex SG and Selex ES, have been completed. The activities concerning the new merging company are running rightly, after a short period of transition.

THYIA new commitment

Due to company restructuring and some concerns with national funding authority, the partner THYIA is no longer able to confirm its commitment for the prosecution of the SHIELD project, as originally declared in the technical annex.

So, a new and reduced involvement of THYIA has been agreed with a reduced amount of MM effort, from M18 to M36. By doing so, the remaining MMs of THYIA is set to 16 MM. THYIA remains as a member of the consortium up to the project end and will work for benefit of the consortium and its success, putting in first place interest of the consortium and the obligations that must be fulfilled. THYIA will work proactively with the consortium up to the end without any risk for the results that must be achieved.

The lack of contributions by THYIA from now on doesn't compromise the quality of the results, since overlapping/redundant knowledge and competences can be found in the rest of consortium as indicated in the Technical Annex and in D1.2 (risk management approach).

T7.4 descoping

In order to minimize the impact of THYIA effort reduction on project activities (whose major involvement was in scenario n°4), it is proposed to remove the demonstration activities (demonstration campaign) foreseen for the scenario n°4 (T7.3), so that the "saved" MM will balance the ones that THYIA will not spend for the rest of the project. The remaining (minor) effort of other partners involved in such scenario will be used to perform feasibility/high level analysis about the potential application of the SHIELD platform in the Social Mobility Environment

It is envisaged that the absence of a 4th demonstration campaign will not compromise the project objectives verification, since the Embedded Systems domain is well represented by the Avionic, Railways

and Face Recognition scenarios, that assure the full coverage of requirements V&V and the industrial impact (see validation and verification documents as well as risk mitigation in the Technical Annex).

Action on D8.4 (Build Secure Embedded Systems with nSHIELD v1)

Despite the plan of delivering the first version of the operational report being Deliverable D8.4 in Month 12, this deliverable is substantially delayed. The reason is that both the concept of "composable security" and the methodology where not clearly enough elaborated to be presented in a report. The final delay is caused by the delivery owner being Josef Noll of Movation, who discussed the concept both with supplier industries like ABB and with application organizations like Norwegian Oil and Gas, representing all oil and gas companies working on the Norwegian shelf. Both suppliers commented that composable security is very ambitious, and that they would recommend to focus on measurable security. Thus, we reconsidered our approach, and will provide D8.4 with the focus on measurable security and the ways how industry can adopt to it, while D8.6 will then provide the extension towards the SHIELD approach.

Action on D8.6 (Build Secure Embedded Systems with nSHIELD v2)

This deliverable has caused considerable controversy within the consortium as it is considered a key deliverable for dissemination but also for a common understanding of the project and objectives. It is planned to be a short and direct document aiming non-technical audience where the necessity of security in embedded systems must be clear and also how adopting the SHIELD approach can help designing SPD compliant embedded systems.
Due to this internal discussion, the deliverable has been delayed but this had no impact in other tasks.
To solve this issue a general agreement is needed and a Task Force team has been created to manage it. Although first Task Force meetings were inconclusive a final decision was made during the plenary meeting in Barcelona (March 2013) concluding with the structure of the deliverable.
As a consequence, D8.6 has also been delayed as it should be an upgraded version of D8.4 and delivering them so close in time makes no sense. These delay has no impact on the technical WPs.

6.3 Changes in the consortium

6.3.1 Selex ES

A new centre of excellence combining Selex Galileo and Selex Elsag was created the 1st of January 2013. Selex Galileo S.p.A. and Selex Elsag S.p.A (the merged companies) were merged into Selex ES S.p.A. (the merging company). Selex ES S.p.A. is wholly owned by Finmeccanica – Società per azioni.

The merging company, by operation of law, has succeeded the merged companies in all rights, obligations and contracts. Therefore the merging company shall carry out, and comply with, all contractual obligations of the merged companies, still in force at the date of January 1st, 2013, in accordance with their terms and conditions. Conversely, any commitment, obligation, debt, contract of whoever towards the merged companies, still in force or due at the date of January 1st, 2013, shall be carried out or settled in favour of the merging company, in accordance with their terms and conditions.

The complete procedure has been accomplished and the information updated on the Participant Portal.

The people already involved in the project remain unchanged with the exception of the contact point that is changed at the end of January.

The activities, split in two separated part before the merging (Selex Galileo and Selex Elsag from the 1st of September to the 31st of December) in the D1.7, have been merged in this document; no grant has

been requested or paid till now and the financial reporting for the whole project duration will be presented by Selex ES. Selex ES is the "new" entity that assumes universally all rights and obligations of the two old legal entities, and the two "old" beneficiaries disappear as in the “Universal Transfer of Rights and Obligations”.

6.3.2 Alfatroll

Alfatroll is formally part of the consortium from January 2013. Alfatroll will cover the effort and the activities of ESIS and NOOM from January 2013 to the end of the project.

6.3.3 Seek and Find (SknFnd)

Seek and Find joined the consortium as of August 2013 in order to strengthen the contribution to the Social Mobility use case. Their embedded SIM is seen as a key technology both enabling communication and allowing update of security features (“composable security”) in a *more secure* way.

6.4 Project meetings

Several project meetings were held during the second year of activities. Several meetings were face-to-face meeting among a limited numbers of partners and finalized to specific activities, see Fig. 1.

PreReview-17Oct2012	17 October 2012	Rome, Finmeccanica	Pre-Meeting Annual Review
Project Meeting Budapest, Sept. 2012.	11 September 2012	Budapest	Project meeting

Alfatroll-Movation	28 January 2013	UNIK	WP7
Annual Review	18 October 2012	Rome	Periodic annual project review

Project Meeting Barcelona 2013	6 March 2013	Barcelona	Project Meeting

TMC meeting 14Jun2013	15 June 2013	Kista/Stockholm	TMC meeting
Project Meeting Stockholm, June12-13	13 June 2013	Stockholm	Project meeting
Stockholm Admin Session	13 June 2013	Stockholm	Administrative session
TMC Mar2013	6 March 2013	Barcelona	TMC meeting

T7.3 working group meeting	4 July 2013	SES-Nerviano Italy	Task 7.3 Avionic Demonstrator
Meeting-SknFnd	1 July 2013	Oslo	WP7 meeting

Figure 1 Project and working group meetings

Minutes of Meeting, Agendas and details are provided on wiki

http://nshield.unik.no/wiki/NSHIELD#Meetings.

The first Annual Review meeting is not described in this document.

6.4.1 Meeting in Budapest (September 2012)

The two days meeting was an internal project review meeting with 21 partners of the Consortium represented by 27 participants.

Scope of the meeting was the analysis of the requirements, including the nSHIELD architecture at node, network and middle ware overlay layer level. Topic for Lessons Learned section of the Review were discussed and assigned to the partners.

During the TMC meeting, TA amendments n.#19, #20,#21, #22, #23, #24 and #25 were analysed and approved

6.4.2 Meeting in Barcelona (March 2013)

The two days meeting was an internal project review meeting with 20 partners of the Consortium represented by 31 participants. One TMC meeting was held in the early morning of the second day.

Topics of the meeting were the analysis of the use of "Formal methods in nSHIELD", the overview of the four scenarios and the way to integrate demonstrators and prototypes. WPs open issues, status of deliverables, look ahead and management activities were also carried out.

During the TMC meeting, TA amendments n. #28, #29 and #30 were analysed and approved.

6.4.3 Meeting in Stockholm (June 2013)

The two days meeting was an internal project review meeting with 17 partners of the Consortium represented by 27 participants. One TMC meeting was held in the early morning of the second day.

The second day of the meeting Antonio Vecchio, ARTEMIS officer, was present for the Administrative section.

Technical section

The SPD functionalities through metric, multi-single metric approach, were evaluated. The complete list of prototypes, provided by the partners, was fixed. In particular, the prototypes involved in the Avionic Scenario were identified. Similar job was recommended to be repeated for the remaining scenarios. The participants discussed the approach to be used to demonstrate the "measurable security" by the proposed demonstrator. Contribution from the responsible of the demonstrator were analysed.

It was agreed a review meeting preparation for the 14th of November at SES premises of Florence (Campi Bisenzio).

During the TMC meeting, TA amendments n. #31, #32 and #33 were analysed and approved.

Administrative section (second day)

The involvement of THYIA in the project was analysed and discussed. Actions on the way to proceed were agreed. The Minute of Meeting is on Wiki
http://nshield.unik.no/wiki/File:Stockholm_nSHIELD_Administrative_Session_MoM.pdf

The date for the 2nd annual Review was preliminarily established for the 15th of November at SES premises of Florence (Campi Bisenzio).

6.4.4 Phone Conference

According to the open issue n14 (First Review Report) a Task Force has been instituted to improve a better coordination among WPs. All the WPs leader and technical experts are part of the Task Force.

- Task Force meetings were held every fifteen days until January and then at least once a month
- TMC meetings were periodically held any time a set of amendments was collected
- Meetings related to Work Packages activities were held via Phone Conferences
- Coordination and management meeting have been organized periodically depending on the activities.

Minutes of Meetings as well as corresponding documents are stored at the project official repository and Collaborative Tool at the nSHIELD website

http://nshield.unik.no/wiki/NSHIELD#Phone_Conferences.

7.1-7.2-7.3 demonstrators deliverable	2013-07-12T14:00:00	Webex+phone call
WP2 conference call 10/06/2013	2013-07-10T11:00:00	10-07-13
WP5 Skype conference call	2013-07-08T17:00:00	Skype
PhoneConf ARTEMIS-JU	2013-07-03T00:10:00	Office phone
PL-phoneconf-1Jul2013	2013-07-01T11:00:00	office phone
Doc status 2nd Webex	2013-06-27T14:00:00	Webex
Doc Status	2013-06-25T10:00:00	Webex
WP7 T7.3 Avionic Scenario	2013-06-04T22:00:00	Webex
WP4 - T4.3 consolidation	2013-05-20T10:00:00	Skype
WP4 periodic group meeting	2013-05-13T14:00:00	Skype
TMC-7May2013	2013-05-07T10:00:00	phone & Webex
PLC-phone-19Apr2013	2013-04-19T14:00:00	office phone
T7.3 Avionic Scenario - 2nd Webex	2013-04-11T14:30:00	see details
T7.3 Avionic Scenario - Webex	2013-04-03T14:30:00	see details
D8.4 phone 27Mar2013	2013-03-27T10:00:00	+47 21523999, 8776#, 236#
TMC meeting	2013-03-25T14:00:00	see list 3948369#
PLC-phone regarding TA	2013-03-20T11:00:00	office phone
PL-conf-1Mar2013	2013-03-01T13:30:00	office phone
TaskForce-27Feb2013	2013-02-27T14:00:00	see list ... 3948369#
WP6-phone-14Feb2013	2013-02-14T11:00:00	+39 010 9165954
TaskForce-13Feb2013	2013-02-13T14:00:00	see list ... 3948369#
PL-consultations-25Jan2013	2013-01-25T13:45:00	office phone
Task Force 2013.01.23	2013-01-23T14:30:00	skype
WP5 2013 01 16	2013-01-16T10:00:00	Skype
Task Force 2013.01.09	2013-01-09T14:30:00	skype
Task Force 2012.12.19	2012-12-19T11:00:00	skype
WP5 2012 12 19	2012-12-19T10:00:00	Skype
WP5 Middleware	2012-12-19T10:00:00	Skype
Task Force 2012.11.28	2012-11-28T14:30:00	skype

Figure 2 Project, TMC and WPs phone conferences

6.5 Project planning and status

Activities from M24 are not affected from any relevant delay. The plan described in the Technical Annex can be considered valid and do not need to change at the moment (M24).

Some deliverables required more participation from partners and they have been delivered in their final version with a slight delay. All the partners agreed and no objections were raised. However this delay has not impacted the project. At M24 all the 18 planned deliverables are submitted and ready to be uploaded on NEF, with exception for D8.4, see Para 6.2. So, the major deviation is related to the deliverable D8.4: “SHIELD run-through” (previously known as D8.4: “SHIELD run-through v1”).

WP2, WP3, WP4, WP5, WP6 and WP8 convergence to objectives are in line with the project and with each WPs objective.

The official starting date of WP7 is March 2013. Most of the partners have started activities to ensure that the envisaged applications are in line with the technology developments in nSHIELD. Although the change of partners in Slovenia and Norway was unexpected, the contributions to the use-cases has been reconsidered and the the WP could be intended on line.

The two Norwegian partners that left the project at the end of the first year, were replaced by two new Norwegian partners, maintaining the same national budget.

The new commitment of THYIA, see Para. 6.2, induces a reduction of the total budget of the project. This because it hasn't been possible to find a new Slovenian partner asking to join to project in order to substitute THYIA in the some activities.

6.6 Impact of deviations

After two years most part of the activities are running on track, with no major deviations and no negative impacts on the project. The actual delays have been recovered with proper corrective actions.

6.7 Changes to the legal status

Selex Galileo and Selex Elsag joined and changed their official name to Selex ES. Selex ES assumes universally all rights and obligations of the old legal entities.

6.8 Project website

nSHIELD project website is still available at address:

http://www.newshield.eu

It contains general project information, public deliverables, and is used for information, news and promotion of the project. The service is provided by Mondragon.

Collaborative Tool and Document Repository are still available at address:

http://nshield.unik.no

The access to repository is limited to authorized persons only. Semantic Media Wiki service is used by consortium for collaboration and day-to-day work and for document repository. It allows on meetings and phone conferences planning and wiki style discussion on technical problems. The service is provided by MAS.

6.9 Dissemination and exploitation activities

nSHIELD dissemination and exploitation activities are reported in WP8 summary, Para. 3.6.

6.10 Coordination activities

Email and the nSHIELD wiki are the main tool to communicate among partners. Call Conference were used to manage WP progress.

Phone calls have been used to communicate directly among partners and on the project level.

6.11 Cooperation with other projects

The consortium is establishing – professional and dissemination – partnerships with similar projects and initiatives to work the project's way into relevant scientific circles. This includes both offline (scientific collaboration) and online projections (e.g. featuring project information on each other's website).

Collaboration is foreseen with other EU-funded projects: SEARCH-LAB plans to evaluate possible synergies with ANIKETOS [5] project, and to approach relevant project participants to initiate collaboration.

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.

Participating at ARTEMIS and FP7 events, Selex Galileo is actively involved in EU projects which could be synergetic with nSHIELD as ASHLEY. Also, Selex Galileo proposes nSHIELD as solution to internal projects which need to have SPD functionalities. An internal project OMNIA has synergies with nSHIELD and this is an example of “internal” Liaisons.

Movation is founding partner of the Norwegian Internet of Things Value Network (http://www.internet-of-things.no), which collects major players like Sintef, Telenor, Standards Norway and the major Universities. Through this network links are established to other European projects, notably the Artemis IoE (Internet of Energy).

The cooperation above is just few examples of cooperation with other projects. The deliverable D1.3 reports the complete liaison activity plan in which all nSHIELD partners are involved. At M34, the D1.11 will report all the Liaisons for nSHIELD.

7 Explanation of the use of the resources

Here below Person-Month Status and Cost tables are reported. Explanations on deviations in the use of resources are reported in Para.3 and Para 4.

Contract N. 269317 Acronym: nSHIELD Period: 01.09.2012 - 31.08.2013		MAS	ASTS	AT	ATHENA	TECNALIA	ALFA	ETH	HAI	ISL	ISD	SknFnd	MGEP	S-LAB	SESM	SICS	T2D	TELC	THYIA	TUC	UNIGE	UNIUD	UNIROMA1	SES
Workpackage 1:	**Actual WP total:**	0	2,5	6,15	0	0	0	0,7	9,5	6,1	1	0	2	0	0	0	0	0	1,5	0	0	1,5	2,57	48,7
Project Management	**Planned WP total:**	0,00	3,00	9,00	3,00	5,00	0,00	1,00	15,00	10,00	2,00	0,00	3,00	0,00	0,00	0,00	0,00	0,00	3,00	4,00	0,00	3,00	3,00	63,00
	%	0	83%	68%	0	0	0	70%	63%	61%	50%	0	67%	0	0	0	0	0	50%	0	0	50%	86%	77%
Workpackage 2:	**Actual WP total:**	0	11	6,7	2	14,8	0	1,5	21,5	0	0	0	0	9,34	0	6	10	0	12	8,8	0	3	0	27,86
SPD Metric, requirements and system design	**Planned WP total:**	0,00	11,00	8,00	6,00	12,00	0,00	2,00	22,00	0,00	0,00	0,00	0,00	10,00	0,00	6,00	10,00	0,00	13,00	10,00	0,00	3,00	0,00	23,00
		0	100%	84%	33%	123%	0	75%	98%	0	0	0	0	93%	0	100%	100%	0	92%	88%	0	100%	0	121%
Workpackage 3:	**Actual WP total:**	0	0	18	5	17,8	0	18	2	0	31	0	0	7,6	13	15	13	3,6	4,5	27,2	25	8	0	14,54
SPD Node	**Planned WP total:**	0,00	0,00	22,00	8,00	6,00	0,00	25,00	4,00	0,00	58,00	0,00	0,00	12,00	15,00	20,00	26,00	6,00	7,00	37,00	30,00	12,00	0,00	24,00
	%	0	0	82%	63%	297%	0	72%	50%	0	53%	0	0	63%	87%	75%	50%	60%	64%	74%	83%	67%	0	61%
Workpackage 4:	**Actual WP total:**	0	0	0	6	18,6	0	0	15	28,5	0	0	13,5	0	0	0	0	0	2,5	10,4	23	9	0	46,04
SPD Network	**Planned WP total:**	0,00	0,00	0,00	10,00	14,00	0,00	0,00	15,00	34,00	0,00	0,00	20,00	0,00	0,00	0,00	0,00	0,00	3,50	14,00	25,00	12,00	0,00	94,00
	%	0	0	0	60%	133%	0	0	100%	84%	0	0	68%	0	0	0	0	0	71%	74%	92%	75%	0	49%
Workpackage 5:	**Actual WP total:**	0	0	0	4	19,7	0	0	15,5	16,5	0	0	0	18,36	0	0	0	0	3,5	13,5	0	0	32,5	47,44
SPD Middleware & Overlay	**Planned WP total:**	0,00	0,00	0,00	14,00	20,00	0,00	0,00	27,00	18,00	0,00	0,00	8,00	28,00	0,00	0,00	0,00	0,00	4,50	18,00	0,00	0,00	41,00	53,00
	%	0	0	0	29%	99%	0	0	57%	92%	0	0	0	66%	0	0	0	0	78%	75%	0	0	79%	90%
Workpackage 6:	**Actual WP total:**	3,00	3,54	10,20	6,00	0,00	4,00	6,00	17,00	11,50	0,00	1,00	0,20	0,00	0,00	0,00	0,00	0,00	0,50	0,00	0,00	3,00	2,00	6,00
Platform integration, validation & demonstration	**Planned WP total:**	7,00	8,00	19,00	21,00	15,00	3,00	3,00	32,00	24,00	6,00	0,00	3,00	29,00	0,00	0,00	0,00	0,00	2,00	0,00	0,00	6,00	4,00	36,00
	%	43%	44%	54%	29%	0	133%	200%	53%	48%	0	0%	7%	0	0	0	0	0	25%	0	0	50%	50%	17%
Workpackage 7:	**Actual WP total:**	2	10,9	0,6	0	2,4	4	6	8,5	0	0	1	0	2,53	8	0	0	0	0,5	2,4	1	0	0	3,7
SPD Applications	**Planned WP total:**	6,00	21,00	2,00	0,00	8,00	11,00	18,00	23,00	0,00	6,00	5,50	0,00	24,00	16,00	0,00	0,00	3,00	3,00	9,00	5,00	0,00	0,00	40,00
	%	33%	52%	30%	0	30%	36%	33%	37%	0	0	18%	0	11%	50%	0	0	0	17%	27%	20%	0	0	9%
Workpackage 8:	**Actual WP total:**	2,5	0,5	2,1	0	1,9	0	0,8	5	6,7	0	0	6	0	0	0	0	0	0	3	0	0	0	5,73
Knowledge exchange and industrial validation	**Planned WP total:**	3,00	6,00	4,00	4,00	8,00	1,00	1,00	6,00	14,00	0,00	0,00	11,00	5,00	0,00	0,00	0,00	0,00	2,00	5,00	0,00	0,00	0,00	13,00
	%	83%	8%	53%	0	24%	0	80%	83%	48%	0	0	55%	0	0	0	0	0	0	60%	0	0	0	44%
	Actual total:	7,50	28,41	43,75	23,00	75,20	8,00	33,00	94,00	69,30	32,00	2,00	21,70	37,83	21,00	21,00	23,00	3,60	25,00	65,30	49,00	24,50	37,07	200,01
Total Project PM	**Planned total:**	16,00	49,00	64,00	66,00	88,00	15,00	50,00	144,00	100,00	72,00	5,50	45,00	108,00	31,00	26,00	36,00	9,00	38,00	97,00	60,00	36,00	48,00	346,00
	%	47%	58%	68%	35%	85%	53%	66%	65%	69%	44%	36%	48%	35%	68%	81%	64%	40%	66%	67%	82%	68%	77%	58%

Table 10 Person-Month Status

7.1 MAS

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY **MOVATION** YEAR2

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs[67]		93000		93000	
	Subcontracting					
	Travel		4000		4000	
	Remaining direct costs					
TOTAL DIRECT COSTS[2]			97000		97000	
TOTAL INDIRECT COSTS[2]						

Table 11 MAS Cost (note: the reporting period in Norway is different from the nSHIELD report, numbers are indicative)

[67] **All costs reported are indicative,** and subject to acceptance of the Research Council of Norway.

7.2 **ASTS**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		93.424,63	9.772,07	103.196,70	
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[68]			93.424,63	9.772,07	103.196,70	
TOTAL INDIRECT COSTS			46.712,32	4.886,04	51.598,35	

Table 12 ASTS Cost

Note: The personnel cost calculation and related indirect costs is only an estimation because it is based on average hourly rates. The individual ones will be used for the official cost statement.

[68] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.3 AT

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ACORDE TECHNOLOGIES FOR THE PERIOD 1ST SEPTEMBER 2012 – 31TH AUGUST 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		4.977,18 €	110.771,18 €	115.748,36 €	
	Subcontracting					
	Consumables			5.272,73 €	5.272,73 €	Electronic components for testing and development (individual elements >1k€)
	Other national items			5.105,03 €	5.105,03 €	
	Remaining direct costs					
TOTAL DIRECT COSTS			4.977,18 €	121.148,94 €	126.126,12 €	
TOTAL INDIRECT COSTS			995,44 €	22.154,24 €	23.149,67 €	

Table 13 AT Cost

7.4 **ATHENA**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR ATHENA RC/ INDUSTRIAL SYSTEMS FOR THE PERIOD 1/9/2012 – 31/8/2013						
Work Package	**Item description**	Amounts				**Explanations**
		Fundamental research	**industrial research**	**Experimental development**	**Total**	
WP3, WP4, WP5 WP6	Personnel costs		66.940			
	Subcontracting					
WP3, WP4, WP5	Travelling Expenses		7.445			
WP3, wP4, WP5	Research Equipment					
	Remaining direct costs		5.386			
TOTAL DIRECT COSTS[69]			79.771			
TOTAL INDIRECT COSTS			15.954			

Table 14 ATHENA Cost

[69] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.5 TECNALIA

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY FUNDACIÓN TECNALIA RESEARCH & INNOVATION FOR THE PERIOD 01/09/2012-31/08/2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP 2,3,4,5,6, 7,8	Personnel costs				215.234,55	Salary cost for 56,70PM
	Subcontracting				618,00	Audit
	Artemisia				2.821,34	Tasa artemisia
	Instrumental & materials				1.916,18	Amortization of several computers
TOTAL DIRECT COSTS[70]					220.590,07€	
TOTAL INDIRECT COSTS					43.046,91	20% of personal costs
TOTAL FOR PERIOD					**263.636,98**	

Table 15 Tecnalia Cost

[70] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.6 **ETH**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ETH FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs	0 €	52400 €	0 €	52400 €	Salary of personnel involved in research, design and development activities. Salary of personnel involved in management activities.
	Subcontracting	0 €	0 €	0 €	0 €	
	Consumable	0 €	0 €	0 €	0 €	
	Remaining direct costs	0 €	0 €	0 €	0 €	
TOTAL DIRECT COSTS[71]		0 €	52400 €	0 €	52400 €	
TOTAL INDIRECT COSTS		0 €	26200 €	0 €	26200 €	Overhead for personnel costs (rate 50%)

Table 16 ETH Cost

[71] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.7 HAI

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY HAI FOR THE PERIOD 01/09/2012-31/08/2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP 2,3,4,5,6, 7,8	Personnel costs		167.515 €		167.515 €	Salary cost for 62 PM
	Subcontracting					
	Major cost item 'Travel'		3.170 €		3.170 €	Participation in 3 nSHIELD plenary project meetings
	Major cost item 'Equipment'		2.153 €		2.153 €	202 € for nSHIELD nodes' h/w. 1951€ for Doors s/w license
	Remaining direct costs					Amortization of several computers
TOTAL DIRECT COSTS[72]			172.838 €		172.838 €	
TOTAL INDIRECT COSTS			9.080 €		9.080 €	20% of personal costs
TOTAL FOR PERIOD			181.918 €		**181.918 €**	

Table 17 HAI Cost

[72] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.8 ISL

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,4,5,6,8	Personnel costs		269098€		269098€	Salaries for one Director, 2 experts and 2 senior engineers for 10 months each as an average
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[73]			269098€		269098€	
TOTAL INDIRECT COSTS			53820€		53820€	

Table 18 ISL Cost

[73] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.9 ISD

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ISD FOR THE PERIOD 1ST SEPT 2012 – 30TH AUGUST 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs[74]					
	Subcontracting					
	Travel					
	Remaining direct costs					
TOTAL DIRECT COSTS						
TOTAL INDIRECT COSTS						

Table 19 ISD Cost

NOTE: ISD receives no funding from the JU. It receives funding only from the Greek National Funding Authority, which receives the cost breakdown directly from ISD and performs the financial audits according to the national rules.

[74] **All costs reported are indicative,** and subject to acceptance of the Research Council of Norway.

7.10 **MGEP**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	Industrial research	Experimental development	Total	
	Personnel costs		€99253.35		€99253.35	Salaries of personnel
	Subcontracting					
	Major cost item 'X'					
	Zolertia Professional Pack Platinum		€1308.95		€1308.95	WSN development platform
	Audit		€780		€780	Audit costs
	Remaining direct costs					
TOTAL DIRECT COSTS[75]			**€101342.30**		**€101342.30**	
TOTAL INDIRECT COSTS			**€19850.67**		**€19850.67**	Overhead rate 20% of personnel costs

Table 20 MGEP Cost

[75] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.11 **SLAB**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		73974 €*		73974 €*	Salaries of 4 different research engineers, for 26,93 PM (for one year of reporting period)
	Subcontracting					Not applicable
	Major cost item: Travel costs		*4118 €*		*4118 €*	Travel cost
	Major cost item 'Y' ……..					Not applicable
	Remaining direct costs					
TOTAL DIRECT COSTS[76]			78092 €*		78092€*	
TOTAL INDIRECT COSTS			7809 €*		7809 €*	

- *The actual costs reported here are forecasts in EUR.*
  The fluctuation of the exchange rate between EUR and HUF could cause the final reported costs differ even more than 10%. The current amount was calculated using official rate of ECB on 2013.08.31 – (300,05 EUR/HUF)

Table 21 SEARCH-LAB Cost

[76] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.12 **SESM**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SESM FOR THE PERIOD 01/09/2012 – 31/08/2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP3, WP7	Personnel costs		89600		89600	16 PMs
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[77]			89600		89600	
TOTAL INDIRECT COSTS			30464		30464	

Table 22 SESM Cost

[77] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.13 **SICS**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY 19 (SICS) FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2, WP3	Personnel costs	25000 €		30068 €	55068 €	System requirements and architecture work.. Swedish node work coordination and nSHIELD face to face meeting in Stockholm. SICS hypervisor Global Platform design and Linux porting design work.
WP3	Subcontracting			10000	10000 €	SICS hypervisor evaluation and improvements
TOTAL DIRECT COSTS[78]		25000 €		40068 €	650068 €	
TOTAL INDIRECT COSTS		13700 €		16537 €	30237 €	55% overhead costs.

Table 23 SICS Cost

[78] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.14 **T2D**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY 19 (SICS) FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2, WP3	Personnel costs		82121 €	40000 €	122121 €	
TOTAL DIRECT COSTS[79]			82121 €	40000 €	122121 €	
TOTAL INDIRECT COSTS			45166 €	22000 €	67166 €	55% overhead costs.

Table 24 T2D Cost

[79] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.15 **TELC**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs		4080		4080	
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[80]			4080		4080	
TOTAL INDIRECT COSTS			2244		2244	Overhead 55% of personnel costs. Includes travel.

Table 25 TELC Cost

[80] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.16 **THYIA**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
2,3,4,5,6, 7	Personnel costs	14580			14580	3 MM personnel costs
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[81]		14580			14580	
TOTAL INDIRECT COSTS		2916			2916	Overhead 20% of personnel costs. Includes travel.

Table 26 THYIA Cost

[81] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.17 **TUC**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TUC FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs	128785			128785	Salaries of full-time and part-time personnel, plus 2 PhD students at Technical University of Crete.
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' …….					
	Remaining direct costs					
TOTAL DIRECT COSTS[82]					128785	
TOTAL INDIRECT COSTS						

Table 27 TUC Cost

[82] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.18 **UNIGE**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY Y FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs	61000 €	*0 €*	*0 €*	61000 €	Salary of PostDoc at University of Genoa, Salary of Full Professor (FP) at University of Genoa according to the following breakdown: 6 PM PostDoc 7.5 PM Full Professor
4	Personnel costs	69.512,40 €	*0 €*	*0 €*	69.512,40 €	Salary of PhD at University of Genoa, Salary of Assistant Professor (AP) and Full Professor (FP) at University of Genoa according to the following breakdown: 10,5 PM Full Professor 5 PM Assistant Professor
7	Personnel costs	7.098,30 €	*0 €*	*0 €*	7.098,30 €	Salary of PhD at University of Genoa, Salary of Assistant Professor (AP) and Full Professor (FP) at University of Genoa according to the following breakdown: 1 PM Full Professor
TOTAL DIRECT COSTS		*137610,7 €*	*0 €*	*0 €*	*137610,7 €*	
TOTAL INDIRECT COSTS		*53668,18 €*	*0 €*	*0 €*	*53668,18 €*	overhead rate 39% of personnel costs

Table 28 UNIGE Cost

7.19 **UNIUD**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIUD FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1	Personnel costs	*4,841.21 €*	0	0	*4,841.21 €*	Salaries for 1 Full Professor (0.5 PM)
1	Subcontracting	0	0	0	0	
1	Major cost item	0	0	0	0	
1	Major cost item	0	0	0	0	
1	Remaining direct costs	0	0	0	0	
TOTAL DIRECT COSTS[83]		*4,841.21 €*	0	0	*4,841.21 €*	
TOTAL INDIRECT COSTS		*2,420.61 €*	0	0	*2,420.61 €*	Overhead: 50% of personnel cost

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIUD FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs	*29,637.62 €*	0	0	*29,637.62 €*	Salaries for 2 Full Professors (1 PM each) + 1 Associate Professor (1 PM) and 1 Assistant Professor (1 PM)
3	Subcontracting	0	0	0	0	
3	Major cost item	0	0	0	0	
3	Major cost item	0	0	0	0	
3	Remaining direct costs	0	0	0	0	
TOTAL DIRECT COSTS[84]		*29,637.62 €*	0	0	*29,637.62 €*	
TOTAL INDIRECT COSTS		*14,818.81 €*	0	0	*14,818.81 €*	Overhead: 50% of personnel cost

[83] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

[84] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIUD FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
4	Personnel costs	*29,389.88 €*	0	0	*29,389.88 €*	Salaries for 1 Full Professor (1 PM) + 1 Associate Professor (2 PM) + 1 Research Assistant (2 PM)
4	Subcontracting	0	0	0	0	
4	Major cost item	0	0	0	0	
4	Major cost item	0	0	0	0	
4	Remaining direct costs	*5,130.63 €*	0	0	*5,130.63 €*	Durable: Rack server (155.17) Notebook (62.50) Consumables: Prototyping boards (4833.95) Power Supply (79.00)
TOTAL DIRECT COSTS[85]		*29,389.88 €*	0	0	*34,520.51 €*	
TOTAL INDIRECT COSTS		*14,694.94 €*	0	0	*14,694.94 €*	Overhead: 50% of personnel cost

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIUD FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
6	Personnel costs	*9,152.25 €*	0	0	*9,152.25 €*	Salaries for 1 Research Assistant (3 PM)
6	Subcontracting	0	0	0	0	
6	Major cost item	0	0	0	0	
6	Major cost item	0	0	0	0	
6	Remaining direct costs	0	0	0	0	
TOTAL DIRECT COSTS[86]		*9,152.25 €*	0	0	*9,152.25 €*	
TOTAL INDIRECT COSTS		4,576.13 €	0	0	4,576.13 €	Overhead: 50% of personnel cost

Table 29 UNIUD Cost

[85] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

[86] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.20 **UNIROMA1**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIROMA1 FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 5, 6	Personnel costs		138262€		138262 €	n. 21.8 PM (5 professors & 6 researchers)
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[87]			69131 €		69131 €	
TOTAL INDIRECT COSTS			207393 €		207393 €	

Table 30 UNIROMA1 Cost

[87] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.21 **SES**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY FOR THE PERIOD						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3, 4,5,6,7,8	Personnel costs	546048			546048	*Salaries of 6engineer and 2 lab technician for ~93 months total*
	Subcontracting					
	Remaining direct costs	3900			3900	Travel
TOTAL DIRECT COSTS[88]		549948			549948	
TOTAL INDIRECT COSTS		276961			276961	

Table 31 SES Cost

[88] Total direct and indirect costs have to be consistent with the direct and indirect costs claimed to the National funding Institution or, when applicable, to the JU.

7.22 **Alfatroll**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ALFATROLL FOR YEAR2						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		37000		3700	
	Subcontracting					
	travel		1600		1600	
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[89]			38600 €		38600	
TOTAL INDIRECT COSTS						

Table 32 Alfatroll Cost (note: the reporting period in Norway is different from the nSHIELD report, numbers are indicative)

[89] **All costs reported are indicative,** and subject to acceptance of the Research Council of Norway.

7.23 **SknFnd**

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY **SKNFND** FOR YEAR 2

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		5000		5000	
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS[90]			5000 €		5000	
TOTAL INDIRECT COSTS						

Table 33 SknFnd Cost (note: the reporting period in Norway is different from the nSHIELD report, numbers are indicative)

[90] **All costs reported are indicative,** and subject to acceptance of the Research Council of Norway.

Beneficiaries without a corresponding National Grant Agreement. Financial statements – Form C and Summary financial report

Separate financial statement (Form C) from each beneficiary not having concluded a Grant Agreement with the respective National Authority will not be submitted in the frame of this periodic report.

8 Certificates

For this intermediate report no certificate is required, in accordance with Article IV.4.3 of the Grant Agreement.