

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 28.02.2013

Name, title and organisation of the scientific representative of the project's coordinator¹:

Dr. Josef Noll (MOVATION)

Tel: +47 9083 8066

Fax:

E-mail: josef.noll@novation.no

Project website² 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 coordinator¹

I, as scientific representative of the coordinator¹ 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 deviations³;
 - has failed to achieve critical objectives and/or is not at all on schedule⁴.
- 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 Coordinator¹:

Date://

Signature of scientific representative of the Coordinator¹:

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

D1.7: Periodic Management Report 2

Due date of deliverable: M18 -2013.02.28

Actual submission date: M20 -2013.04.30

Start date of project: 01/09/2011

Duration: 36 months

Organization name of lead contractor for this deliverable:

Selex ES, SE

Revision [Final]

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		
Elisabetta Campaiola	Selex ES		
Marco Cesena	Selex ES		
Francesco Delli Priscoli	UNIROMA1		
Paolo Azzoni	ETH		
George Dramitinos	ISD		
Christian German	SICS		
Iñaki Eguia	Tecnalia		
Alexandros Papanikolaou	TUC		
Antonio Abramo	UNIUD		
Antonio Di Marzo	SESM		
Balázs Berkes	SLAB		
Ignasi Barri Vilardell	INDRA		
Carlo Pompili	Telcred		
Esposito Mariana	ASTS		
Esther López	ACORDE		
Hans Thorsen	T2DATA		
John Gialelis	ISI		
Lorena de Celis	ACORDE		
Andrea Morgagni	Selex Elsag		
Nikolaos Pappas	HAI		
Roberto Uribeetxeberria	MGEP		
Paolo Gastaldo	UNIGE		
Lucio Mercenaro	UNIGE		
Kresimir Dabcevic	UNIGE		
Reviewed by			
Name	Company		
Josef Noll	Movation		
Approved by			
Name	Company		
Cecilia Coveri	Selex ES		



Modification History		
Issue	Date	Description
Draft A	2013-01-21	First issue for comments.
	2013-02-13	First partners contribution
	2013-02-25	Additional partners contribution
Draft B	2013-04-30	New partners description
	2013-05-15	Additional partners contribution
Final		



Contents

1	Publishable summary	13
1.1	Overview.....	13
1.2	Major findings	14
2	Project objectives for the period (1/9/2012- 28/2/2013)	15
3	Work progress and achievements during the period	17
3.1	WP2.....	17
3.2	WP3.....	21
3.3	WP4.....	25
3.4	WP5.....	28
3.5	WP6.....	34
3.6	WP7.....	36
3.7	WP8.....	38
4	Project Beneficiary (Grouped by Country)	43
4.1	Italy	43
4.1.1	Ansaldo	43
4.1.2	Selex Elsig SE.....	45
4.1.3	ETH I.P.S Sistemi Programmabili - Eurotech Security	51
4.1.4	Selex Galileo SG	53
4.1.5	SESM scarl SESM	56
4.1.6	Università degli Studi di Genova UNIGE	58
4.1.7	Università degli Studi di Udine UNIUD.....	62
4.1.8	Università degli studi di Roma "La Sapienza" UNIROMA1	66
4.1.9	Selex ES.....	71
4.2	Spain	76
4.2.1	Acorde Technologies AT.....	76
4.2.2	Fundación Tecnalia Research & Innovation TECNALIA	79
4.2.3	Mondragon Goi Eskola Politeknikoa MGEP	83
4.2.4	Indra Software Labs (ISL)	88
4.3	Slovenia.....	96
4.3.1	THYIA Tehnologije	96
4.4	Norway	97
4.4.1	Movation AS (MAS) and Alfatroll (ALFA)	97
4.5	Sweden.....	100
4.5.1	Swedish Institute of Computer Science SICS.....	100
4.5.2	T2 Data AB T2D.....	103
4.5.3	Telcred TELC	106
4.6	Hungary	107
4.6.1	Security Evaluation Analysis and Research Lab. S-LAB.....	107
4.7	Greece.....	109
4.7.1	ATHENA Research and Innovation Centre ATHENA.....	109



4.7.2	Hellenic Aerospace Industry	113
4.7.3	Integrated Systems Development ISD	121
4.7.4	Technical University of Crete TUC	123
5	Deliverables and milestones tables	131
5.1	Deliverables	131
5.2	Milestones	133
6	Project management	134
6.1	Consortium management tasks and achievements	134
6.2	Encountered problems	134
6.3	Changes in the consortium	134
6.3.1	Selex ES	134
6.3.2	Alfatroll	135
6.3.3	ESIS	135
6.3.4	NOOM	135
6.4	Project meetings	135
6.5	Project planning and status	136
6.6	Impact of deviations	136
6.7	Changes to the legal status	136
6.8	Project website	136
6.9	Dissemination and exploitation activities	136
6.10	Co-ordination activities	136
6.11	Cooperation with other projects	136
7	Explanation of the use of the resources	138
7.1	MAS	140
7.2	ASTS	141
7.3	AT	142
7.4	ATHENA	143
7.5	SE	144
7.6	TECNALIA	145
7.7	ETH	146
7.8	HAI	147
7.9	ISL	148
7.10	ISD	149
7.11	SG	150
7.12	MGEP	151
7.13	SLAB	152
7.14	SESM	153
7.15	SICS	154
7.16	T2D	155
7.17	TELC	156
7.18	THYIA	157



7.19	TUC	158
7.20	UNIGE	159
7.21	UNIUD	160
7.22	UNIROMA1	161
7.23	SES	162
7.24	Alfatroll.....	163
8	Beneficiaries without a corresponding National Grant Agreement. Financial statements – Form C and Summary financial report	164
9	Certificates.....	165



Figures

Figure 1: Multiple sources for requirements collection	18
Figure 2: Hierarchical structure of nSHIELD System Architecture	19
Figure 3: Project meetings	135

Tables

Table 1: WP2 Management Report	20
Table 2: WP3 Management Report	24
Table 3: WP4 Management Report	27
Table 4: WP5 Management Report	33
Table 5: WP6 Management Report6	35
Table 6: WP7 Management Report	37
Table 7: WP8 Management Report	42
Table 8: Deliverables	132
Table 9: Milestones	133
Table 10: Person-Month Status	139
Table 11: MAS Cost	140
Table 12: ASTS Cost	141
Table 13: AT Cost	142
Table 14: ATHENA Cost	143
Table 15: SE Cost	144
Table 16: TECNALIA Cost	145
Table 17: ETH Cost.....	146
Table 18: HAI Cost.....	147
Table 19: ISL Cost	148
Table 20: ISD Cost.....	149
Table 21: SG Cost.....	150



Table 22: MGEP Cost.....	151
Table 23: SEARCH-LAB Cost	152
Table 24: SESM Cost	153
Table 25: SICS Cost	154
Table 26: T2D Cost.....	155
Table 27: TELC Cost	156
Table 28: THYIA Cost.....	157
Table 29: TUC Cost.....	158
Table 30: UNIGE Cost	159
Table 31: UNIUD Cost	160
Table 32: UNIROMA1 Cost	161
Table 33: SES Cost	162
Table 34: Alfatroll Cost	163



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

The nSHIELD project is, at the same time, a *complement* and significant technology breakthrough of “pSHIELD”, a pilot project funded in ARTEMIS Call 2009 as the first investigation towards the realization of the **SHIELD Architectural Framework for Security, Privacy and Dependability (SPD)**. The roadmap, already started in the pilot project, will bring to address SPD in the context of Embedded Systems (ESs) as “built-in” rather than as “add-on” functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ES.

pSHIELD has covered the definition phase of this roadmap: nSHIELD will be in charge of the development and implementation phases. The SHIELD General Framework consists of four layered system architecture and Application Layer in which four scenarios are considered: 1) Railway, 2) Voice/Facial Recognition, 3) Dependable Avionic Systems and 4) Social Mobility and Networking.

The leading concept is to **demonstrate composability** of SPD technologies. Starting from current SPD solutions in ESs, the project will develop **new technologies** and consolidate the ones already explored in pSHIELD in a solid basement that will become the reference milestone for a new generation of “SPD-ready” ESs. nSHIELD will approach SPD at 4 different levels: node, network, middleware and overlay. For each level, the state of the art in SPD of individual technologies and solutions will be improved and integrated (hardware and communication technologies, cryptography, middleware, smart SPD applications, etc.). The SPD technologies will be then enhanced with the “composability” functionality that is being studied and designed in pSHIELD, in order to fit in the SHIELD architectural framework.

The composability of this architectural framework will have great impact on the system design costs and time to market of new SPD solutions in ESs. At the same time, the integrated use of SPD metrics in the framework will have impact on the development cycles of SPD in ESs because the qualification, (re-)certification and (re-)validation process of a SHIELD framework instance will be faster, easier and widely accepted.

The use of an overlay approach to SPD and the introduction of semantic technologies address the complexity associated with the design, development and deployment of built-in SPD in ESs. Using semantics, the available technologies can be automatically composed to match the needed, application specific SPD levels, resulting also in an effort reduction during all the design, operational and maintaining phases. The nSHIELD approach, as explored in the pilot project, is based on **modularity and expandability**, and can be adopted to bring built-in SPD solutions in all the strategic sector of ARTEMIS, such as transportation, communication, urban environment.

To achieve these challenging goals the project aims at creating an **innovative, modular, composable, expandable and high-dependable architectural framework**, concrete tools and common SPD metrics capable of improving the overall SPD level in any specific application domain, with minimum engineering effort. The whole ESs lifecycle will be supported to provide the highest cross-layer and cross-domain levels of SPD and guaranteeing their maintenance and evolution in time.

In order to verify these important achievements, the project has identified relevant scenarios to validate the nSHIELD integrated system:

- Railways Security
- Voice/facial recognition
- Dependable avionic systems
- Social Mobility and Networking

The project will have a great impact on the SPD market of the ESs. By addressing the reusability of previous designed solutions, the interoperability of advanced SPD technologies and the standardized SDP certificability, it is possible to estimate an overall 30% cost reduction for a full nSHIELD oriented design methodology. Additionally, for social mobility and networking scenario the expected market in few

years will be 15% of 5 billion mobile users. Finally, this project by taking in consideration the current Directive 2009/125/EC and the future one motivate by conclusions of the Competitiveness Council of 28 May 2009 that pointed out "it is of particular interest to maintain strong R&D investments in high-tech industries in Europe, especially in manufacturing sectors with indispensable technologies," great social and economic impacts for European economy will be achieved.

nSHIELD project focuses on:

1. **Demonstrate composability:** Composability of SPD functionality at different layers among different technologies will be refined and developed, taking into account performances and dynamic composability of any kind of technologies.
2. **New technologies:** A wide set of technologies will be used to realise SPD composability and design guidelines will be provided to make any "nSHIELD compliant technology" composable with the others.
3. **Innovative, modular, composable, expandable and high-dependable architectural framework:** nSHIELD will refine and develop the framework in a complex scenario
4. **Metrics:** A complete exhaustive set of metrics for SPD description will be refined and consolidated in the nSHIELD project and used to validate the whole functionalities of the framework
5. **Validate the nSHIELD integrated system in one application scenario:** the new project will validate the architectural framework by means of four (complex) scenarios relevant in an industrial perspective.
6. **Certification Aspects:** nSHIELD will be the first step towards SPD certification for future ES.

1.2 Major findings

In the half of the project, the high level scenarios overview has been preliminary investigated and analysed according to the potential standardization of the SPD metrics. Additionally Formal Methods and no Formal Methods approaches have been evaluated.

Many important activities 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 will be 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 definition of SPD Metrics and the practical implementation of the SPD Metrics themselves have been discussed and analysed in details, including the need of the definition of a "contact point" between the metrics and their implementation.

Additionally, testing methodology, incorporation of requirements, scenario description and specification of trials have been preliminary evaluated.

Details of the technical work are outlined on the nSHIELD <http://nshield.unik.no/wiki/NSHIELD>.

2 Project objectives for the period (1/9/2012-28/2/2013)

Within the third reporting period of the nSHIELD project (01.09.2012-28.02.2013) 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: “SPD Metric, requirements and system design” is the topic of this work package. Identification of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration has been the major activity developed in this period.

No other activity was planned for this period, waiting for the start of the preliminary scenarios realization integration.

WP3 Objectives and Achievements: “SPD Node” is the topic of this work package. The scope is the definition of SPD intrinsic capabilities at node layer through the creation of an Intelligent ES HW/SW Platform consisting of three different kinds of intelligent ES Nodes: SDR/Cognitive Enabled node, nano and micro node.

The WP3 objectives are:

- improve SPD technologies at Node level;
- develop appropriate composability mechanisms at such level;
- deliver a SPD node prototype.

The activities of the third semester of the project have been mainly focused on design and development activities.

Deliverables for the period: D3.2, D3.3.

WP4 Objectives and Achievements: “SPD Network” is the topic of this work package. This WP follows an approach similar to the WP3, focusing on the transmission (communication) level. Improve SPD technologies at Network level.

The WP4 objectives are:

- Improve SPD technologies at Network level;
- Develop a prototype to be integrated in the demonstrators

The activity of this half has been dedicated to the development of code/algorithms included in D4.2 “Preliminary SPD node technologies prototype”. In particular Trust Definition and Approaches, including evaluation of trust, have been investigated and described as important values of network device or component.

Deliverables for the period: D4.2, D4.3

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;

Deliverables for the period: D5.2, D5.3

The WP5 objectives are:

- Define a common semantic to describe the SPD interfaces and functionalities;
- Improve SPD middleware technologies;
- Provide support to legacy SPD systems;

- Introduce the Overlay concepts and functionalities;
- Develop a prototype to be integrated in the demonstrators.

The activity of this period has been focused on the detailed description of the SPD technologies that are currently under development in work package 3, conforming to the architecture and the composability requirements specified in deliverables D2.4 and D2.5.

Technologies required by the different kind of scenarios at micro node and power node together with horizontal SPD technologies are investigated. The conclusion of this study will be included in D5.2 and D5.3.

WP6 Objectives and Achievements: “Platform integration, validation & demonstration”.

The WP6 objectives are:

- Integration of software components;
- Validation of implemented solution through an iterative and incremental process.

The activity of this period has been devote to investigate and define the guidelines and the plan for checking the nSHIELD SPD architecture to be future proof, and close the systems engineering life cycle by supporting the installation, downloading and upgrading cycle and addressing the security and integrity issues involved.

Deliverables for the period: D6.1

WP7 Objectives and Achievements: “SPD Applications”. Limited activity was planned for this period. This package will definitely start after the preliminary description of each scenarios demonstration held during the second internal project meeting. In this occasion, the common philosophy for scenarios demonstration will be illustrated and analysed according to nSHIELD guide lines.

WP8 Objectives and Achievements: “Knowledge exchange and industrial validation” is the topic of this work package. This WP defines the strategy for dissemination and standardization which are essential part of the project. Moreover activities as website stand up and maintenance are needed for communication between partners and the external world.

Deliverable for the period: D8.4.

The WP8 activities for the period are:

- Website for disseminating the project over the web and other media channels (wiki, YouTube etc.)
- nSHIELD Summary Report

The Exploitation task will start on M18 but the industrial partners are already discussing on how to promote and facilitate the exploitation of the results.

Regarding the D8.4 “Build Secure Embedded System with nSHIELD v1”, this deliverable had suffered of a delay (actual delivery date June 2012). Several meetings and discussions were needed to get a common view on how to promote «measurable security» as a key concept for future operations. For this reason and at this moment (M18), D8.4 has to be considered as draft. When all these intermediate results will be available to all partners then this document will be finalized. This deliverable is expected to be ready and available by June 2013

3 Work progress and achievements during the period

3.1 WP2

WP2 - Leader TECNALIA	
Period: 1 September 2012- 28 February 2013	
1	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p> <p>The convergence to objectives is in line with the project and WP objectives. Summarising, the WP aims to:</p> <ul style="list-style-type: none"> • 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. <p>During October of 2012, ARTEMIS JU officers and reviewers expressed the confirmation of the approach WP2 was achieving. The indicators for these were:</p> <ol style="list-style-type: none"> 1) The SPD requirements defined by each different layer were the correct ones and were aligned with the architecture and convergent with different use cases described. 2) Metrics have been determined in a quantitative and formal way. The formalisation comes from three points of view: <ol style="list-style-type: none"> a. Mathematical approach for measuring each of the metrics identified b. Formal alignment towards specification and standards (Common Criteria) c. Compositional approaches identified but not prioritised yet. <p>Definition of a heterogeneous and distributed reference architecture which aims to link the dissimilar components of nSHIELD System</p>
2	<p><i>Highlight clearly significant and tangible results</i></p> <p>The following deliverables have been delivered and approved in the last review:</p> <ul style="list-style-type: none"> • D2.1 Preliminary System Requirements M03 • D2.2 Preliminary System Requirements and Specifications M06 • D2.3 Preliminary System architecture design M09 • D2.4 Reference system architecture design M12 • D2.5 Preliminary SPD Metrics specifications M12 <p>D2.6, D2.7 and D2.8 will be developed by next milestones. 5 of 8 deliverables submitted.</p> <p>Significant result are:</p> <ol style="list-style-type: none"> 1) Requirements described in a standardized way to ensure a common understanding and to facilitate later exploration and usage for implementation

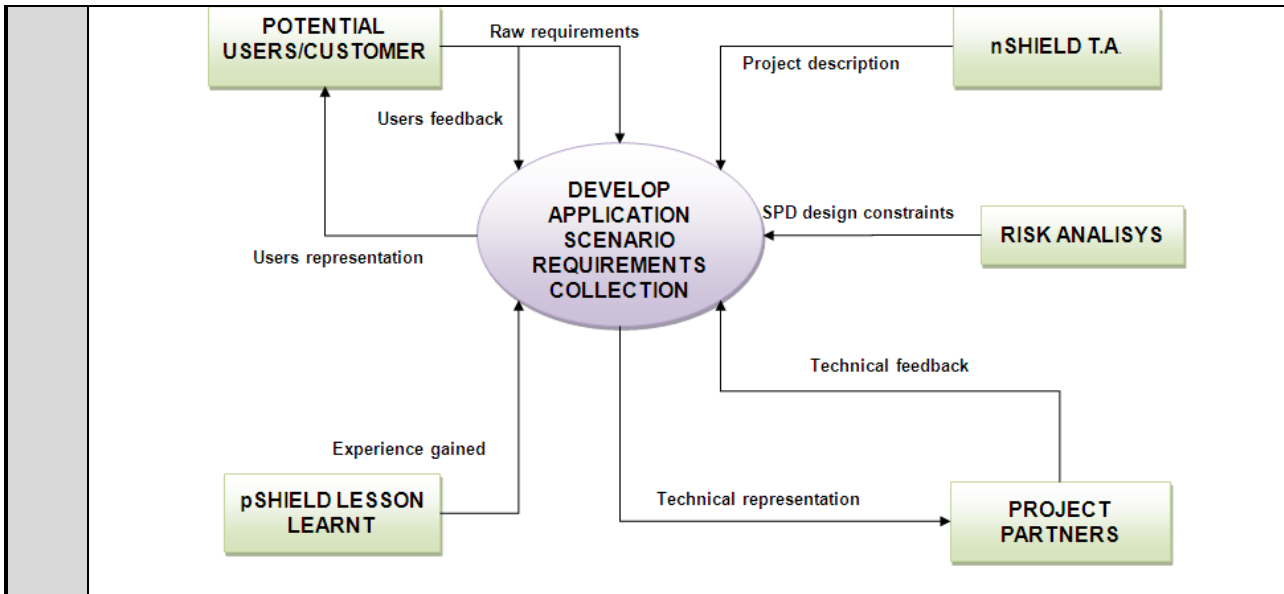


Figure 1: Multiple sources for requirements collection

- 2) SPD Metrics quantification and formalization: nSHIELD full domain metrics have been identified and quantified. Methods and tools are envisaged to implement. The composition method could be derived towards an incremental certification scope and view which would link both formalization and quantification (This scope is an undergoing task)
Identification of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration.
- 3) Finalization of nSHIELD Reference System Architecture. The architectural proposal was based and further analysed on the definition or design of the following:
 - a. Modified Embedded Systems Development Lifecycle Model
 - b. A viewpoint driven approach addressing each of the 4 nSHIELD functional layers (Node, Network, Middleware, Overlay)
 - c. 3 main types of nSHIELD Embedded System Devices (ESDs)
 - d. Support of legacy devices
 - e. Analysis of services, capabilities and structuring of each nSHIELD functional layer based on architectural views
 - f. Preliminary definition of interfaces and information flows to be detailed in implementation WPs (WP3-WP5)
 - g. Realization of the architecture for an application scenario (Railway SMS)
- 4) Proposal by TUC of a novel dynamic and applicable formal methodology for evaluating the SPD composed metric. The new approach supports a dynamic choreographed modelling scheme. The scheme permits the modelling of legitimate/malicious behaviour, dynamic composition and setting of environment parameters and attack scenarios. To retain consistency with this new model, the original SPD metrics of D2.5 were re-classified in three categories (SPD metrics, security attributes and security properties).

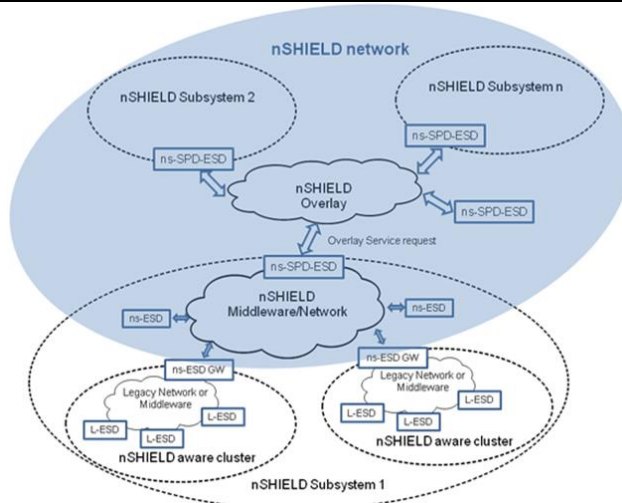


Figure 2: Hierarchical structure of nSHIELD System Architecture

3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>Not applicable</p>																																																																																										
4	<p><i>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)</i></p> <p>Not applicable.</p>																																																																																										
5	<p><i>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)</i></p> <p>The following table summarizes the use of resources for every partner:</p> <table border="1"> <thead> <tr> <th>Partic. No.</th> <th>Partic. Short name</th> <th>Planned Effort Period M12-M18</th> <th>Spent effort Period M12-M18</th> <th>Difference</th> </tr> </thead> <tbody> <tr><td>2</td><td>ASTS</td><td>1.82</td><td>1.82</td><td>0</td></tr> <tr><td>3</td><td>AT</td><td>0</td><td>0.5</td><td>0.5</td></tr> <tr><td>4</td><td>ATHENA</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>5</td><td>SE*</td><td>1.1</td><td>6.0</td><td>4.9</td></tr> <tr><td>6</td><td>TECNALIA</td><td>3</td><td>10</td><td>7</td></tr> <tr><td>8</td><td>ETH</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>9</td><td>HAI</td><td>0</td><td>3</td><td>3</td></tr> <tr><td>12</td><td>SG*</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>15</td><td>S-LAB</td><td>2</td><td>1.96</td><td>-0.04</td></tr> <tr><td>16</td><td>SESM</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>17</td><td>SICS</td><td>1</td><td>1</td><td>0</td></tr> <tr><td>18</td><td>T2D</td><td>0.6</td><td>0.6</td><td>0</td></tr> <tr><td>20</td><td>THYIA</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>21</td><td>TUC</td><td>0</td><td>1.3</td><td>+1.3</td></tr> <tr><td>23</td><td>UNIUD</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>25</td><td>SES**</td><td>0.4</td><td>2</td><td>1.6</td></tr> <tr> <td colspan="2">TOTAL</td> <td>9,92</td> <td>27,68</td> <td>18,26</td> </tr> </tbody> </table>	Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference	2	ASTS	1.82	1.82	0	3	AT	0	0.5	0.5	4	ATHENA	0	0	0	5	SE*	1.1	6.0	4.9	6	TECNALIA	3	10	7	8	ETH	0	0	0	9	HAI	0	3	3	12	SG*	0	0	0	15	S-LAB	2	1.96	-0.04	16	SESM	0	0	0	17	SICS	1	1	0	18	T2D	0.6	0.6	0	20	THYIA	0	0	0	21	TUC	0	1.3	+1.3	23	UNIUD	0	0	0	25	SES**	0.4	2	1.6	TOTAL		9,92	27,68	18,26
Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference																																																																																							
2	ASTS	1.82	1.82	0																																																																																							
3	AT	0	0.5	0.5																																																																																							
4	ATHENA	0	0	0																																																																																							
5	SE*	1.1	6.0	4.9																																																																																							
6	TECNALIA	3	10	7																																																																																							
8	ETH	0	0	0																																																																																							
9	HAI	0	3	3																																																																																							
12	SG*	0	0	0																																																																																							
15	S-LAB	2	1.96	-0.04																																																																																							
16	SESM	0	0	0																																																																																							
17	SICS	1	1	0																																																																																							
18	T2D	0.6	0.6	0																																																																																							
20	THYIA	0	0	0																																																																																							
21	TUC	0	1.3	+1.3																																																																																							
23	UNIUD	0	0	0																																																																																							
25	SES**	0.4	2	1.6																																																																																							
TOTAL		9,92	27,68	18,26																																																																																							

PP

	<p>*From September to December 2012 only</p> <p>** From January to February 2013</p>
6	<p><i>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)</i></p> <p>Not applicable</p>
7	<p><i>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)</i></p> <p>Not applicable</p>
8	<p><i>If applicable, propose corrective actions</i></p> <p>Not applicable</p>

Table 1: WP2 Management Report

3.2 WP3

WP 3 - Leader ISD	
Period: 1 September 2012- 28 February 2013	
1	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p> <p>The activities of the third semester of the project have been mainly focused on design and development activities.</p> <p>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. 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.</p> <p>The research and designed activities have been focused on the following topics:</p> <ul style="list-style-type: none"> • AT: Power supply protection mechanisms; Custom anti-tamper module. • ATHENA: Prototype set of DDoS defence mechanisms; Novel cryptographic key exchange algorithm (Controlled Randomness). • ETH: Voice and face recognition algorithms. • ISD: Development of an audio based surveillance/anti-tampering system. • SE: 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: Development of a nSHIELD Embedded System Device Gateway that will provide enhanced capabilities in terms of security and dependability to the cluster where it will be integrated. • 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: Investigation of a framework for delegation of access rights (authorization) at node level. • THYIA: no contribution in this half. • TUC: Working on the following prototypes: smartcard-based authentication protocol, lightweight crypto library API, location privacy scheme, lightweight automatic access control protocol, cryptographic key establishment protocol, GPU accelerated functionality for power nodes. • 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. • SES: Contribution to D3.2 “Preliminary SPD node technologies prototype”

2	<p><i>Highlight clearly significant and tangible results</i></p> <p>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:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ○ In the first case, AT is working in the design of a “smart power” module, following the architecture proposal done in WP2 (modules and metrics). ○ 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: <ul style="list-style-type: none"> ▪ Measures consisting of continuous monitoring and detection of tamper attacks. ▪ Measures that are typically implemented at manufacture level as passive physical barriers. AT has investigated different solutions for this option, encapsulation and physical barriers. • ATHENA: <ul style="list-style-type: none"> ○ Design and prototype implementation of the node reporting functions to support DDoS attacks mitigation mechanisms. ○ Design and prototype implementation for the controlled randomness protocol on the micro and power nodes. • ETH: <ul style="list-style-type: none"> ○ 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). • 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. • SE: Prototypes, matching with WP2 requirements, specification and interface design. Inputs to the deliverables D3.2 and D3.3. • SESM: The architecture of nESD GTW has been defined and designed. The nESD GTW will be implemented by the means of FPGA and Softcore Microprocessor. The final objective will be the deployment of a nESD-GTW that will foster the communications between legacy power Node and SHIELD components. A proactive collaboration geared towards the usage of such architecture into the avionic dependable demonstrator has been established with SG. • 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 BeagleBone. • 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.
---	--

	<ul style="list-style-type: none"> • THYIA: no contribution in this half • TUC: Has completed the design for the following: smartcard-based authentication protocol, cryptographic key establishment protocol, lightweight automatic access control protocol. Has partially working prototypes for the following: lightweight crypto library API, location privacy scheme, GPU accelerated functionality for power nodes. • 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. • SES: inputs to the deliverables D3.2 and D3.3 and coordination activities. 																																																																																																														
3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>Not applicable</p>																																																																																																														
4	<p><i>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)</i></p> <p>Not applicable</p>																																																																																																														
5	<p><i>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)</i></p> <p>The following table summarizes the use of resources for every partner:</p> <table border="1" data-bbox="341 1182 1410 1917"> <thead> <tr> <th>Partic. No.</th> <th>Partic. Short name</th> <th>Planned Effort Period M12-M18</th> <th>Spent effort Period M12-M18</th> <th>Difference</th> </tr> </thead> <tbody> <tr><td>1</td><td>MAS</td><td>3</td><td>3,5</td><td>0.5</td></tr> <tr><td>3</td><td>AT</td><td>7</td><td>5.5</td><td>-1.5</td></tr> <tr><td>4</td><td>ATHENA</td><td>3</td><td>3</td><td>0</td></tr> <tr><td>6</td><td>TECNALIA</td><td>1</td><td>4</td><td>3</td></tr> <tr><td>5</td><td>SE*</td><td>0.8</td><td>0.7</td><td>-0.1</td></tr> <tr><td>7</td><td>Alfatroll</td><td>2</td><td>3</td><td>1</td></tr> <tr><td>8</td><td>ETH</td><td>6</td><td>6</td><td>0</td></tr> <tr><td>9</td><td>HAI</td><td></td><td></td><td></td></tr> <tr><td>11</td><td>ISD</td><td>12</td><td>11.5</td><td>-0.5</td></tr> <tr><td>12</td><td>SG*</td><td>3.3</td><td>1.2</td><td>-2.1</td></tr> <tr><td>15</td><td>S-Lab</td><td>2.45</td><td>2.45</td><td>0</td></tr> <tr><td>16</td><td>SESM</td><td>1</td><td>1</td><td>0</td></tr> <tr><td>17</td><td>SICS</td><td>5</td><td>7</td><td>2</td></tr> <tr><td>18</td><td>T2D</td><td>5</td><td>4</td><td>-1</td></tr> <tr><td>19</td><td>TELC</td><td>6</td><td>3</td><td>-3</td></tr> <tr><td>20</td><td>THYIA</td><td></td><td></td><td></td></tr> <tr><td>21</td><td>TUC</td><td>9.6</td><td>9.6</td><td>0</td></tr> <tr><td>22</td><td>UNIGE</td><td>11.5</td><td>11.5</td><td>0</td></tr> <tr><td>23</td><td>UNIUD</td><td>4</td><td>4</td><td>0</td></tr> <tr><td>25</td><td>SES**</td><td>1.8</td><td>0.5</td><td>-1.3</td></tr> <tr> <td></td> <td>TOTAL</td> <td>84.45</td> <td>80.95</td> <td>3.5</td> </tr> </tbody> </table> <p>Total planned: 84.45 Total spent: 80.95 *From September to December 2012 only</p>	Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference	1	MAS	3	3,5	0.5	3	AT	7	5.5	-1.5	4	ATHENA	3	3	0	6	TECNALIA	1	4	3	5	SE*	0.8	0.7	-0.1	7	Alfatroll	2	3	1	8	ETH	6	6	0	9	HAI				11	ISD	12	11.5	-0.5	12	SG*	3.3	1.2	-2.1	15	S-Lab	2.45	2.45	0	16	SESM	1	1	0	17	SICS	5	7	2	18	T2D	5	4	-1	19	TELC	6	3	-3	20	THYIA				21	TUC	9.6	9.6	0	22	UNIGE	11.5	11.5	0	23	UNIUD	4	4	0	25	SES**	1.8	0.5	-1.3		TOTAL	84.45	80.95	3.5
Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference																																																																																																											
1	MAS	3	3,5	0.5																																																																																																											
3	AT	7	5.5	-1.5																																																																																																											
4	ATHENA	3	3	0																																																																																																											
6	TECNALIA	1	4	3																																																																																																											
5	SE*	0.8	0.7	-0.1																																																																																																											
7	Alfatroll	2	3	1																																																																																																											
8	ETH	6	6	0																																																																																																											
9	HAI																																																																																																														
11	ISD	12	11.5	-0.5																																																																																																											
12	SG*	3.3	1.2	-2.1																																																																																																											
15	S-Lab	2.45	2.45	0																																																																																																											
16	SESM	1	1	0																																																																																																											
17	SICS	5	7	2																																																																																																											
18	T2D	5	4	-1																																																																																																											
19	TELC	6	3	-3																																																																																																											
20	THYIA																																																																																																														
21	TUC	9.6	9.6	0																																																																																																											
22	UNIGE	11.5	11.5	0																																																																																																											
23	UNIUD	4	4	0																																																																																																											
25	SES**	1.8	0.5	-1.3																																																																																																											
	TOTAL	84.45	80.95	3.5																																																																																																											

PP

** From January to February 2013	
6	<i>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)</i>
	Not applicable
7	<i>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)</i>
	Not applicable
8	<i>If applicable, propose corrective actions</i>
	Not applicable

Table 2: WP3 Management Report

3.3 WP4

WP4 - Leader Selex Elsag	
Period: 1 September 2012- 28 February 2013	
1	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p> <p>The activities of the third semester of the project have been mainly focused on design and development activities.</p> <p>The results of these activities are described in detail in the deliverable D4.3 “Preliminary SPD network technologies prototype report”, with corresponding developed code/algorithms included in D4.2 “Preliminary SPD node technologies prototype”. The deliverables were submitted as planned, and will be extended and finalized in the second part of the project.</p> <p>The research and designed activities have been focused on the following topics:</p> <ul style="list-style-type: none"> • ATHENA: Recognizing & modelling of denial-of-service attacks • HAI: Coordination of reputation based resource management schemes. Trust aware routing and experimentations with different topologies and RF capabilities/properties. • ISL: Development of a secure channel for the communication of the nSHIELD nodes, based on 6LowPan+IPSEC+IKE. • MAS: • MGEP: Intrusion detection in wireless sensor networks (distributed systems) • SE: Smart SPD-driven transmission layer study and analysis of the distributed self-x models • SG: Preliminary analysis on Integrated Modular Avionics nodes • TECNALIA: Applying SPD metrics for trusted and dependability connectivity to smart grid systems • THYIA: No activity in this period • TUC: Reputation systems for secure routing. Secure communication protocols on the (OSI) network and link layer. • UNIGE: Development of the security-aware framework for Cognitive Radio Networks. In-depth definition of the enablers and requisites for development of the Smart Transmission Layer. • UNIUD: Development of a Cellular Automata inspired computational model for dependable and self-reconfigurable computation. • SES: Project coordination
2	<p><i>Highlight clearly significant and tangible results</i></p> <p>Both project deliverables for this period (D4.2 and D4.3) have been completed on time. The following results in terms of research, design and development have been achieved during this reporting period:</p> <ul style="list-style-type: none"> • ATHENA: simulation and development of a methodology to recognize and model denial-of-service attacks based on network traffic, power consumption and signal strength traffic • HAI: Reputation-based resource management technologies evaluation • ISL: Definition of an outline for Preliminary SDP Network Technologies Prototype Requirements for T4.4 as task coordinators. • MGEP: Preliminary deploy of a reputation based anomaly detection system for IDS suitable for WSN • SE: inputs to the D4.2 and D4.3 deliverables “Preliminary SPD network technologies prototype” and “Preliminary SPD network technologies prototype report” • SG: Preliminary data study for Avionic Scenario

	<ul style="list-style-type: none"> • TECNALIA: contribution for D4.2 • TUC: Contribution to D4.3 and D4.4 Design and implementation (in progress) of a prototype of a novel reputation and trust-based system for secure routing and intrusion detection. • UNIGE: An algorithm for efficient countering of the intelligent jamming attacks in Cognitive Radio Networks was modelled, tested and ported to an embedded platform. • UNIUD: Development of the simulator infrastructure. • SES: No contribution on the deliverables. 																																																																						
3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>No deviation</p>																																																																						
4	<p><i>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)</i></p> <p>Not applicable</p>																																																																						
5	<p><i>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)</i></p> <p>Every partner summarizes the resources spent on WP4 in the dedicated section.</p> <table border="1"> <thead> <tr> <th>Partic. No.</th> <th>Partic. Short name</th> <th>Planned Effort Period M12-M18</th> <th>Spent effort Period M12-M18</th> <th>Difference</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>ATHENA</td> <td>0</td> <td>2.5</td> <td>2.5</td> </tr> <tr> <td>5</td> <td>SE*</td> <td>12.1</td> <td>11</td> <td>1.1</td> </tr> <tr> <td>6</td> <td>TECNALIA</td> <td>4</td> <td>5</td> <td>1</td> </tr> <tr> <td>9</td> <td>HAI</td> <td>3.5</td> <td>3</td> <td>-0.5</td> </tr> <tr> <td>10</td> <td>ISL</td> <td>11</td> <td>11</td> <td>0</td> </tr> <tr> <td>12</td> <td>SG*</td> <td>2.4</td> <td>2</td> <td>-0.4</td> </tr> <tr> <td>13</td> <td>MGEP</td> <td>3</td> <td>3</td> <td>0</td> </tr> <tr> <td>20</td> <td>THYIA</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>21</td> <td>TUC</td> <td>5</td> <td>5</td> <td>0</td> </tr> <tr> <td>22</td> <td>UNIGE</td> <td>10</td> <td>12</td> <td>2</td> </tr> <tr> <td>23</td> <td>UNIUD</td> <td>3</td> <td>3</td> <td>0</td> </tr> <tr> <td>25</td> <td>SES**</td> <td>4.7</td> <td>5.4</td> <td>0.7</td> </tr> <tr> <td></td> <td>TOTAL</td> <td>58.7</td> <td>62.9</td> <td>4.2</td> </tr> </tbody> </table> <p>*From September to December 2012 only ** From January to February 2013</p>	Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference	4	ATHENA	0	2.5	2.5	5	SE*	12.1	11	1.1	6	TECNALIA	4	5	1	9	HAI	3.5	3	-0.5	10	ISL	11	11	0	12	SG*	2.4	2	-0.4	13	MGEP	3	3	0	20	THYIA	0	0	0	21	TUC	5	5	0	22	UNIGE	10	12	2	23	UNIUD	3	3	0	25	SES**	4.7	5.4	0.7		TOTAL	58.7	62.9	4.2
Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference																																																																			
4	ATHENA	0	2.5	2.5																																																																			
5	SE*	12.1	11	1.1																																																																			
6	TECNALIA	4	5	1																																																																			
9	HAI	3.5	3	-0.5																																																																			
10	ISL	11	11	0																																																																			
12	SG*	2.4	2	-0.4																																																																			
13	MGEP	3	3	0																																																																			
20	THYIA	0	0	0																																																																			
21	TUC	5	5	0																																																																			
22	UNIGE	10	12	2																																																																			
23	UNIUD	3	3	0																																																																			
25	SES**	4.7	5.4	0.7																																																																			
	TOTAL	58.7	62.9	4.2																																																																			
6	<p><i>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)</i></p> <p>The SPD Networks cognitive solutions developed in pSHIELD has been considered to be the basis of the ARTEMIS-JU project nSHIELD WP4.</p>																																																																						
7	<p><i>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)</i></p> <p>The major exploitation perspective for technologies developed in WP4 is to push for the</p>																																																																						

	<p>standardization of the SPD Network technologies to obtain a platform that can be used in different context to offer SPD services (or at least the possibility to compose SPD services).</p> <p>Moreover the adoption of cognitive algorithms should be enforced to increase the validity of the platform and other solutions should be taken into account too to extend its applicability.</p> <p>This opens the interactions with projects belonging to the cognitive elaboration area.</p>
8	<i>If applicable, propose corrective actions</i>
	Not applicable.

Table 3: WP4 Management Report

3.4 WP5

WP 5- Leader Selex-ES	
Period: 1 September 2012- 28 February 2013	
	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p>
1	<p><u>Task 5.1 SPD driven Semantics</u></p> <p>Following the guidelines declared in Deliverable 5.1, UNIROMA1 has stated the definition of the new SHIELD models, in order to meet the new project needs.</p> <p>With respect to the identified challenges, and 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.</p> <p>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).</p> <p>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</p> <p>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 UNIROMA1 prototypes.</p> <p>Analysis on semantic parsers in Java language, to be integrated in the OSGI platform, has been performed at design level. However, preloaded models are being prepared as first solution for the prosecution of integration phases.</p> <p>Preliminary Analysis about the integration between policies representation and semantic representation have been started</p> <p>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</p> <p>HAI conducted an assessment on UML diagrams, candidates for the nSHIELD semantic model</p> <p>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.</p> <p>Traditionally non-semantic IDS do not express the modelling of the intrusion detection application in terms of the domain of interest. On the other hand, semantic approaches posit that it is important not only to incorporate the terminology of a domain but also to make sure that domain expert can fully exploit his/her domain expertise for designing his/her intrusion detection application.</p> <ul style="list-style-type: none"> • The following characteristics are an advantage compared to more traditional methods: • Grasping the knowledge of a domain: the domain knowledge can be captured by domain ontology. • Expressing the intrusion detection system much more in terms of the end-user domain: by using the domain ontology, the design of the intrusion system can be expressed in terms of the end-user's domain. • Generating the intrusion detection system more easily: from the knowledge given in the

domain ontology, it is possible to derive a number of properties for an object.

- Making intelligent reasoning: it is not easy to make intelligent reasoning from a scene to the other one. However, it is possible to do that using ontology.

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 the proposed ontologies for intrusion detection

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 stated the design and development of the new SHIELD Middleware Core services, in order to meet the new project needs.

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.

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 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 preliminarily developed in the OSGI framework and represent one of the UNIROMA1 prototypes.

Significant effort has been put in place to enable the new partners to seamlessly integrate with the OSGI heritage from pSHIELD (UNIROMA1 is the owner of the software platform).

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 middleware core services.

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. Identified appropriate technologies and successfully setup existing nSHIELD OSGI framework (Knopflerfish) where identified technologies will be integrated.

Collaborated with partners to identify and address interoperability issues between interfaces and between said interfaces and the nSHIELD platform. Also collaborated with partners to identify 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". This means that this solution does 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.

SLAB developed a preliminary version of intrusion detection service to provide DDoS protection for middleware core and innovative SPD services

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, SE 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.

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 INDRA is 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 responsibilities this node has.

- If `Nodei.getOrganizationalUnit().equal(“STRING”)` decide what kind of functionalities, permissions, roles or responsibilities 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. SE 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)

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

	<p>needs.</p> <p>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.</p> <p>The first formal model for theoretical composability of SPD functionalities have been developed based on Coloured Petri Nets.</p> <p>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</p> <p>Liaisons between the modelling of SPD functionalities for control purposes, and their semantic representation (Task 5.1) have been maintained and enriched.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>HAI has started working on the multi-layered Overlay Security Agent, in the direction of the design of abstracted and open user services</p> <p>Transversal WP activities and remarks:</p> <p>Support to WP5 coordination activities has been provided by UNIROMA1 (in particular it is T5.4 leader)</p> <p>Preliminary investigations to the demonstrator architecture definition for WP6.</p> <p>Maintenance of a repository server to improve WP5 participants' awareness and collaborative work.</p> <p>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.</p>
2	<p><i>Highlight clearly significant and tangible results</i></p> <p>Deliverables:</p> <p>The above mentioned results have been used mainly as major inputs for Deliverable 5.1 on Middleware Technologies assessment.</p> <p>Moreover these results represent a contribution mainly to Deliverable 5.3 in terms of report of designed solutions and Deliverable 5.2 with respect to the development of prototypes.</p> <p>Additional input have been provided to Deliverable 2.X (requirements and architecture refinement)</p> <p>Prototypes:</p> <ul style="list-style-type: none"> • MGEP has created a sample ontology for Intrusion Detection Systems that extends the ontology delivered in pSHIELD • 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

	<ul style="list-style-type: none"> SE has created a Protection Profile for the SHIELD Middleware SE has identified criteria to Policy Definition and classification S-LAB has developed a prototype of Intrusion Detection Bundle 																																																																						
3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>Not applicable</p>																																																																						
4	<p><i>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)</i></p> <p>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.</p> <p>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 (ISL).</p> <p>Due to the delay of the project in the initial phases. We are aware of the deviation, but of course we will deliver the work. Moreover, we have to consider that INDRA has been forced to dedicated more PM in other work packages (1 and 8) due to the nSHIELD meeting in Barcelona and the Press Release (both actions managed by ISL).</p>																																																																						
5	<p><i>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)</i></p> <p>The following table summarizes the use of resources for every partner:</p> <table border="1"> <thead> <tr> <th>Partic. No.</th> <th>Partic. Short name</th> <th>Planned Effort Period M12-M18</th> <th>Spent effort Period M12-M18</th> <th>Difference</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>ATHENA</td> <td>0</td> <td>2</td> <td>2</td> </tr> <tr> <td>5</td> <td>SE*</td> <td>6.2</td> <td>6</td> <td>0.2</td> </tr> <tr> <td>6</td> <td>TECNALIA</td> <td>4</td> <td>3</td> <td>-1.0</td> </tr> <tr> <td>9</td> <td>HAI</td> <td>7</td> <td>6</td> <td>-1.0</td> </tr> <tr> <td>10</td> <td>ISL</td> <td>6</td> <td>6</td> <td>0</td> </tr> <tr> <td>12</td> <td>SG*</td> <td>2.4</td> <td>2</td> <td>-0.4</td> </tr> <tr> <td>13</td> <td>MGEP</td> <td>6.5</td> <td>6.5</td> <td>0</td> </tr> <tr> <td>15</td> <td>S-LAB</td> <td>6</td> <td>7.23</td> <td>1.23</td> </tr> <tr> <td>20</td> <td>THYIA</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>21</td> <td>TUC</td> <td>5.4</td> <td>5.4</td> <td>0</td> </tr> <tr> <td>24</td> <td>UNIROMA</td> <td>9.9</td> <td>10</td> <td>0.1</td> </tr> <tr> <td>25</td> <td>SES**</td> <td>2.8</td> <td>4.9</td> <td>2.1</td> </tr> <tr> <td></td> <td>TOTAL</td> <td>56.2</td> <td>59.03</td> <td>3.23</td> </tr> </tbody> </table> <p>*From September to December 2012 only ** From January to February 2013</p>	Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference	4	ATHENA	0	2	2	5	SE*	6.2	6	0.2	6	TECNALIA	4	3	-1.0	9	HAI	7	6	-1.0	10	ISL	6	6	0	12	SG*	2.4	2	-0.4	13	MGEP	6.5	6.5	0	15	S-LAB	6	7.23	1.23	20	THYIA	0	0	0	21	TUC	5.4	5.4	0	24	UNIROMA	9.9	10	0.1	25	SES**	2.8	4.9	2.1		TOTAL	56.2	59.03	3.23
Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference																																																																			
4	ATHENA	0	2	2																																																																			
5	SE*	6.2	6	0.2																																																																			
6	TECNALIA	4	3	-1.0																																																																			
9	HAI	7	6	-1.0																																																																			
10	ISL	6	6	0																																																																			
12	SG*	2.4	2	-0.4																																																																			
13	MGEP	6.5	6.5	0																																																																			
15	S-LAB	6	7.23	1.23																																																																			
20	THYIA	0	0	0																																																																			
21	TUC	5.4	5.4	0																																																																			
24	UNIROMA	9.9	10	0.1																																																																			
25	SES**	2.8	4.9	2.1																																																																			
	TOTAL	56.2	59.03	3.23																																																																			
6	<p><i>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)</i></p> <p>Not applicable</p>																																																																						

7	<p><i>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)</i></p>
	<p>A press release has been published few months ago in INDRA.</p> <p>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.</p> <p>Post in the Mondragon University ICT blog: http://mukom.mondragon.edu/ict/mu-at-artemis-and-itea-2-co-summit/</p>
8	<p><i>If applicable, propose corrective actions</i></p>
	<p>Organize work groups taking advantage of the next Barcelona meeting. Common agreements should be reached during this meeting, in order to define and clarify the different parts of the work to be performed during 2013 and 2014.</p> <p>Increasing the number of meetings (skype, telephone) in order to coordinate the different proposals of partners involved in WP5.</p>

Table 4: WP5 Management Report

3.5 WP6

WP 6- Leader HAI	
Period: 1 September 2012- 28 February 2013	
1	<i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i>
	<p>The WP aims to:</p> <ul style="list-style-type: none"> • Check the compatibility and proceed to the integration of software and hardware components (upon feasibility) • Develop an nSHIELD System solution • Validate the solution through an iterative and incremental process <p>The WP is separated in the following tasks</p> <ol style="list-style-type: none"> 1. T6.1: Multi-Technology System Integration 2. T6.2: Multi-Technology Validation and Verification 3. T6.3: Multi-Technology SPD Lifecycle Support <p>of which only the last should present activity (through the period of reference).</p>
	<i>Highlight clearly significant and tangible results</i>
	<p>The following deliverable, reflecting to T6.3, is in progress and has a deadline in the end of the reference period:</p> <ul style="list-style-type: none"> • D6.1 Lifecycle and SPD Support Plan (M18) <p>and is expected to be delivered with a short delay. The deliverable will contain the plan for SPD Lifecycle support, based in different standards and international methodologies.</p>
3	<i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i>
	<p>The aforementioned delay mainly concerns the kick off of WP6 and is due to its dependence and necessary interaction with all the WPs of technical development. It is a delay that will have no serious impact on the progress of validating and demonstrating activities.</p>
4	<i>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)</i>
	Not applicable
5	<i>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)</i>
	<p>The following table summarizes the use of resources for every partner:</p>

PP

Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference
1	MAS	1.5	1.5	0
2	ASTS	0	0	0
3	AT	0	0	0
4	ATHENA	0	0	0
5	SE*	3.2	0.1	-3.1
6	TECNALIA	6	7	1
7	ALFA	2	2	0
8	ETH	0	0	0
9	HAI	3	1 Delay in T6.3	-2.0
10	ISL	5.5	5.5	0
11	ISD	0	0	0
12	SG*	1.5	1.3	-0.2
13	MGEP	0	0	0
15	S-LAB	6	0.9 Delay in T6.3	-5.1
23	UNIUD	0	0	0
24	UNIROMA1	0	0	0
26	SES**	0.8	0.2	-0.6
	TOTAL	29.5	19.5	11.0

*From September to December 2012 only
** From January to February 2013

6	<i>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)</i>
	Not applicable
7	<i>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)</i>
	Not applicable
8	<i>If applicable, propose corrective actions</i>
	Not applicable

Table 5: WP6 Management Report6

PP

D1.7

3.6 WP7

WP 7- Leader Movation	
Period: 1 September 2012- 28 February 2013	
1	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p> <p>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.</p> <p>The official starting date of WP7 is with Milestone M3 at 1. March 2013. Though this date is after this reporting period, most of the partners have started activities to ensure that the envisaged applications are in line with the technology developments in nSHIELD.</p> <p>WP7 is organised in four tasks, each of them representing one of the use case scenarios.</p>
2	<p><i>Highlight clearly significant and tangible results</i></p> <p>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.</p>
3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>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 is actively searching for partners being able to enhance the «Social Mobility» use case, which is currently only foreseen as a feasibility study.</p>
4	<p><i>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)</i></p> <p>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.</p>
5	<p><i>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)</i></p> <p>The following table summarizes the use of resources for every partner:</p>

PP

Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference
1	MAS	1	1.	0.
2	ASTS	0	6.02	6.02
3	AT	0	0	0
5	SE	0	0	0
6	TECNALIA	0	0	0
7	ALFA	2	2	0
8	ETH	0	0	0
9	HAI	0	0	0
11	ISD	0	0	0
12	SG	0	0	0
15	S-LAB	0	0	0
16	SESM	2.0	2.0	0
19	TELC	0	0	0
20	THYIA	0	0	0
21	TUC	0	0	0
22	UNIGE	0	0	0
26	SES**	0.6	0	-0.6
	TOTAL	5.6	11.02	5.42

** From January to February 2013

6	<p><i>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)</i></p> <p>The use cases are further developed to enlarge the visibility of the topic «measurable security»</p>
7	<p><i>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)</i></p> <p>The main focus is on targeted dissemination, addressing networks for collaboration in the domain. nSHIELD partners have partly established these networks, and are in collaboration with selected players in the market</p>
8	<p><i>If applicable, propose corrective actions</i></p> <p>Not applicable</p>

Table 6: WP7 Management Report

PP

D1.7

3.7 WP8

WP 8- Leader: MGEP, Mondragon Goi Eskola Politeknikoa	
Period: 1 September 2012 - 28 February 2013	
1	<p><i>A summary progress towards objectives, supported by measurable indicators and details for each task and each partner</i></p> <p>The objectives of WP8 are:</p> <ul style="list-style-type: none"> • Industrial Dissemination • Industrial Standardization of innovative solutions; • Industrial Exploitation of results. <p><u>1. - Dissemination</u></p> <p>This task aims at disseminating the project results and at influencing new standards. A dissemination plan has been internally delivered in the previous period. Dissemination activities will consist in the publication of all important results in well-known conferences and journals (listed in section 2 of this document). 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 (also in section 2).</p> <p><u>2. - Standardization</u></p> <p>The standardization task is a key component to increase the impact in the SPD sector. Close interaction with standardization groups to monitor on-going activities and the preparation of documents and proposals for standardization groups are planned. W standardization plan was internally delivered. As in the project the focus is to deliver missing scientific profound input to extend existing standardization for new intelligent SPD applications. The strong focus on verification, test and validation allows nSHIELD to provide scientific proofed selection guidelines for different technical proposals. This will result in guidelines, quality test procedures and certification rules to cover open needs of end-users. The standardization activities will be led by the strong industrial partnership of the consortium, influencing new and existing standards and regulations, both at European and international level.</p> <p><u>3. - Exploitation</u></p> <p>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. These plans will be updated, in order to adapt them to the evolution of the project and the changes in the relevant markets. Issues of intellectual property and exploitation rights (including patents) will also be coordinated in this task, including potential synergies among the project partners.</p> <p><u>Summary of contribution to WP8 per partner:</u></p> <p>MOVATION (MAS)</p> <p>Movation joined the ARTEMIS Summit in October 2012 together with Mondragon and Selex Elsag to present nSHIELD. As co-founder of the Internet-of-Things Value Creation Network in Norway, Movation co-organised a workshop in February 2013 together with Telenor, Sintef and Standard Norway. Josef Noll was panellist discussing the “way ahead”, where security was a major issue. Ongoing discussions with industrial actors such as ABB, resulting from the IFEA standardisation, are seen as steps ahead towards a common approach. Initial contacts have been established to the Norwegian Oil and Gas Association, and especially the ISO15926 working unit, harmonizing the infrastructure, knowledge and environmental monitoring of all oil and gas activities on the Norwegian shelf. Two of their activities are link to security and risk analysis. Workshops and conferences are agreed to bring the topics towards the operators on the Norwegian shelf.</p>

Ansaldo (ASTS)

No activity in this half

Acorde (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.

ALFA (Alfatroll)

Alfatroll co-organised the UAS Nordic conference in November 2012, collecting high profile business executives from European Countries.

ATHENA (ATHENA)

No activity in this half

Fundacion Tecnalía (TECNALIA)

Tecnalia has participated in WP8 successful progress providing the contributions requested by the leader. Tecnalía is involved in Task 8.1 “Dissemination” of WP8. Tecnalía has identified the dissemination activities in which Tecnalía has planned to participate during the project. Tecnalía has disseminated nSHIELD internally to other divisions: ENERGY division In order to prove it in the smartgrid area. Tecnalía also contributed to D8.2 with Review, feedback and Tecnalía’s dissemination activities. We contacted several industrial and financial organisations in informal meeting and presented nSHIELD project. These organisations are from Basque Country: ZIV, Ikusi, Metro Bilbao.

Eurotech Security ETH (ETH)

ETH has participated to conferences and events on security and has contributed to publication related to security. In particular ETH has adopted the results obtained in WP3 (algorithms for face recognition and face features tracking) in a Eurotech product called “Secucam”.

Hellenic Aerospace Industry (HAI)

HAI dedicated the aforementioned effort in dissemination activities as well as in forming and describing the verification and testing plan for the first draft version of nSHIELD operational manual.

Indra (ISL)

Regarding the dissemination plan Indra (ISL) has published several press releases in many relevant newspapers, media agencies, and technology web portals. Moreover, Indra has uploaded all the mentions of nSHIELD project derived from the press release in the wiki and webpage of nSHIELD project. To check this information, please visit these websites:

- http://nshield.unik.no/wiki/NSHIELD_Dissemination#Public_dissemination
- <http://www.newshield.eu/2012/01/in-the-press/>

Following the same methodology, we have promoted an nSHIELD Internet release for the Indra corporative web portal and also for the Indra’ magazine called “Boletín Global de Noticias” (included in the D8.1.2 in subsection Brochures, flyers and posters). A company magazine available internal and externally.

SELEX Galileo (SG)

SG has contributed on providing information for the nSHIELD website. Support to coordination and dissemination activities.

Mondragon Goi Eskola Politeknikoa (MGEP)

During this period year, MGEP, as leader of WP8 has managed nShield project public website <http://www.newshield.eu>. The elaboration of deliverable D8.4: “SHIELD run-through” (previously known as D8.4: “Operational Manual v1”) has also been coordinated by MGEP. It must be mentioned that the delivery of this document suffered some delay.

MGEP organised and chaired the Embedded System Security Session in the XII Spanish Meeting on Cryptology and Information Security (RECSI 2012) that took place in Donostia-San Sebastián (Spain)

	<p>on 4-7 September 2012. MGEP also promoted nSHIELD internally in the Mondragon University ICT blog: http://mukom.mondragon.edu/ict/mu-at-artemis-and-itea-2-co-summit/</p> <p>Security Evaluation Analysis and Research Lab (S-LAB)</p> <p>No activity in this half</p> <p>Technical University of Crete (TUC)</p> <p>Corrections for the period ending M12) Two papers by TUC have been accepted for inclusion in conference proceedings. A poster regarding the nSHIELD project was presented in a summer school on security and privacy. Work is in progress for extending two conducted surveys on lightweight cryptography primitives for embedded systems (for block ciphers and stream ciphers), so as to submit them to a journal by the end of February 2012.</p> <p>Additions for the period M12-M18) One paper was submitted for journal publication "Embedded Systems Security: A Survey of Research Efforts in the EU", Manifavas C., Fysarakis K., Papanikolaou A., Papaefstathiou I, Submitted to ACM Transactions on Embedded Computing Systems (TECS).</p> <p>SELEX ES (SES)</p> <p>SG has contributed on maintaining contact and updating for the nSHIELD website. Minor coordination activities.</p>
2	<p><i>Highlight clearly significant and tangible results</i></p> <p><u>Deliverables:</u></p> <p><i>Public</i></p> <ul style="list-style-type: none"> • D8.4 SHIELD run-through v1 (M12) / State: Draft version <p><u>Scientific publications by partner:</u></p> <ul style="list-style-type: none"> • Journal papers: <ul style="list-style-type: none"> ○ None during this period • Conference proceedings: <ul style="list-style-type: none"> ○ TUC: George Hatzivasilis, and Charalampos Manifavas. "Building Trust in Ad hoc Distributed Resource-sharing Networks Using Reputation-based Systems". In 16th Panhellenic Conference on Informatics with international participation (PCI 2012), University of Piraeus, Greece, 5-7 October, 2012. <p><u>Other dissemination actions carried out by partners:</u></p> <ul style="list-style-type: none"> • Organization of especial sessions: <ul style="list-style-type: none"> ○ 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. • Presentations: <ul style="list-style-type: none"> ○ Josef Noll presented the Socialtainment use case during the Researchers Night at Kjeller on 28 September 2012. The Researchers Night is part of the Research Days, organised by the Research Council of Norway. ○ Josef Noll was invited to give a keynote on Security, Privacy and Dependability in Mobile Systems at the Second International Conference on Mobile Services, Resources, and Users, Venice, October 2012. • Workshops and exhibitions: <ul style="list-style-type: none"> ○ J. Noll, "Measurable Security in Mobile Networks", Invited Talk at the IDC Enterprise Mobility Series, 28.Nov 2012, Budapest, Hungary.

	<ul style="list-style-type: none"> • Industrial dissemination (companies and institutions contacted): <ul style="list-style-type: none"> ○ Norwegian Defence Research Establishment (FFI). Meeting on 12th September 2012. ○ Alfatroll organizes the UAS Nordic conference 2012, 13.November 2012, Oslo , with high profile representatives from European UAV business. ○ ITEA2/Artemis Co-Summit 2012 took place on 30-31. October 2012 at CNIT in Paris, and nSHIELD was represented by Roberto Uribeetxeberria (Mondragon Goi Eskola Politeknikoa), Josef Noll (Movation/UNIK) and Luigi Trono (Selex Galileo). ○ TECNALIA contacted several industrial and financial organisations in informal meeting and presented nSHIELD project. These organisations are from Basque Country: ZIV, Ikusi, Metro Bilbao. • For other dissemination action such as press releases, please refer to: <ul style="list-style-type: none"> ○ http://nshield.unik.no/wiki/NSHIELD_Dissemination#Public_dissemination ○ http://www.newshield.eu/2012/01/in-the-press/ 																																																		
3	<p><i>If applicable, explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning</i></p> <p>The major deviation is related to the deliverable D8.4: “SHIELD run-through” (previously known as D8.4: “Build Secure Embedded Systems with nSHIELD” v1).</p> <ul style="list-style-type: none"> • 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 should be made during the plenary meeting in Barcelona (March 2013). 																																																		
4	<p><i>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)</i></p> <p>Not applicable.</p>																																																		
5	<p><i>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)</i></p> <p>There were no significant deviations in the use of resources.</p> <table border="1" data-bbox="311 1646 1380 1995"> <thead> <tr> <th>Partic. No.</th> <th>Partic. Short name</th> <th>Planned Effort Period M12-M18</th> <th>Spent effort Period M12-M18</th> <th>Difference</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>MAS</td> <td>1</td> <td>1</td> <td>0</td> </tr> <tr> <td>2</td> <td>ASTS</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>AT</td> <td>0.5</td> <td>0.4</td> <td>-0.1</td> </tr> <tr> <td>4</td> <td>ATHENA</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>SE*</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>6</td> <td>TECNALIA</td> <td>2</td> <td>2.51</td> <td>0.51</td> </tr> <tr> <td>7</td> <td>ALFA</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>8</td> <td>ETH</td> <td>0.6</td> <td>0.6</td> <td>0</td> </tr> <tr> <td>9</td> <td>HAI</td> <td>1</td> <td>2</td> <td>1.0</td> </tr> </tbody> </table>	Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference	1	MAS	1	1	0	2	ASTS	0	0	0	3	AT	0.5	0.4	-0.1	4	ATHENA	0	0	0	5	SE*	0	0	0	6	TECNALIA	2	2.51	0.51	7	ALFA	0	0	0	8	ETH	0.6	0.6	0	9	HAI	1	2	1.0
Partic. No.	Partic. Short name	Planned Effort Period M12-M18	Spent effort Period M12-M18	Difference																																															
1	MAS	1	1	0																																															
2	ASTS	0	0	0																																															
3	AT	0.5	0.4	-0.1																																															
4	ATHENA	0	0	0																																															
5	SE*	0	0	0																																															
6	TECNALIA	2	2.51	0.51																																															
7	ALFA	0	0	0																																															
8	ETH	0.6	0.6	0																																															
9	HAI	1	2	1.0																																															

PP

	10	ISL	2.5	2.5	0
	12	SG*	1.4	1.0	-0.4
	13	MGEP	0.4	0.4	0
	15	S-LAB	0	0	0
	20	THYIA	0	0	0
	21	TUC	0	0	0
	26	SES**	0.6	0.4	-0.2
		TOTAL	10.0	10.81	0.81
	*From September to December 2012 only				
	** From January to February 2013				
6	<p><i>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)</i></p> <p>ISL has contacted teams of the company involved in interesting projects such as ATHENA (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.</p>				
7	<p><i>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)</i></p> <p>The exploitation is expected to be in many business segments such as Transportation, Automation and Manufacturing Industry, Health, etc. One driving force for the exploitation will be the convincing proof-of-concept prototypes and demonstrators that will be developed in nSHIELD. Another one will be the exploitation strategies that will be devised for the projects results that are submitted for standardization.</p> <p>Activities related to standardisation:</p> <ul style="list-style-type: none"> - Standards Norway is a founding member of the Internet of Things Value Network (http://internet-of-things.no), and within Norway we 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. In a meeting on 16Oct2012 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. 				
8	<p><i>If applicable, propose corrective actions</i></p> <p>Not applicable.</p>				

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:	ASTS
Work Package(s)	WP 2 SPD metrics, requirements and system design WP 7 SPD Applications
Task(s)	Task 2.2 Multi-technology SPD metrics Task 7.1 Railway Security
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 2.2 Multi-technology SPD metrics 0 Task 7.1 Railway Security 0
Effort actual or spent in this period:	Task 2.2 Multi-technology SPD metrics 1,82 Task 7.1 Railway Security 6,02
% of work completed at the end of the period (indicative):	Task 2.2 Multi-technology SPD metrics 100% Task 7.1 Railway Security 30%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<p>Task 2.2 Multi-technology SPD metrics:</p> <ul style="list-style-type: none"> ➤ Identification of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration. <p>Task 7.1 Railway Security</p> <ul style="list-style-type: none"> ➤ Definition and analysis of a Reference architecture for the scenario demonstration ➤ Preliminary Analysis of threat scenarios and related risk analysis 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ NTR 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ NTR 	

Meetings performed during the period:

- Pre-review meeting in Budapest 11-12 September 2012
- Review meeting in Rome 17-18 October 2012
- Phone Call on WP 6 - 14 February 2013

Deviations between actual and planned person-months:

- For this period 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:

- NTR

4.1.2 Selex Elsag SE

Beneficiary:	SELEX Elsag
Work Package(s)	<p>WP1 – Project Management</p> <p>WP2 – SPD metrics, requirements and system design</p> <p>WP3 – SPD Node</p> <p>WP4 – SPD Network</p> <p>WP5 – SPD Middleware and Overlay</p> <p>WP6 – Platform integration, validation & demonstration</p> <p>WP7 – SPD Applications</p> <p>WP8 – Knowledge exchange and industrial validation</p>
Task(s)	<p>Task 1.1 – Project management</p> <p>Task 1.2 - Liaisons</p> <p>Task 2.1 - Multi-technology requirements & specification</p> <p>Task 2.2 - Multi-technology SPD metrics</p> <p>Task 2.3 - Multi-technology architectural design</p> <p>Task 3.1 - SDR/Cognitive Enabled node</p> <p>Task 3.2 - Micro node</p> <p>Task 3.3 - Power node</p> <p>Task 3.4 - Dependable self-x Technologies</p> <p>Task 4.1 - Smart SPD driven transmission</p> <p>Task 4.2 - Distributed self-x models</p> <p>Task 4.3 - Reputation-based resource management technologies</p> <p>Task 4.4 - Trusted and dependable Connectivity</p> <p>Task 5.1 – SPD driven Semantics</p> <p>Task 5.2 – Core SPD services</p> <p>Task 5.3 – Policy-based management</p> <p>Task 5.4 – Adaptation of legacy systems</p> <p>Task 6.1 – Multi-Technology System Integration</p> <p>Task 6.2 – Multi-Technology Validation & Verification</p> <p>Task 7.1 – Railways security</p> <p>Task 7.3 – Dependable Avionic Systems</p> <p>Task 7.4 – Social Mobility</p> <p>Task 8.1 – Dissemination</p>
Period:	1 st September 2012 – 31 st December 2012
Effort planned in this period:	<p>Task 1.1 – Project management 2,0 PM</p> <p>Task 1.2 – Liaisons 0,5 PM</p>

PP

	<p>Task 2.2 – Multi-technology SPD metrics – 0.8 PM</p> <p>Task 2.3 – Multi-technology architectural design – 0.3 PM</p> <p>Task 3.3 – Power node 0,4 PM</p> <p>Task 3.4 – Dependable self-x Technologies 0,4 PM</p> <p>Task 4.1 - Smart SPD driven transmission 7,0 PM</p> <p>Task 4.2 - Distributed self-x models 4,5 PM</p> <p>Task 4.3 - Reputation-based resource mngmt. technologies 0,3 PM</p> <p>Task 4.4 - Trusted and dependable Connectivity 0,3 PM</p> <p>Task 5.1 - SPD driven Semantics 2,5 PM</p> <p>Task 5.2 - Core SPD services 0,5 PM</p> <p>Task 5.3 - Policy-based management 1,5 PM</p> <p>Task 5.4 - Adaptation of legacy systems 1,7 PM</p> <p>Task 6.1 - Multi-Technology System Integration 1,6 PM</p> <p>Task 6.2 - Multi-Technology Validation & Verification 1,6 PM</p>
<p>Effort actual or spent in this period:</p>	<p>Task 1.1 – Project management 2,5 PM</p> <p>Task 1.2 – Liaisons 0,5 PM</p> <p>Task 2.2 - Multi-technology SPD metrics – 2.,5 PM</p> <p>Task 2.3 - Multi-technology architectural design – 1,5 PM</p> <p>Task 3.3 - Power node 0,3 PM</p> <p>Task 3.4 - Dependable self-x Technologies 0,3 PM</p> <p>Task 4.1 - Smart SPD driven transmission 5,0 PM</p> <p>Task 4.2 - Distributed self-x models 5,5 PM</p> <p>Task 4.3 - Reputation-based resource management tech. 0,3 PM</p> <p>Task 4.4 - Trusted and dependable Connectivity 0,2 PM</p> <p>Task 5.1 - SPD driven Semantics 1,5 PM</p> <p>Task 5.2 - Core SPD services 1,0 PM</p> <p>Task 5.3 - Policy-based management 1,5 PM</p> <p>Task 5.4 - Adaptation of legacy systems 2,0 PM</p> <p>Task 6.2 - Multi-Technology Validation & Verification 0,1 PM</p>
<p>% of work completed at the end of the period (indicative):</p>	<p>Task 1.1 – Project management – 100%</p> <p>Task 1.2 – Liaisons – 100%</p> <p>Task 2.1 - Multi-technology requirements & specification – 100%</p> <p>Task 2.2 - Multi-technology SPD metrics – 100%</p> <p>Task 2.3 - Multi-technology architectural design – 100%</p> <p>Task 3.1 - SDR/Cognitive Enabled node – 100%</p> <p>Task 3.2 - Micro node – 100%</p> <p>Task 3.3 - Power node – 100%</p> <p>Task 3.4 - Dependable self-x Technologies – 100%</p>

	<p>Task 4.1 - Smart SPD driven transmission – 100%</p> <p>Task 4.2 - Distributed self-x models – 100%</p> <p>Task 4.3 - Reputation-based resource management technologies -100%</p> <p>Task 4.4 - Trusted and dependable Connectivity – 100%</p> <p>Task 5.1 - SPD driven Semantics – 100%</p> <p>Task 5.2 - Core SPD services – 100%</p> <p>Task 5.3 - Policy-based management - 100%</p> <p>Task 5.4 - Adaptation of legacy systems – 100%</p> <p>Task 6.1 - Multi-Technology System Integration – 100%</p> <p>Task 6.2 - Multi-Technology Validation & Verification – 100%</p>
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • Task 1.1 <ul style="list-style-type: none"> ➤ Project Management activities; ➤ Participation to task force call conferences; • Task 2.1 <ul style="list-style-type: none"> ➤ 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; <p><u>Objectives:</u> defining the requirement of the nSHIELD framework driven by the use case</p> <p><u>Results:</u> Preparation of D2.2 deliverable and proposition of a standard methodology</p> • Task 2.2 <ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> • 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 ➤ Contribution to identification of metrics required for the SPD measurements, according to the railway security scenario proposed for the demonstration. ➤ Identification of a formal model for SPD metrics <p><u>Objectives:</u> defining the SPD metrics of the nSHIELD framework</p> <p><u>Results:</u> inputs to the D2.5 deliverable and proposition of a conceptual model approach on metrics</p> • Task 2.3 <ul style="list-style-type: none"> ➤ 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; 	

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 (liaison 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 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, SE 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: inputs to the D5.3 deliverable

• 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 D5.2 deliverables

• 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.

• 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

• Task 8.1

- Contribution to deliverable 8.4

<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none">➤ 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
<p>Corrective actions:</p> <ul style="list-style-type: none">➤ 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
<p>Meetings performed during the period:</p> <ul style="list-style-type: none">➤ 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
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none">➤ Resources have been temporarily diverted from WP6 to WpP2 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.
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none">➤ None

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

Beneficiary:	ETH
Work Package(s)	WP1 – Project Management WP3 – SPD Node WP8 – Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project management Task 3.2 Micro/Personal node Task 8.1 Dissemination Task 8.3 Exploitation
Period:	1 st September 2012 – 28 st February 2013
Effort planned in this period:	Task 1.1 Project management: 0,2 MM Task 3.2 Micro/Personal node: 6 MM Task 8.1 Dissemination: 0,3 MM Task 8.3 Exploitation: 0,3 MM
Effort actual or spent in this period:	Task 1.1 Project management: 0,2 MM Task 3.2 Micro/Personal node: 6 MM Task 8.1 Dissemination: 0,3 MM Task 8.3 Exploitation: 0,3 MM
% of work completed at the end of the period (indicative):	Task 1.1 Project management: 50 % Task 3.2 Micro/Personal node: 96 % Task 8.1 Dissemination: 80 % Task 8.3 Exploitation: 60%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>During the first semester of the second year the activities have been performed in the following tasks:</p> <ul style="list-style-type: none"> ➤ Task 1.1 <ul style="list-style-type: none"> ○ Management activities required by the project: financial and technical planning, management of research activities, review meeting preparation. ➤ Task 3.2 <ul style="list-style-type: none"> ○ 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 	

<p>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).</p> <ul style="list-style-type: none"> ○ 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”. <ul style="list-style-type: none"> ➤ Task 8.1 <ul style="list-style-type: none"> ○ Participation to conferences and events on security. ○ Contribution to publication related to security. ➤ Task 8.3 <ul style="list-style-type: none"> ○ Adoption of the results obtained in WP3 (algorithms for face recognition and face features tracking) in a Eurotech product called “Secucam”.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ No deviations from planned activities during reporting the period.
<p>Corrective actions:</p> <p>-</p>
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ 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 and WP6.
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none"> ➤ There are no deviations between actual and planned efforts in the active tasks during the period.
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none"> ➤ 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”, organized by OSSIF and ABI.

4.1.4 Selex Galileo SG

Beneficiary:	SG
Work Package(s)	WP1 – Project Management WP3 – SPD Node WP4 – SPD Network WP5 – SPD Middleware & Overlay WP8 – Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project management Task 1.2 Liaisons Task 3.1 SDR/Cognitive Enabled node Task 3.2 Micro/Personal node Task 3.3 Power node Task 4.1 Smart SPD driven transmission Task 4.4 Trusted and dependable Connectivity Task 5.1 SPD driven Semantics Task 5.2 Core SPD services Task 6.3 Life cycle SPD support Task 8.1 Dissemination Task 8.2 Standardization
Period:	1 st Sept 2012 – 31 st December 2013
Effort planned in this period:	Task 1.1 Project management – 4 MM Task 1.2 Liaisons –1,5 MM Task 3.1 SDR/Cognitive Enabled node – 1.0 MM Task 3.2 Micro/Personal node – 1.0 MM Task 3.3 Power node – 1.3 MM Task 4.1 Smart SPD driven transmission – 1.2 MM Task 4.4 Trusted and dependable Connectivity – 1.2 MM Task 5.1 SPD driven Semantics – 1.2 MM Task 5.2 Core SPD services – 1.2 MM Task 6.3 Lifecycle SPD support – 1.5 MM Task 8.1 Dissemination – 0.7 MM Task 8.2 Standardization – 0.7 MM
Effort actual or spent in this period:	Task 1.1 Project management – 3.3 MM Task 1.2 Liaisons – 0.7 MM Task 3.1 SDR/Cognitive Enabled node – 0,1 MM Task 3.2 Micro/Personal node – 0.9 MM

	<p>Task 3.3 Power node – 0,2 MM</p> <p>Task 4.1 Smart SPD driven transmission – 1.0 MM</p> <p>Task 4.4 Trusted and dependable Connectivity – 1.0 MM</p> <p>Task 5.1 SPD driven Semantics – 1.0 MM</p> <p>Task 5.2 Core SPD services – 1.0 MM</p> <p>Task 6.3 Lifecycle SPD support – 1.3 MM</p> <p>Task 8.1 Dissemination – 0.5 MM</p> <p>Task 8.2 Standardization – 0.5 MM</p>
<p>% of work completed at the end of the period (indicative):</p>	<p>Task 1.1 Project management – 100%</p> <p>Task 1.2 Liaisons – 100%</p> <p>Task 3.1 SDR/Cognitive Enabled node – 100%</p> <p>Task 3.2 Micro/Personal node – 100%</p> <p>Task 3.3 Power node – 100%</p> <p>Task 4.1 Smart SPD driven transmission – 100%</p> <p>Task 4.4 Trusted and dependable Connectivity – 100%</p> <p>Task 5.1 SPD driven Semantics – 100%</p> <p>Task 5.2 Core SPD services – 100%</p> <p>Task 6.3 Lifecycle SPD support – 100%</p> <p>Task 8.1 Dissemination – 100%</p> <p>Task 8.2 Standardization – 100%</p>
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>The description of the activities performed in the related tasks is provided in the following list:</p> <ul style="list-style-type: none"> ➤ WP1 (Task 1.1, Task 1.2) <ul style="list-style-type: none"> ○ Prepared Q1.6 Quality control Report ○ Management activities required by the project: financial and technical planning, management of research activities, internal review meeting preparation. ○ Several telephone conferences and meeting were held during the first year and several actions were taken in order to facilitate the work between partners. ➤ WP3 (Task 3.1, Task 3.2, Task 3.3) <ul style="list-style-type: none"> ○ Contributing to Integrated Modular Avionics Nodes evaluation focusing on the dependability and real time ➤ WP4 (Task 4.1, Task 4.4) <ul style="list-style-type: none"> ○ Contributing to analysis of data transmission between Integrated Modular Avionics nodes. Integrity and confidentiality of data study for Avionic Scenario. ➤ WP5 (Task 5.1, Task 5.2) <ul style="list-style-type: none"> ○ Contributing to analysis of semantics technology and interoperability between different SPD functionalities ○ participation on review requirements and architecture deliverables with respect to the sections that involve semantic technologies and Core SPD Services with regard to the 	

<p>avionic scenario.</p> <ul style="list-style-type: none">➤ WP6 (Task 6.3)<ul style="list-style-type: none">○ Support to preliminary issue of Life cycle plan➤ WP8 (Task 8.1, Task 8.2)<ul style="list-style-type: none">○ Contribution on providing information for the nSHIELD website.○ Contribution on providing information on nSHIELD Wiki.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none">➤ No deviations from plan for SG during the period.➤ Some deliverables have a delay due to the following reasons: several partners were still working on pSHIELD activities and for them the technology assessment depends on pSHIELD; some partners started their activities later because of a delay in the signature of national contracts.
<p>Corrective actions:</p> <ul style="list-style-type: none">➤ 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.➤ Weekly activity check will be performed in order to keep up with the plan and respect deadlines.
<p>Meetings performed during the period:</p> <ul style="list-style-type: none">➤ TMC on 28/11/2012➤ Several phone conferences with partners to check status of work and communicate actions
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none">➤ At month 16 no deviation from actual and planned.
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none">➤ nSHIELD has been presented at the ARTEMIS & ITEA Co-summit 2012 on October 2012 in Paris

4.1.5 SESM scarl SESM

Beneficiary:	SESM
Work Package(s)	WP3 -SPD Node WP7 - Application
Task(s)	Task 3.3 Power Node Task 7.3 Dependable Avionic
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 3.3 Power Node: 1M Task 7.3 Dependable Avionic: 2 M
Effort actual or spent in this period:	Task 3.3 Power Node: 1M Task 7.3 Dependable Avionic: 2M
% of work completed at the end of the period (indicative):	Task 3.3 Power Node– 40% 6 out of 15 Task 7.3 Dependable Avionic: 12.5% 2 out of 16

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

The Wp3 aims to identify, design and exploit new technologies and new architectural solution that can be employed into SHIELD nodes. The WP3 breakdown structure is organized in subtasks, each of them devoted to specific node type (power node, personal node, nano node, etc.). In such context, SESM is focused, within the task 3.3 – Power node, to identify a node’s architecture and a subset of technologies to be used to endow SHIELD functionalities to heterogeneous large legacy systems. The results of the task 3.3 will be directly exploited into the Wp7. Hence, SESM is involved in the Wp7 – task 7.3 avionic scenario.

Since the Wp7 and Wp3 are in somehow logically interconnected, we envision an adaptation of the WP3’s outcomes (Power Node technologies) to the avionic scenario. The customization/adaptation will be mainly driven by the avionic standards (ARINC 653, DO178, DO254, etc.). Albeit, the WP3’s results will be exploited on an avionic scenario, the Wp3’s outcomes can be adopted in different domain (Transportation, Air Traffic Control, House Automation, etc.) to foster the SHIELD concept.

During the last 6 months the following activities have been performed.

A subset of technologies, to be employed, has been identified and some of them consolidated through test and verification processes. At same time a preliminary architecture has been depicted, as reported into WP3.2. Once all the technologies and the architecture will be consolidated an integration process will be triggered and internal mock-up delivered. The result of such activities (scouting, design, verification and integration) will be an open source ns-ESD-GW, as defined into D2.3, that will expose the following features:

- Monitor Interface
- Data Integrity
- Encryption and Decryption
- Dynamic Reconfiguration
- Abnormal Event detection
- Diagnostic

The ns-ESD-GW is a SHIELD proxy; it acts as an intermediary for requests from SHIELD components seeking SPD resources from L-ESD (Legacy Embedded System Device) and vice versa.

The ns-ESD-GW will foster the usage of the SHIELD methodology into a new embedded system and into a legacy embedded system as well. According to the planned activates, the ns-ESD-GW will encompass the following modules:

- Monitor module;
- Coordination module;
- Security module.

Furthermore, several pivotal steps towards the definition of the avionic scenario, and the integration of the ns-ESD-GW and SHIELD methodology into the avionic scenario have been made. Currently we are in a stage of refinement of the application scenario. In the next moths we will work on the detailed specification of:

- Hardware components;
- Software components;

Due to limited time, we have foreseen a massive usage of COTS component.

Description of criticalities met during the period:

- No any criticisms need to be reported.

Corrective actions:

- No any corrective actions have been performed

Meetings performed during the period:

- Rome Internal Meeting (Galileo Avionica, SESM) 16 Jan 2013, Internal Phone Call 30 January 2013

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

4.1.6 Università degli Studi di Genova UNIGE

Beneficiary:	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 – 28th February 2013
Effort planned in this period:	Task 3.4 Dependable self-x technologies: 4.5 PM Task 3.5 Cryptographic technologies: 5.5 PM
Effort actual or spent in this period:	Task 3.4 Dependable self-x technologies: 4.5 PM Task 3.5 Cryptographic technologies: 5.5 PM
% of work completed at the end of the period (indicative):	Task 3.4 Dependable self-x technologies: 70% Task 3.5 Cryptographic technologies: 80%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • Task 3.4 <ul style="list-style-type: none"> ➤ Preliminary hardware prototype of scalable node according to the nSHIELD three node typology: <ul style="list-style-type: none"> ○ The prototype is an embedded device. ○ The prototype is matching WP2 metrics on Security, Privacy and Dependability ○ The prototype is matching project requirement of scalability. ○ The prototype is matching the requirement of configurability. ➤ Implementation of a demo with the above mentioned prototype: <ul style="list-style-type: none"> ○ Configuration of the on board embedded micro controller as a Linux PC. ○ Compilation of the gnu-gmp libraries for the on board embedded micro controller. ○ Compilation of the Elliptic Curve Cryptography algorithm (Task 3.5) for the on board embedded micro controller. ○ “Execution time” comparison with standard PC. • Task 3.5 <ul style="list-style-type: none"> ➤ Preliminary prototype of the cryptographic framework based on Elliptic Curve Cryptography (ECC), which includes the following modules <ul style="list-style-type: none"> ○ prime finite field arithmetic; ○ conversion of elliptic curve points from affine representation to projective representation; ○ elliptic curve point addition (affine coordinates, Jacobian coordinates); 	

PP

<ul style="list-style-type: none">○ elliptic curve point doubling (affine coordinates, Jacobian coordinates);○ elliptic curve point multiplication (binary method; affine coordinates, Jacobian coordinates)○ elliptic curve point multiplication (Montgomery ladder; affine coordinates, Jacobian coordinates)➤ Testbed: implementation of Diffie-Elmann key-exchange protocol on an embedded microprocessor (ARM) by using the cryptographic framework
Description of criticalities met during the period: <ul style="list-style-type: none">➤ None
Corrective actions: <ul style="list-style-type: none">➤ Not applicable
Meetings performed during the period: <ul style="list-style-type: none">➤ Project meeting September,11, 2012➤ Annual review October, 17, 2012
Deviations between actual and planned person-months: <ul style="list-style-type: none">➤ None
Dissemination activities and exploitation perspectives: <ul style="list-style-type: none">➤ None

PP

D1.7

Beneficiary:	UNIGE
Work Package(s)	WP4 - SPD Network
Task(s)	Task 4.1 Smart SPD driven transmission Task 4.2 Distributed self-x models
Period:	1 st September 2012 – 28 th February 2013
Effort planned in this period:	Task 4.1 Smart SPD driven transmission 5PM Task 4.2 Distributed self-x models 5PM
Effort actual or spent in this period:	Task 4.1 Smart SPD driven transmission 6PM Task 4.2 Distributed self-x models 6PM
% of work completed at the end of the period (indicative):	Task 4.1 Smart SPD driven transmission 35% Task 4.2 Distributed self-x models 35%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • Task 4.1 <ul style="list-style-type: none"> ➤ Final goal <ul style="list-style-type: none"> ○ Design and development of SPD-based transmissions methodologies among nSHIELD node levels ➤ Activities and results <ul style="list-style-type: none"> ○ Finalizing the C++ based cognitive radio simulator able to demonstrate the effectiveness of the proposed defence schemes related to Cognitive Radio and Software Defined Radio security ○ Algorithm for efficient countering of the Smart Jamming Attacks has been designed and tested, and then ported to OMBRA v2.0 embedded platform ○ A detailed technical proposal of the Smart Transmission Layer (in collaboration with Selex Elsag), proposing the means of implementation of the technology (hardware and software components), its enablers and the expected functionality • Task 4.2 <ul style="list-style-type: none"> ➤ Final goal: <ul style="list-style-type: none"> ○ Design of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks ➤ Completed activities: <ul style="list-style-type: none"> ○ Self-x has been defined as an inherent concept of the Security-Aware framework, developed within the task T4.1. Hence, the Security-Aware framework as the property of the Smart Transmission Layer incorporates the self-management and self-reconfigurability potentials of the SDR-based and CR-based nodes. 	
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ 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 	

<p>networks and the corresponding security functionalities (since they heavily depend on the node capabilities)</p> <ul style="list-style-type: none">➤ Unable to contact partner THYIA
<p>Corrective actions:</p> <ul style="list-style-type: none">➤ Clear definition of the nodes' functionalities within WP3➤ Re-distribution of THYIA's work activities, in case it is shown that the partner does not participate in the project anymore
<p>Meetings performed during the period:</p> <ul style="list-style-type: none">➤ nSHIELD project meeting Budapest, 11.9.2012.➤ nSHIELD annual review Rome, 18.10.2012.
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none">➤ Some additional effort was needed for working together with other partners for defining final demonstrators and scenarios and adapting developed algorithms to them.
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none">➤ ---APPROVED FOR PUBLICATION---: 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➤ ---SUBMITTED FOR IEEE SECON 2013---: Kresimir Dabcevic, Lucio Marcenaro, Carlo S. Regazzoni, "Reputation-based frequency switching algorithm for defense against intelligent jamming attacks in centralized Cognitive Radio Networks"

4.1.7 Università degli Studi di Udine UNIUD

Beneficiary:	UNIUD
Work Package(s)	WP1 – Project Management WP2 – SPD metrics, requirements and system design WP3 – SPD node
Task(s)	Task 1.1 – Project management Task 1.2 – Liaisons 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:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 1.1 – Project management: 0.5 PM Task 1.2 – Liaisons: 0 PM Task 2.1 – Multi-technology requirements & specifications: 0 PM Task 2.2 – Multi-technology SPD metrics: 0 PM Task 2.3 – Multi-technology architectural design: 0 PM Task 3.1 – SDR/Cognitive Enabled node: 4 PM Task 3.2 – Micro node: 0 PM Task 3.3 – Power node: 0 PM Task 3.4 – Dependable self-x Technologies: 0 PM Task 3.5 – Cryptographic technologies: 0 PM Task 4.1 – Smart SPD driven transmission: 0 PM Task 4.2 – Distributed self-x models: 3 PM Task 4.3 – Reputation-based resource management technologies: 0 PM

PP

	Task 4.4 – Trusted and dependable connectivity:	0 PM
	Task 6.1 – Multi-technology system integration:	0 PM
	Task 6.2 – Multi-technology validation and verification:	0 PM
	Task 6.3 – Lifecycle SPD support:	0 PM
Effort actual or spent in this period:	Task 1.1 – Project management:	0.5 PM
	Task 1.2 – Liaisons:	0 PM
	Task 2.1 – Multi-technology requirements & specifications:	0 PM
	Task 2.2 – Multi-technology SPD metrics:	0 PM
	Task 2.3 – Multi-technology architectural design:	0 PM
	Task 3.1 – SDR/Cognitive Enabled node:	4 PM
	Task 3.2 – Micro node:	0 PM
	Task 3.3 – Power node:	0 PM
	Task 3.4 – Dependable self-x Technologies:	0 PM
	Task 3.5 – Cryptographic technologies:	0 PM
	Task 4.1 – Smart SPD driven transmission:	0 PM
	Task 4.2 – Distributed self-x models:	3 PM
	Task 4.3 – Reputation-based resource management technologies:	0 PM
	Task 4.4 – Trusted and dependable connectivity:	0 PM
	Task 6.1 – Multi-technology system integration:	0 PM
	Task 6.2 – Multi-technology validation and verification:	0 PM
	Task 6.3 – Lifecycle SPD support:	0 PM
% of work completed at the end of the period (indicative):	Task 1.1 – Project management:	100%
	Task 1.2 – Liaisons:	N.A.
	Task 2.1 – Multi-technology requirements & specifications:	N.A.
	Task 2.2 – Multi-technology SPD metrics:	N.A.
	Task 2.3 – Multi-technology architectural design:	N.A.
	Task 3.1 – SDR/Cognitive Enabled node:	100%
	Task 3.2 – Micro node:	N.A.
	Task 3.3 – Power node:	N.A.
	Task 3.4 – Dependable self-x Technologies:	N.A.
	Task 3.5 – Cryptographic technologies:	N.A.
	Task 4.1 – Smart SPD driven transmission:	N.A.
	Task 4.2 – Distributed self-x models:	100%
	Task 4.3 – Reputation-based resource management technologies:	N.A.
	Task 4.4 – Trusted and dependable connectivity:	N.A.
	Task 6.1 – Multi-technology system integration:	N.A.
	Task 6.2 – Multi-technology validation and verification:	N.A.
	Task 6.3 – Lifecycle SPD support:	N.A.

PP

D1.7

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; email discussions.

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 (nano nodes), we selected a commercial embedded system as reference architecture, in order to perform preliminary evaluations and to have a development target. We selected an ARM based platform as reference board because of 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"), and 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 analysing the hardware behaviour 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 modelled.

- 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 nano node 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 addition 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 file system 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 resumes events that allow 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. To this purpose, a bio-inspired model based on the concept of cellular automata has been developed. The main idea is to allow for the redundant, dynamical commitment to the execution of the different portions of

code composing a specific task. Local policies for the code allocation, message passing, and execution converging to the exact computation have been derived.

➤ Task 4.2

Development of the simulator infrastructure. A C# specification of the modelling infrastructure, implementing the whole policy mechanism of autonomous self-distribution, self-execution, has been realized. Given a logical grid of execution nodes, the simulator allows to inject a generic application, that has been previously decomposed from standard compilation flow into a Static Single Assignment specification of given granularity. The application spread autonomously into a predefined subset of execution nodes and, once triggered, proceeds towards its completion through the implementation of local, nearest neighbours, self-governing execution rules. Data are broadcasted towards the execution node waiting for their arrivals through broadcast, message passing, isotropic communication waves. Once in possess of the input data, each node continues further towards execution generating, in turn, new partial results. The process proceeds until final results are generated, the execution halts and the executing node set are released. The simulator has been successfully tested on sorting application to check its functional behaviour.

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

4.1.8 Università degli studi di Roma “La Sapienza” UNIROMA1

Beneficiary:	UNIROMA1
Work Package(s)	WP1 - Project Management
Task(s)	Task 1.1 Project Management
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 1.1: 0.5 PM
Effort actual or spent in this period:	Task 1.1: 1.0 PM
% of work completed at the end of the period (indicative):	Task 1.1: 200 %
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>In the third semester 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 meeting, document review and cross-contribution to D8.4).</p> <p>UNIROMA1 strongly supported the coordinator in the preparation and execution of the first review meeting. Moreover, UNIROMA1, as Task Leader in WP5, performed additional management activities to set-up and manage WP5 participants.</p>	
<p>Description of criticalities met during the period:</p> <p>Not applicable</p>	
<p>Corrective actions:</p> <p>Not applicable</p>	
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ 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) 	
<p>Deviations between actual and planned person-months:</p> <p>Not applicable</p>	
<p>Dissemination activities and exploitation perspectives:</p> <p>Not applicable</p>	

Beneficiary:	UNIROMA1
Work Package(s)	WP5 - 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:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 5.1 2.2 PM Task 5.2 3.4 PM Task 5.4 4.3 PM
Effort actual or spent in this period:	Task 5.1: 2.2 PM Task 5.2: 3.4 PM Task 5.4: 4.4 PM
% of work completed at the end of the period (indicative):	Task 5.1 100% Task 5.2 100% Task 5.4 102%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
Task 5.1 SPD driven Semantics	
<ul style="list-style-type: none"> ➤ Following the guidelines declared in Deliverable 5.1, UNIROMA1 has stated 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, 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, 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 ➤ 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 UNIROMA1 prototypes. ➤ Analysis on semantic parsers in Java language, to be integrated in the OSGI platform, has 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 the scope of WP2 to contribute and review requirements and architecture deliverables with respect to the sections that involve semantic technologies and their implementation.
- Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Measurable Outcome: The above mentioned results have been used mainly as major inputs for Deliverable 5.1 on Middleware Technologies assessment. Moreover these results represent a contribution mainly to 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)

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 started the design and development of the new SHIELD Middleware Core services, in order to meet the new project needs.
- 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.
- 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 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 preliminarily developed in the OSGI framework and represent one of the UNIROMA1 prototypes.
- Significant effort has been put in place to enable the new partners to seamlessly integrate with the OSGI heritage from pSHIELD (UNIROMA1 is the owner of the software platform).
- 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 middleware core services.
- Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Measurable Outcome: The above mentioned results have been used as major inputs for Deliverable 5.1 on Middleware Technologies assessment. Moreover these results represent a significant part of 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)

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

- 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 represent one of the UNIROMA1 prototype
- Liaisons between the modelling of SPD functionalities for control purposes, and their semantic

<p>representation (Task 5.1) have been maintained and enriched.</p> <ul style="list-style-type: none"> ➤ 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. ➤ 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. ➤ Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work. <p><u>Measurable Outcome:</u> The above mentioned results have been used as major inputs for Deliverable 5.1 on Middleware Technologies assessment. Moreover these results represent a significant part of Deliverable 5.3 in terms of report of designed solutions and Deliverable 5.2 with respect to the development of prototypes.</p> <p>Additional input have been provided to Deliverable 2.X (requirements and architecture refinement)</p> <p>Transversal WP activities and remarks:</p> <ul style="list-style-type: none"> ➤ 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.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ Since UNIROMA1 was the main contributor and owner of the OSGI platform, on which also the nSHIELD prototypes will be developed, a significant time-consuming effort was needed to allow the new partners to integrate their new prototypes into a consolidated software code.
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ No corrective actions are needed because the delay introduced by the above-mentioned criticality has a limited impact on the development phase
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ 14th February, 2013 – Proxy of WP5 for WP6 Phone Call (HAI) ➤ 7th February, 2013 – WP5 Phone Call (SE) ➤ 16th January, 2013 – WP5 Phone Call (SE) ➤ 19th December, 2012 – WP5 Phone Call (SE) ➤ 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)
<p>Deviations between actual and planned person-months:</p> <p>Not applicable</p>

Dissemination activities and exploitation perspectives:

Not applicable

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 preliminary 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.

4.1.9 Selex ES

Beneficiary:	SES
Work Package(s)	<p>WP1 – Project Management</p> <p>WP2 – SPD metrics, requirements and system design</p> <p>WP3 – SPD Node</p> <p>WP4 – SPD Network</p> <p>WP5 – SPD Middleware and Overlay</p> <p>WP6 – Platform integration, validation & demonstration</p> <p>WP7 – SPD Applications</p> <p>WP8 – Knowledge exchange and industrial validation</p>
Task(s)	<p>Task 1.1 – Project management</p> <p>Task 1.2 - Liaisons</p> <p>Task 2.1 - Multi-technology requirements & specification</p> <p>Task 2.2 - Multi-technology SPD metrics</p> <p>Task 2.3 - Multi-technology architectural design</p> <p>Task 3.1 - SDR/Cognitive Enabled node</p> <p>Task 3.2 - Micro node</p> <p>Task 3.3 - Power node</p> <p>Task 3.4 - Dependable self-x Technologies</p> <p>Task 4.1 - Smart SPD driven transmission</p> <p>Task 4.2 - Distributed self-x models</p> <p>Task 4.3 - Reputation-based resource management technologies</p> <p>Task 4.4 - Trusted and dependable Connectivity</p> <p>Task 5.1 – SPD driven Semantics</p> <p>Task 5.2 – Core SPD services</p> <p>Task 5.3 – Policy-based management</p> <p>Task 5.4 – Adaptation of legacy systems</p> <p>Task 6.3 Life cycle SPD support</p> <p>Task 7.1 – Railways security</p> <p>Task 7.3 – Dependable Avionic Systems</p> <p>Task 7.4 – Social Mobility</p> <p>Task 8.1 dissemination</p> <p>Task 8.2 Standardization</p>
Period:	1 st January 2013 – 28 th February 2013
Effort planned in this period:	<p>Task 1.1 – Project management 3,0 PM</p> <p>Task 1.2 – Liaisons 0,7 PM</p>

PP

	<p>Task 2.1 – Multi-technology requirements & specification – 0.0 PM</p> <p>Task 2.2 – Multi-technology SPD metrics – 0.2 PM</p> <p>Task 2.3 – Multi-technology architectural design – 0.2 PM</p> <p>Task 3.1 – SDR/Cognitive Enabled node 0,5 PM</p> <p>Task 3.2 – Micro node 0,5 PM</p> <p>Task 3.3 – Power node 0,7 PM</p> <p>Task 3.4 – Dependable self-x Technologies 0,1 PM</p> <p>Task 4.1 - Smart SPD driven transmission 2.4 PM</p> <p>Task 4.2 - Distributed self-x models 1.5 PM</p> <p>Task 4.3 - Reputation-based resource mngmt. technologies 0,2 PM</p> <p>Task 4.4 - Trusted and dependable Connectivity 0,6 PM</p> <p>Task 5.1 - SPD driven Semantics 1,0 PM</p> <p>Task 5.2 - Core SPD services 1,0 PM</p> <p>Task 5.3 - Policy-based management 0,5 PM</p> <p>Task 5.4 - Adaptation of legacy systems 0,3 PM</p> <p>Task 6.1 - Multi-Technology System Integration 0,4 PM</p> <p>Task 6.2 - Multi-Technology Validation & Verification 0,4 PM</p> <p>Task 7.1 - Railways security 0,6 PM</p> <p>Task 7.3 - Dependable Avionic Systems 0,0 PM</p> <p>Task 7.4 - Social Mobility 0,0 PM</p> <p>Task 8.1 – Dissemination 0,3 PM</p> <p>Task 8.2 – Standardization 0,3</p>
<p>Effort actual or spent in this period:</p>	<p>Task 1.1 Project management – 2.7 MM</p> <p>Task 1.2 Liaisons –0,8 MM</p> <p>Task 2.1 – Multi-technology requirements & specification – 0.0 PM</p> <p>Task 2.2 – Multi-technology SPD metrics – 1,0 PM</p> <p>Task 2.3 – Multi-technology architectural design – 1.0 PM</p> <p>Task 3.1 - SDR/Cognitive Enabled node 0.1 MM</p> <p>Task 3.2 - Micro node 0.1 MM</p> <p>Task 3.3 - Power node 0.3 MM</p> <p>Task 3.4 - Dependable self-x Technologies 0.2 PM</p> <p>Task 4.1 - Smart SPD driven transmission 3.2 PM</p> <p>Task 4.2 - Distributed self-x models 1.5 PM</p> <p>Task 4.3 - Reputation-based resource management tech. 0.2 PM</p> <p>Task 4.4 - Trusted and dependable Connectivity 0,5 PM</p> <p>Task 5.1 - SPD driven Semantics 2.2 MM</p> <p>Task 5.2 - Core SPD services 1.2 PM</p> <p>Task 5.3 - Policy-based management 1,0 PM</p>

PP

	<p>Task 5.4 - Adaptation of legacy systems 0.5 PM</p> <p>Task 6.1 - Multi-Technology System Integration 0,0 PM</p> <p>Task 6.2 - Multi-Technology Validation & Verification 0,0 PM</p> <p>Task 6.3 Lifecycle SPD support – 0.2 MM</p> <p>Task 7.1 - Railways security 0,0 PM</p> <p>Task 7.3 - Dependable Avionic Systems 0.0 PM</p> <p>Task 7.4 - Social Mobility 0,0 PM</p> <p>Task 8.1 – Dissemination 0.2 MM</p> <p>Task 8.2 – Standardization 0.2 MM</p>
<p>% of work completed at the end of the period (indicative):</p>	<p>Task 1.1 – Project management – 10,7%</p> <p>Task 1.2 – Liaisons – 8,3%</p> <p>Task 2.1 - Multi-technology requirements & specification – 35%</p> <p>Task 2.2 - Multi-technology SPD metrics – 43,8%</p> <p>Task 2.3 - Multi-technology architectural design – 75%</p> <p>Task 3.1 - SDR/Cognitive Enabled node – 2,6%</p> <p>Task 3.2 - Micro node – 3,3%</p> <p>Task 3.3 - Power node – 4,9%</p> <p>Task 3.4 - Dependable self-x Technologies – 28,6%</p> <p>Task 4.1 - Smart SPD driven transmission – 11%</p> <p>Task 4.2 - Distributed self-x models – 8,1%</p> <p>Task 4.3 - Reputation-based resource management technologies -11,76%</p> <p>Task 4.4 - Trusted and dependable Connectivity – 12,5%</p> <p>Task 5.1 - SPD driven Semantics – 35,5%</p> <p>Task 5.2 - Core SPD services – 22,6%</p> <p>Task 5.3 - Policy-based management - 8,1%</p> <p>Task 5.4 - Adaptation of legacy systems – 6,3%</p> <p>Task 6.1 - Multi-Technology System Integration - 0%</p> <p>Task 6.2 - Multi-Technology Validation & Verification – 0%</p> <p>Task 6.3 Lifecycle SPD support – 28,6%</p> <p>Task 7.1 - Railways security - 0,0%</p> <p>Task 7.3 - Dependable Avionic Systems – 0,0%</p> <p>Task 7.4 - Social Mobility – 0,0%</p> <p>Task 8.1 – Dissemination – 3,4%</p> <p>Task 8.2 – Standardization 2,5 %</p>
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>The description of the activities performed in the related tasks is provided in the following list:</p> <ul style="list-style-type: none"> ➤ WP1 (Task 1.1, Task 1.2) 	

- Management activities required by the project: financial and technical planning, internal review meeting preparation.
- Contact with the partners to obtain the information to be updated in the Annual Review as required by Antonio Vecchio during the meeting of February in Brussels.
- Contact with THYIA to know the intention of the partner about the proceeding of the project
- Several telephone conferences and meeting were held during those two months and several actions were taken in order to facilitate the work between partners.
- WP2 (Task 2.1, Task 2.2)
 - Contribution (for the Common Criteria related aspects) to determination of metrics in a quantitative and formal way.
- WP3 (Task 3.1, Task 3.2, Task 3.3)
 - Contribution to D3.2 “Preliminary SPD node technologies prototype”
 - Results: inputs to the deliverables D3.2 “Preliminary SPD node technologies prototype” and D3.3 “Preliminary SPD node technologies prototype report”
- WP4 (Task 4.1, Task 4.4)
 - In-depth technical proposal of the Smart SPD-driven transmission layer
 - Preparation of Barcelona meeting presentation (WP4 results)
- WP5 (Task 5.1, Task 5.2)
 - Refinement and tailoring to the middleware architecture (liaison 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”.
 - Collaboration with partners to identify and address interoperability issues between interfaces and between said interfaces and the nSHIELD platform.
 - participation on review requirements and architecture deliverables with respect to the sections that involve semantic technologies and Core SPD Services with regard to the avionic scenario.
 - Preparation of Barcelona meeting presentation (WP5 results)
- WP7 (Task 7.3)
 - Preliminary discussion on the possible integration between OMNIA and nSHIELD goals finalized to the Avionic Demonstrator.
 - Preparation of Barcelona meeting presentation (Avionic Demonstrator)
- WP8 (Task 8.1, Task 8.2)
 - Discussion on the subject of D8.4 and outcomes of project

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
- At month 18 a delay has been required for D5.2 and D5.3. The reviewer accepted to delay the documents of three months. Both the deliverables will be issued by the first half of May. The delay doesn't have impact on the other activities of the project.
- Unable to contact partner THYIA
- Change of coordinator

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.
- Amendments to the project have been approved in order to have better results
- Tasks and duties allocated to partner THYIA have been re-distributed among other partners
- Support to the new coordinator by partners and colleagues

Meetings performed during the period:

- WP5 phone conference 16/01/2013
- WP7 Avionic Scenario meeting in Rome 16/01/2013
- Task Force phone conference 23/01/2013
- PL consultations by phone conference 25/01/2013
- Task force phone conference 13/02/2013
- WP6 phone conference 14/02/2013
- Administrative meeting in Brussels 20/02/2013
- Task force phone conference 27/02/2013

Deviations between actual and planned person-months:

- No deviations from plan for Selex ES during the period.

Dissemination activities and exploitation perspectives:

- The project has is part of the R&D projects portfolio of Selex ES.
- Further activities will be carried out as project execution is more advanced.

4.2 Spain

4.2.1 Acorde Technologies AT

Beneficiary:	AT – Acorde Technologies
Work Package(s)	WP1 - Project management WP2 - Scenarios, requirements and system design WP3 - SPD node WP6 - Platform Integration, validation & demonstration WP7 - SDP Applications WP8 - Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project management 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 3.5 Cryptographic technologies Task 6.1 Multi-technology System Integration Task 6.2 Multi-technology Validation & Verification Task 7.1 Railways security Task 8.1 Dissemination Task 8.2 Standardization
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 1.1 Project management – 0.9 PM Task 2.3 Multi-technology architectural design – 0 PM Task 3.1 SDR/Cognitive Enabled node – 0 PM Task 3.2 Micro Node – 2 PM Task 3.3 Power Node – 2.5 PM Task 3.5 Cryptographic technologies – 2.5 PM Task 6.1 Multi-technology System Integration – 0 PM Task 6.2 Multi-technology Validation & Verification – 0 PM Task 7.1 Railways security – 0 PM Task 8.1 Dissemination – 0.3 PM Task 8.2 Standardization – 0.2 PM
Effort actual or spent in this period:	Task 1.1 Project management – 0.9 PM Task 2.3 Multi-technology architectural design – 0.5 PM Task 3.1 SDR/Cognitive Enabled node – 2.5

	<p>Task 3.2 Micro Node – 0.5 PM</p> <p>Task 3.3 Power Node – 0 PM</p> <p>Task 3.5 Cryptographic technologies – 2.5 PM</p> <p>Task 6.1 Multi-technology System Integration – 0 PM</p> <p>Task 6.2 Multi-technology Validation & Verification – 0 PM</p> <p>Task 7.1 Railways security – 0 PM</p> <p>Task 8.1 Dissemination – 0.3 PM</p> <p>Task 8.2 Standardization – 0.1 PM</p>
<p>% of work completed at the end of the period (indicative):</p>	<p>Task 1.1 Project management 48%</p> <p>Task 2.3 Multi-technology architectural design – 73%</p> <p>Task 3.1 SDR/Cognitive Enabled node – 80%</p> <p>Task 3.2 Micro Node – 14%</p> <p>Task 3.3 Power Node – 0%</p> <p>Task 3.5 Cryptographic technologies – 87%</p> <p>Task 6.1 Multi-technology System Integration – 0%</p> <p>Task 6.2 Multi-technology Validation & Verification – 0%</p> <p>Task 7.1 Railways security – 0%</p> <p>Task 8.1 Dissemination – 30%</p> <p>Task 8.2 Standardization – 40%</p>
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • WP1 (Task 1.1 Project management) <ul style="list-style-type: none"> ➢ 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...). • WP2 (Task 2.3 Multi-technology architectural design) <ul style="list-style-type: none"> ➢ 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. ➢ <u>Results:</u> Deliverable D2.4 has been finalized during this period as an <i>intermediate</i> version of the “System Architecture Design”. • WP3 (Task 3.2, task 3.3, task 3.5) <ul style="list-style-type: none"> ➢ 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. In the first case, AT is working in the design of a “smart power” module, following the architecture proposal done in WP2 (modules and metrics). ➢ 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: <ul style="list-style-type: none"> ○ Measures that are typically implemented at manufacture level as passive physical barriers ○ Measures consisting of continuous monitoring and detection of tamper attacks. 	

<p>AT has investigated different solutions for the first option, encapsulation and physical barriers.</p> <ul style="list-style-type: none"> ➤ <u>Results</u>: These analysis and design will be summarized in the internal deliverable D3.2 and the public one D3.3 • WP6: Platform integration, validation and demonstration <ul style="list-style-type: none"> ➤ 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. • WP8: Knowledge exchange and industrial validation <ul style="list-style-type: none"> ➤ During this period of time the nSHIELD project has been included in the company profile presentations. The nSHIELD project t has been shown in several customer presentations and public conferences where ACORDE has participated.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ Not applicable
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ Not applicable
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ Project meeting, 10th September 2012, Budapest ➤ First Review, 17th October (pre-review meeting) – 18th October (Review) 2012, Rome ➤ WP6 phone meeting: 14th February 2013
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none"> ➤ Tasks that are going to be performed by AT in the scope of T3.2: (Micro Node) needs to be clarified, and it will be done during Barcelona meeting (March 2013).
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none"> ➤ References to the project have been added to be presentations of the company, and included within the R&D projects portfolio. Further activities will be carried out as project execution is more advanced.

4.2.2 Fundación Tecnalía Research & Innovation TECNALIA

Beneficiary:	TECNALIA
Work Package(s)	<p>WP1 – Project Management</p> <p>WP2 – SPD Metrics, Requirements and System Design</p> <p>WP3 – SPD Node</p> <p>WP4 – SPD Network</p> <p>WP5 – SPD Middleware & Overlay</p> <p>WP6 – Platform integration, validation & demonstration</p> <p>WP8 – Knowledge exchange and industrial validation</p>
Task(s)/Deliverables	<p>Task 1.1: Project Management/D1.6 quality control report</p> <p>Task 2.2: Multi-technology SPD metrics/Deliverable 2.8 SPD Metrics specification</p> <p>Task 2.3: Multi-technology architectural design/Deliverable D2.7 Final architecture design</p> <p>Task 3.4: Dependable self-x technologies/Deliverable 3.5 Prototype report</p> <p>Task 3.5: Cryptographic technologies/Deliverable 3.5 Prototype report</p> <p>Task 4.3: Reputation based resource management technologies/Deliverable 4.2 SPD Network technologies prototype</p> <p>Task 4.4: Trusted and dependable Connectivity/ Deliverable 4.2 SPD Network technologies prototype</p> <p>Task 5.2: Core SPD Services/Deliverable 5.2 Preliminary SPD middleware and overlay technologies prototype</p> <p>Task 6.3: Lifecycle support/Deliverable 6.1 Lifecycle and SPD Support Plan</p> <p>Task 8.1: Dissemination/Deliverable: Dissemination</p>
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	<p>Task 1.1: Project Management - 2</p> <p>Task 2.2 Multi-technology SPD metrics - 2</p> <p>Task 2.3: Multi-technology architectural design - 1</p> <p>Task 3.4: Dependable self-x technologies – 0,5</p> <p>Task 3.5: Cryptographic technologies – 0,5</p> <p>Task 4.3: Reputation based resource management technologies - 2</p> <p>Task 4.4: Trusted and dependable Connectivity - 2</p> <p>Task 5.2 Core SPD Services – 4</p> <p>Task 6.3: Lifecycle support - 6</p> <p>Task 8.1: Dissemination – 2</p>
Effort actual or spent in this period:	<p>Task 1.1: Project Management - 3</p> <p>Task 2.2 Multi-technology SPD metrics - 8</p> <p>Task 2.3: Multi-technology architectural design - 2</p>

	Task 3.4: Dependable self-x technologies – 2 Task 3.5: Cryptographic technologies – 2 Task 4.3: Reputation based resource management technologies – 2,5 Task 4.4: Trusted and dependable Connectivity – 2,5 Task 5.2 Core SPD Services – 3 Task 6.3: Lifecycle support - 7 Task 8.1: Dissemination – 2,51
% of work completed at the end of the period (indicative):	Task 1.1: Project Management – 100% Task 2.2 Multi-technology SPD metrics - 90% Task 2.3: Multi-technology architectural design – 80% Task 3.4: Dependable self-x technologies – 100% Task 3.5: Cryptographic technologies – 100% Task 4.3: Reputation based resource management technologies – 100% Task 4.4: Trusted and dependable Connectivity – 100% Task 5.2 Core SPD Services – 100% Task 6.3: Lifecycle support – 90% Task 8.1: Dissemination – 100%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>WP1</p> <p>During October in nSHIELD project meeting it was accepted within the whole consortium to change the leadership of WP2. TECNALIA will lead from November on. TECNALIA will put more efforts in management for coordinating WP2 and its convergences towards the overall coordination and other WPs.</p> <p>Moreover TECNALIA has organised several meetings and conference calls for coordinating WP2. Since January 2013, each month task leaders of WP2 and relevant participants have participated in meeting for correct progress of the WP.</p> <p>WP2</p> <p>TECNALIA in WP2 will be the new coordinator. The main challenge is to distribute the overall work done in WP2 in the rest of the technical WPs such as WP3, WP4 and WP5 and towards the integration of it in WP6.</p> <p>TECNALIA specifically is working in:</p> <ul style="list-style-type: none"> • Task 2.2 <ul style="list-style-type: none"> ➤ Defining a new and novel method of composition of metrics: it will be based on a formal and bounded algorithm very close to incremental certification concepts • Task 2.3 <ul style="list-style-type: none"> ➤ Spreading architectural concepts towards other WPs and relevant tasks. Defining a more detailed architecture. • Result <ul style="list-style-type: none"> ➤ TECNALIA wants to move forward and to make the architecture be more adopted in other technical and integration WPs: This is the challenge for year 2; so that we will need to develop different iterative interactions. 	

WP3

The objective of TECNALIA in WP3 is to contribute analysing the state of the art in the area of security in node level, specifically in mobile area and new secure elements (Cryptographic SD cards, Ad-hoc secure elements and Secured SIM). TECNALIA will also contribute, in summary, studying the possibility of inserting digital certificates for M2M in order to preserve privacy putting PKI infrastructure serving M2M (node to node).

- Task 3.4

- TECNALIA is involved in Task 3.4 “Dependable self-x technologies” of WP3. TECNALIA finished working in Task 3.4. TECNALIA is working in the analysis of inserting digital certificates for M2M in order to preserve privacy putting PKI infrastructure serving M2M (node to node). For doing that, we are analysing the inclusion of a prototype

- Task 3.5

- TECNALIA is involved in Task 3.5 “Cryptographic technologies” of WP3. TECNALIA contributed in Task 3.5 and has participated in WP3 successful progress contributing to WP3 leader requests as well as Task 3.5 leader requests, providing the contributions requested.
- Results:
 - TECNALIA contributions for D3.2

WP4

The objective of TECNALIA on WP4 is to define the mechanisms for task of *reputation* and *trusted and dependable connectivity*. For such a task TECNALIA:

- Contributed to deliverable D4.2 Network Technology Assessment by defining the criteria to follow for reputation based techniques. TECNALIA is analysing the inclusion of its prototype for network SPD technology. (it might be developed in the SmartGrid area)
- Results:
 - TECNALIA contribution for D4.2

WP5

The objective of TECNALIA in WP5 is to contribute to the definition of SPD terminology and taxonomy that will be linked to deliverable 2.8 “SPD metrics” in order to have compliant mechanisms between overlay layer and metric mechanism. TECNALIA has also provided new contributions for new SPD Services (as the choreography service for its analysis) and contributed to the SOTA of task 5.3 “Policy Based Management

- Results:
 - D5.2 SPD Middleware and Overlay technology prototype

WP6

TECNALIA started developing the methodology plan for SPD Lifecycle support. This plan is based in different standards and international methodologies. This plan will execute the final document related of how nSHIELD system must be adopted by final users.

- Result
 - D6.1 SPD Lifecycle support

WP8

TECNALIA has participated in WP8 successful progress providing the contributions requested by the leader.

- Task 8.1

- TECNALIA is involved in Task 8.1 “Dissemination” of WP8. TECNALIA has identified the dissemination activities in which TECNALIA has planned to participate during the project.

<p>➤ Results:</p> <ul style="list-style-type: none"> ○ TECNALIA has disseminated nSHIELD internally to other divisions: ENERGY division In order to prove it in the SmartGrid area. ○ TECNALIA contributions for D8.2. Review, feedback and TECNALIA's dissemination activities.
<p>Description of criticalities met during the period:</p> <p>➤ Change of WP2 leader was a critical challenge to face. TECNALIA will take the opportunity to move WP2 closer to other WPs</p>
<p>Corrective actions:</p> <p>➤ None</p>
<p>Meetings performed during the period:</p> <p>➤ Phone calls each 1 month with WP2 task leaders and participants</p> <p>➤ Phone calls for first tasks of WP3, WP4 and WP5 each 2 month coordinated by task leaders.</p>
<p>Deviations between actual and planned person-months:</p> <p>➤ The deviations between actual and planned person months is because of the fact that the personnel cost rate used to calculate the planned project budget was done by researcher with higher cost rate, and the current personnel cost rate of the people involved in the project is lower than the planned one, but we have included more researchers to cope that gap. Therefore the calculated % work completed at the end of the period reported is not the actual one, in fact the actual %work completed at the end of this period is the planned one.</p>
<p>Dissemination activities and exploitation perspectives:</p> <p>➤ We contacted several industrial and financial organisations in informal meeting and presented nSHIELD project. These organisations are from Basque Country: ZIV, Ikusi, Metro Bilbao</p>

4.2.3 Mondragon Goi Eskola Politeknikoa MGEP

Beneficiary:	MGEP – Mondragon Goi Eskola Politeknikoa
Work Package(s)	WP1 - 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:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 1.1 Project management - PM: 0,5 Task 4.3 Reputation-based resource management technologies - PM: 1,1 Task 4.4 Trusted and dependable Connectivity - PM: 1,9 Task 5.1 SPD driven Semantics - PM: 6,5 Task 6.1 Multi-Technology System Integration - PM: 0 Task 8.1 Dissemination - PM: 0,4
Effort actual or spent in this period:	Task 1.1 Project management - PM: 0,5 Task 4.3 Reputation-based resource management technologies - PM: 1,1 Task 4.4 Trusted and dependable Connectivity - PM: 1,9 Task 5.1 SPD driven Semantics - PM: 6,5 Task 6.1 Multi-Technology System Integration - PM: 0 Task 8.1 Dissemination - PM: 0,4
% of work completed at the end of the period (indicative):	Task 1.1 Project management - 50% Task 4.3 Reputation-based resource management technologies - 40% Task 4.4 Trusted and dependable Connectivity - 40% Task 5.1 SPD driven Semantics - 90% Task 6.1 Multi-Technology System Integration - 0% Task 8.1 Dissemination - 35%

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

During this six-month 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 align 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 two days technical meeting in Budapest 11-12/09/2012 and the nSHIELD first year review in Rome 18/10/2012 as well as the Artemis-Itea2 co-summit in Paris 30-31/10/2012 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. If the local agent cannot determine the behaviour of an activity, this agent will contact with the agents near him to determine if that activity is malicious or not. Once that one activity is considered malicious, the IDS will take necessary measures to mitigate the situation.

IDS agents located in nodes are compounded by five parts; Local Data Collection module gathers different inputs, systems logs, network traffic or sensor values. After, recollected inputs are analysed by Local Detection Engine that will raise alarm flag if finds evidence of malicious activities. Once alarm is raised the Local Response and Global Response will take care of the situation to mitigate the failure. But if the Local Detection engine cannot determine the conduct of certain behaviour, the Cooperative Detection engine will ask nodes' opinion about that activity, to define if it is normal or malicious.

The detection system proposed for this IDS is an hybrid between anomaly and specification-based detection systems. At the initialization of the system some specific parameters are configured, as response time or frequency of notifications. This allows the IDS to monitor the different protocols of the system and search for possible attacks. Besides, the IDS also have a series of rules based on node behaviour to cover the widest range of attacks that would not be covered with specification-based detection. To determine the behaviour of a node, reputation and trust is used.

We have considered IDS based on cooperation between nodes and fully distributed architecture. Keeping these two main features we propose architecture of cooperation, based on reputation to create a network of autonomous sensors capable of detecting most kind of attacks and network failures using an anomaly detection system together with specification-based detection system. All this designed from the premise of creating a system that fits the characteristics of sensor networks and maintaining the protocol as lightweight as possible to guarantee the autonomy of the nodes.

➤ **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.

- Results: We have proposed a reputation based anomaly detection system for IDS suitable for WSN. We have started deploying our algorithms in a WSN composed by Z1 low-power wireless modules. The Z1 module is a general-purpose development platform for wireless sensor networks (WSN) designed for researchers and developers (<http://www.zolertia.com/products/Z1>). Later we will implement the same systems in the HW chosen by the consortium for demonstrators.

➤ Task 5.1 SPD driven Semantics

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.

Traditionally non-semantic IDS do not express the modelling of the intrusion detection application in terms of the domain of interest. On the other hand, semantic approaches posit that it is important not only to incorporate the terminology of a domain but also to make sure that domain expert can fully exploit his/her domain expertise for designing his/her intrusion detection application.

The following characteristics are an advantage compared to more traditional methods:

- Grasping the knowledge of a domain: the domain knowledge can be captured by domain ontology.
- Expressing the intrusion detection system much more in terms of the end-user domain: by using the domain ontology, the design of the intrusion system can be expressed in terms of the end-user's domain.
- Generating the intrusion detection system more easily: from the knowledge given in the domain ontology, it is possible to derive a number of properties for an object.
- Making intelligent reasoning: it is not easy to make intelligent reasoning from a scene to the other one. However, it is possible to do that using ontology.

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 the proposed ontologies for intrusion detection

- Results: MGEP has created sample ontology for Intrusion Detection Systems that extends the ontology delivered in pSHIELD.

➤ Task 6.1 Multi-Technology System Integration

This task has not started yet. Start date is Month 19.

➤ Task 8.1 Dissemination

During this period year, MGEP, as leader of WP8 has managed nSHIELD project public website <http://www.newshield.eu>. The elaboration of deliverable D8.4: "SHIELD run-through" (previously known as D8.4: "Operational Manual v1") has also been coordinated by MGEP. It must be mentioned that the delivery of this document suffered some delay (see "criticalities" section below).

- Results:
 - 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/>

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.

Another cause of deviation in WP4 is the lack of a common platform for demonstrators.

- Participants in WP4 have already identified candidates for this, but as the final decision has not been made we are using a general-purpose development platform for WSN.

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 should be made during the plenary meeting in Barcelona (March 2013).

- In order not to stop the implementation work, participants in WP4 are using general-purpose development platforms. Once the final decision about the common demonstrator platform is made (expected for the Barcelona meeting in March 2013) porting the solution from the actual frameworks should not be a major issue.

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 18 October 2012

Phone conferences:

- 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:

- Deliverables related to Dissemination on WP8:
 - MGEP has coordinated and contributed to D8.4: "SHIELD run-through" (draft version, final delayed)
 - Management of www.newshield.eu
- Papers published with results from nSHIELD:

-
- No paper was published during this period
 - 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.
 - 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:	ISL
Work Package(s)	WP1 - Management
Task(s)	Task 1.1 Project Management
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 1.1 Project Management → 1,8 PM
Effort actual or spent in this period:	Task 1.1 Project Management → 1,8 PM
% of work completed at the end of the period (indicative):	Task 1.1 Project Management → 18% of the overall T1.1
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>Basically in this period, the most important task performed in this period has been the first 2013 nSHIELD meeting coordination (Barcelona).</p> <p>➤ Task 1.1 Project Management, 16% of work completed at the end of the period for the following specific tasks:</p> <ul style="list-style-type: none"> ➤ 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 of our company; ➤ Approving and validating the visible outputs, such as deliverables, presentation material, papers, etc., thus adding a level of quality assurance to the project; ➤ Supervising the website (more related with WP8); 	
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ We do not identified in this period for this work package. 	
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ 	
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ Phone call with the project coordinator at the end of December to confirm the location of the meeting (Athens or Barcelona). 	
<p>Deviations between actual and planned person-months:</p>	
<p>Dissemination activities and exploitation perspectives:</p>	

PP

Beneficiary:	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:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 4.3 Reputation-based resource management technologies → 6 PM Task 4.4 Trusted and dependable connectivity → 5 PM
Effort actual or spent in this period:	Task 4.3 Reputation-based resource management technologies → 6 PM Task 4.4 Trusted and dependable connectivity → 5 PM
% of work completed at the end of the period (indicative):	Task 4.3 Reputation-based resource management technologies → 50% Task 4.4 Trusted and dependable connectivity → 23% (Overall percentages)
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>Our effort in this package is based on providing security, privacy and dependability features in the network layer. In order to face these challenges, we will face security in the link and network layer (layer 2 and 3 of the OSI reference model). Taking our technical experience into account and following the internal work package agreements, our company will propose a clear leadership for T4.4.</p> <ul style="list-style-type: none"> ➤ Task 4.4 Trusted and dependable connectivity, 16% of work completed at the end of the period for the following specific tasks: <ul style="list-style-type: none"> ➤ 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. ➤ Contribute to T4.4 in the Preliminary SPD Network Technologies Prototype Requirements. 	
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ Probably it will be better if we had defined at the beginning of the project the hardware reference and the operative system reference to work with. 	
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ Increasing the number of meetings (skype, telephone) in order to coordinate the different proposals of partners involved in WP4. 	
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ 2 WP4 skype conferences (December 2012). ➤ 24th January 2013 Skype conference with Kresimir and Lucio in order to talk about Indra's proposals for WP4. 	

PP

D1.7

PP

Deviations between actual and planned person-months:

Not applicable

Dissemination activities and exploitation perspectives:

Not applicable

Beneficiary:	ISL
Work Package(s)	WP5 - SPD Middleware and Overlay
Task(s)	Task 5.3 Policy-based Management
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 5.3 Policy-based Management → 6 PM
Effort actual or spent in this period:	Task 5.3 Project Management → 6 PM
% of work completed at the end of the period (indicative):	Task 5.3 Policy-based Management → 33% of the overall T5.3
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>➤ Task 1.5 Policy-based Management, 10% of work completed at the end of the period for the following specific tasks:</p> <p>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.</p> <p>In this task INDRA is studying what kind of policies can be proposed, among all, INDRA has identified the following kind:</p> <ul style="list-style-type: none"> • Power policy-based: change the roles of the nodes in function of the battery or power life of them. For instance: <ul style="list-style-type: none"> ○ If <code>Nodei.getremaingBattery() <= threshold</code> then REDUCE the routing capabilities of the node and turn it into a “leaf node”. <p>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.</p> ○ If <code>Nodei.getremaingBattery() <= threshold</code> then CHANGE the routing capabilities of the node. <p>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.</p> • Security policy-based: change the roles of the nodes in function of the certificates of nodes. For instance: <ul style="list-style-type: none"> ○ If <code>Nodei.getFQDN().equal("STRING")</code> decide what kind of functionalities, permissions, roles or responsibilities this node has. ○ If <code>Nodei.getOrganizationalUnit().equal("STRING")</code> decide what kind of functionalities, permissions, roles or responsibilities this node has. <p>Summarizing use the nodes' certificates to apply policies in the middleware or application layer.</p> 	
<p>Description of criticalities met during the period:</p> <p>➤ We have to congratulate Andrea Fiaschetti and Andrea Morgani, given that they are great WP</p>	

coordinators. Their efforts and proposals in this (and other WPs) are essential.
Corrective actions: <ul style="list-style-type: none">➤ Increasing the number of meetings (Skype, telephone) in order to coordinate the different proposals of partners involved in WP5.
Meetings performed during the period: <ul style="list-style-type: none">➤ 3 WP5 Skype conferences (December 2012, January 2013, February 2013).
Deviations between actual and planned person-months: <p>Due to the delay of the project in the initial phases.</p>
Dissemination activities and exploitation perspectives: <p>Not applicable</p>

PP

Beneficiary:	ISL
Work Package(s)	WP6 - Platform Integration, validation and Demonstration
Task(s)	Task 6.1 Multi-technology System Integration
Period:	1st Sept 2012 – 28st February 2013
Effort planned in this period:	Task 6.1 Multi-technology System Integration → 5,5 PM
Effort actual or spent in this period:	Task 6.1 Multi-technology System Integration → 5,5 PM
% of work completed at the end of the period (indicative):	Task 6.1 Multi-technology System Integration → 23%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
Not Integration nor validation and demonstration could be possible if we are developing the SPD Network, Middleware and Overlay.	
Description of criticalities met during the period:	
➤	
Corrective actions:	
➤	
Meetings performed during the period:	
➤	
Deviations between actual and planned person-months:	
Is not possible to integrate, validate or demonstrate a global platform if we are not ready to do it, given that previous work packages are delayed.	
Dissemination activities and exploitation perspectives:	
Not applicable	

PP

D1.7

PP

Beneficiary:	ISL
Work Package(s)	WP8 - Dissemination and Exploitation
Task(s)	Task 8.1 Dissemination Task 8.3 Exploitation
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 8.1 Dissemination → 1 Task 8.2 Standardization → 1,5 Task 8.3 Exploitation → 0 (TOTAL 14)
Effort actual or spent in this period:	Task 8.1 Dissemination → 1 Task 8.2 Standardization → 1,5 Task 8.3 Exploitation → 0
% of work completed at the end of the period (indicative):	Task 8.1 Dissemination → 20% Task 8.2 Standardization → 37% Task 8.3 Exploitation → 6% (Overall percentages)
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<p>➤ Task 8.1 Dissemination, 50% of work is completed in order to achieve the dissemination goals of the project. 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.</p> <p>➤ Also we are involved in Deliverable D8.1.2 Dissemination Plan. Regarding the dissemination plan INDRA is working on:</p> <ul style="list-style-type: none"> ○ 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. <ul style="list-style-type: none"> ▪ 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 ...). <p>Press Release has been published with a high media impact.</p> <ul style="list-style-type: none"> ○ 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). 	

<ul style="list-style-type: none"> ○ 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/ <p>➤ Also we are involved in Deliverable D8.3 Standardization Plan, completing the following sections:</p> <ul style="list-style-type: none"> ➤ 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.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ We do not identified in this period for this work package.
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ None
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ Phone call with Luigi at the end of December to decide the location of the meeting (Athens or Barcelona).
<p>Deviations between actual and planned person-months:</p> <p>Not applicable</p>
<p>Dissemination activities and exploitation perspectives:</p> <p>Not applicable</p>

4.3 Slovenia

4.3.1 THYIA Tehnologije

No information received from THYIA.

Beneficiary:	THYIA
Work Package(s)	No Information received
Task(s)	No Information received
Period:	1st Sept 2012 – 28st February 2013
Effort planned in this period:	No Information received
Effort actual or spent in this period:	No Information received
% of work completed at the end of the period (indicative):	No Information received
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
No Information received	
Description of criticalities met during the period:	
No Information received	
Corrective actions:	
No Information received	
Meetings performed during the period:	
No Information received	
Deviations between actual and planned person-months:	
No Information received	
Dissemination activities and exploitation perspectives:	
No Information received	

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.

4.4.1 Movation AS (MAS) and Alfatroll (ALFA)

Beneficiary:	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:	1st Sept 2012 – 28th February 2013
Effort planned in this period:	Task 6.1 – Multi-technology System Integration – 1.5 + 2 PM Task 6.2 – Multi-Technology Validation & Verification – 0 PM Task 7.1 – Railroad Security – 2 PM Task 7.3 – Dependable Avionic Systems - 0 + 2 PM Task 7.4 – Social Mobility – 0.5 PM Task 8.1 – Dissemination - 0 PM Task 8.2 – Standardization – 0.5 PM Task 8.3 – Exploitation – 0 PM
Effort actual or spent in this period:	Task 6.1 – Multi-technology System Integration – 1.5 +2 PM Task 6.2 – Multi-Technology Validation & Verification – 0 PM Task 7.1 – Railroad Security – 0 PM Task 7.3 – Dependable Avionic Systems – 0.5 + 2 PM Task 7.4 – Social Mobility – 0.5 PM Task 8.1 – Dissemination – 1 PM

	Task 8.2 – Standardization – 0 PM Task 8.3 – Exploitation – 0 PM
% of work completed at the end of the period (indicative):	Task 6.1 – Multi-technology System Integration –20% Task 6.2 – Multi-Technology Validation & Verification - Task 7.1 – Railroad Security – 60% Task 7.3 – Dependable Avionic Systems – 60% Task 7.4 – Social Mobility – 20% Task 8.1 – Dissemination – 40% Task 8.2 – Standardization – 30 % Task 8.3 – Exploitation – 20 %
<p>This description of the activities contains the contribution from all partners (Movation, Alfatroll) of Norway in nSHIELD:</p> <ul style="list-style-type: none"> ➤ 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 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. ➤ Movation also worked on getting the fourth use case, Social Mobility, back on track. Due to changes in partners, we don't have a core team with sustainable PM committed to the task 7.4. 	
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ 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 little ➤ (ii) Movation is actively searching for a good partner from the embedded world to drive the Social Mobility scenario. 	
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ (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) Through the network of 150+ SMEs and contacts to the industry we are convinced to be able to present a partner focussing on the feasibility of the SHIELD approach in the Social Mobility scenario. 	
<p>Meetings performed during the period:</p>	

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

	<u>Date</u> 	<u>Phone</u> 
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.

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 conferences 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).

4.5 Sweden

4.5.1 Swedish Institute of Computer Science SICS

Beneficiary:	SICS
Work Package(s)	WP2 - SPD metrics, requirements and system design WP3 - SPD Node
Task(s)	Multi-technology architectural design
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 2.1 Multi-technology requirements & specification: 0,7 MM Task 2.3 Multi-technology architectural design: 0,3 MM Task 3.1 Nano node 2MM Task 3.2 Micro/Personal node 2 MM Task 3.3 Power node 1 MM
Effort actual or spent in this period:	Task 2.1 Multi-technology requirements & specification: 0,7 MM Task 2.3 Multi-technology architectural design: 0,3 MM Task 3.1 Nano node 1MM Task 3.2 Micro/Personal node 5 MM Task 3.3 Power node 1 MM
% of work completed at the end of the period (indicative):	Task 2.1 Multi-technology requirements & specification: 90% Task 2.3 Multi-technology architectural design: 80% Task 3.1 Nano node 50% Task 3.2 Micro/Personal node 90% Task 3.3 Power node 50%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>WP2</p> <ul style="list-style-type: none"> ➤ Before, at the Budapest meeting, and directly after the meeting we have been working 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. <ul style="list-style-type: none"> • Task 2.1 <ul style="list-style-type: none"> ➤ 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. • Task 2.3 <ul style="list-style-type: none"> ➤ Review of the current system architecture and suggestions for modifications/improvements. 	

WP3

- 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.
- **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.
 - Work on porting the hypervisor to Linux was started and the porting design was settled.
- **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 BeagleBone.
 - Hypervisor performance figures were collected for running Free RTOS on the hypervisor.
 - Work on porting the hypervisor to Linux was started and the porting design was settled. We have almost completed the Linux port at the end of the period and expect a full running port the beginning of March.
 - We have evaluated and designed Global Platform support on the BeagleBone. We expect the full support to be ready at next reporting period.
 - 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 time.
- **Task 3.3**
 - We assisted with looking into the power node requirements and system architecture design together with the rest of the nSHIELD partners.

Description of criticalities met during the period:

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

Corrective actions:

- The systems requirements document quality was not met and identified during the nSHIELD internal review. We together with Selex managed to improve the quality by changing the requirement handling process and timely submit new collected requirements prior to the Rome review.
- We are currently in time with the original WP3 schedule.

Meetings performed during the period:

- nSHIELD face-to-face meeting in Budapest, September 11&12, 2012. Participants from SICS: Christian Gehrman.
- nSHIELD review meeting in Rome, October 17&18, 2012. Participants from SICS: Christian Gehrman and Viktor Do.
- nSHIELD specification working meeting, December 4, 2012. Participants from SICS: Christian Gehrman
- nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24,

PP

2013. Participants from SICS: Christian Gehrmann
--

Deviations between actual and planned person-months:

- | |
|---|
| <ul style="list-style-type: none">➤ We had no deviations between actual and planned efforts in WP2 during the period.➤ We had no deviations between actual and planned efforts in WP3 during the period. |
|---|

Dissemination activities and exploitation perspectives:
--

- | |
|--|
| <ul style="list-style-type: none">➤ No dissemination activities related to our WP3 work was performed during the period but is planned for the next when we have completed the Linux port and the Global Platform support. |
|--|

4.5.2 T2 Data AB T2D

Beneficiary:	T2D
Work Package(s)	WP2 - SPD metrics, requirements and system design
Task(s)	Multi-technology architectural design
Period:	1 st Sept 2012 – 29 st February 2013
Effort planned in this period:	Task 2.1 Multi-technology requirements & specification: 0.3 MM h Task 2.3 Multi-technology architectural design: 0.3MM
Effort actual or spent in this period:	Task 2.1 Multi-technology requirements & specification: 0.3 MM h Task 2.3 Multi-technology architectural design: 0.3 MM h
% of work completed at the end of the period (indicative):	Task 2.1 Multi-technology requirements & specification: 70% Task 2.3 Multi-technology architectural design: 70%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> ➤ Task 2.1 <ul style="list-style-type: none"> ➤ Improved structure for Preliminary System Requirements and Specifications. ➤ Contributed to improved mapping of requirement between platform and application. ➤ Task 2.3 <ul style="list-style-type: none"> ➤ Review of architecture. 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ Contributed to delivery of nSHIELD review. 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Comments on presentations during the preparations prior to review in Rome. Applications requirement versus platform requirements. 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Budapest, September 11-12, 2012. ➤ Rome, October 17-18, 2012. ➤ nSHIELD specification with SICS , December 4, 2012 ➤ nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24. 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ We had no deviations between actual and planned efforts in WP2 during the period. 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ No dissemination activities was planned or performed during the period. 	

Beneficiary:	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:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 3.1 Nano node 2MM Task 3.2 Micro/Personal node 2 MM Task 3.3 Power node 1 MM
Effort actual or spent in this period:	Task 3.1 Nano node 1MM Task 3.2 Micro/Personal node 2 MM Task 3.3 Power node 1 MM
% of work completed at the end of the period (indicative):	Task 3.1 Nano node 50% Task 3.2 Micro/Personal node 90% Task 3.3 Power node 50%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> ➤ Secure boot integration with SICS, ➤ Task 3.1 <ul style="list-style-type: none"> ➤ A secure boot design developed together with SICS and we successfully showed secure boot of the SICS hypervisor and FreeRTOS on Beaglebone. ➤ Modular design of firmware. ➤ I2C driver for parameter management and memory sizing. ➤ Contributed to Preliminary SPD Node Technologies Prototype (D3.2). ➤ Contributed to Preliminary SPD Node Technologies Prototype Report (D3.3). ➤ Task 3.3 <ul style="list-style-type: none"> ➤ power node version of boot algorithm. 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ No deviations from plan during the period. 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ We are currently in time with the original WP3 schedule. 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ nSHIELD face-to-face meeting in Budapest, September 11&12, 2012 ➤ nSHIELD review meeting in Rome, October 17&18, 2012 	

-
- | |
|---|
| <ul style="list-style-type: none">➤ nSHIELD specification working meeting, December 4, 2012➤ nSHIELD Swedish node co-ordination face- to-face meeting at Telcred, Stockholm, January 24. |
|---|

Deviations between actual and planned person-months:

- | |
|---|
| <ul style="list-style-type: none">➤ We had no deviations between actual and planned efforts in WP3 during the period. |
|---|

Dissemination activities and exploitation perspectives:
--

- | |
|--|
| <ul style="list-style-type: none">➤ No dissemination activities related to our WP3 work was performed during the period but is planned for the next when we have completed the Linux port and the Global Platform support. |
|--|

4.5.3 Telcred TELC

Beneficiary:	TELC
Work Package(s)	WP3 - SPD Node
Task(s)	Task 3.2 Micro node Task 3.5 Cryptographic technologies
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 3.2 Micro node 0 PM Task 3.5 Cryptographic technologies 1 PM
Effort actual or spent in this period:	Task 3.2 Micro node 0 PM Task 3.5 Cryptographic technologies 0.1 PM
% of work completed at the end of the period (indicative):	Task 3.2 Micro node 100% Task 3.5 Cryptographic technologies 5%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 3.2 <ul style="list-style-type: none"> ➤ 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 <ul style="list-style-type: none"> ➤ Initial discussions with UNIGE during nSHIELD meeting in Budapest and with SICS in Stockholm. ➤ Results: None so far (work on this task has just started). 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ 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. 	
Corrective actions:	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Feb 24th meeting with SICS and T2D 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ Task 3.2: No deviations ➤ Task 3.3: 0.9 PM less than expected. We had expected to start this activity, but are waiting for UNIGE. 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ M.Sc. thesis produced (but not yet published). 	

4.6 Hungary

4.6.1 Security Evaluation Analysis and Research Lab. S-LAB

Beneficiary:	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
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
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	2.2 - Multi-technology SPD metrics: 2MM 3.4 - Dependable self-x Technologies: 1.2MM 3.5 - Cryptographic technologies: 1.25MM 5.2 - Core SPD services: 6MM 6.3 - Lifecycle SPD Support: 6MM
Effort actual or spent in this period:	2.2 - Multi-technology SPD metrics: 1.96MM 3.4 - Dependable self-x Technologies: 1.2MM 3.5 - Cryptographic technologies: 1.25MM 5.2 - Core SPD services: 7.23MM 6.3 - Lifecycle SPD Support: 0.9MM
% of work completed at the end of the period (indicative):	2.2 - Multi-technology SPD metrics: 3.4 - Dependable self-x Technologies: 100% 3.5 - Cryptographic technologies: 100% 5.2 - Core SPD services: 50% 6.3 - Lifecycle SPD Support: 10%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	<ul style="list-style-type: none"> • Tasks 2.1 and 2.2 <ul style="list-style-type: none"> • Requirements, specification, and SPD metrics development work (continuation of work for

<p>previous period)</p> <ul style="list-style-type: none"> • Tasks 3.4 and 3.5 <ul style="list-style-type: none"> • Security evaluation methodology for partners' technologies • Results: to be used in later phases of WP3 and WP6 • Task 5.2 <ul style="list-style-type: none"> • preliminary version of technologies for middleware core and innovative SPD services • prototype of Intrusion Detection Bundle <ul style="list-style-type: none"> ➤ Results: D5.2 and D5.3 • Task 6.3 <ul style="list-style-type: none"> ➤ Revision of D6.1 Lifecycle SPD Support Plan deliverable ➤ Planning of integration / validation activities ➤ Results: deliverable D6.1 Lifecycle SPD Support Plan
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ WP5 efforts for future periods is now forecast to be higher than defined (14MMs), thus effort reallocation between work packages for S-LAB efforts may be necessary and will be requested
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ Bi-weekly Task Force conferences ➤ 19 December, 2012 – WP5 teleconference ➤ 16 January, 2013 – WP5 teleconference ➤ 6 February, 2013 – WP5 teleconference ➤ 14 February, 2013 – WP6 teleconference
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none"> ➤ Delays in T6.1 caused spending less efforts then planned
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none"> ➤

4.7 Greece

4.7.1 ATHENA Research and Innovation Centre ATHENA

Beneficiary:	ATHENA RC / Industrial Systems Institute
Work Package(s)	WP2 – SPD metrics, requirements and system design
Task(s)	Task 2.2 Multi-technology SPD metrics Task 2.3 Multi-technology architectural design
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 2.2 Multi-technology SPD metrics : Task 2.3 Multi-technology architectural design
Effort actual or spent in this period:	Task 2.2 Multi-technology SPD metrics : Task 2.3 Multi-technology architectural design
% of work completed at the end of the period (indicative):	Task 2.2 Multi-technology SPD metrics : - Task 2.3 Multi-technology architectural design: -
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
The effort put, with respect to WP2 / T2.2 activities, ATHENA / Industrial Systems Institute is as follows:	
Description of criticalities met during the period:	
➤ None	
Corrective actions:	
➤ Not applicable	
Meetings performed during the period:	
➤ None	
Deviations between actual and planned person-months:	
➤ None	
Dissemination Activities and exploitation perspectives:	
➤ None	

PP

Beneficiary:	ATHENA RC / Industrial Systems Institute
Work Package(s)	WP3 - SPD Node
Task(s)	Task 3.4 : Dependable self-x Technologies Task 3.5 : Cryptographic technologies
Period:	1 st Sept 2012 – 28 st February 2013
Effort planned in this period:	Task 3.4 : Dependable self-x Technologies : Task 3.5 : Cryptographic technologies :
Effort actual or spent in this period:	Task 3.4 : Dependable self-x Technologies : 1 MMs Task 3.5 : Cryptographic technologies : 2:MMs
% of work completed at the end of the period (indicative):	Task 3.4 : Dependable self-x Technologies : 50% Task 3.5 : Cryptographic technologies : 70%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <p>With respect to WP3 activities, ATHENA / Industrial Systems Institute is intended to put effort on certain items as they are presented below per task:</p> <ul style="list-style-type: none"> ➤ 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) <p>The effort put per task during M13-18 is as follows:</p> <ul style="list-style-type: none"> ➤ 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. <p>Relative contribution was provided to deliverables D3.2 and 3.3</p>	
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ None 	
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ Not applicable 	
<p>Meetings performed during the period:</p> <ul style="list-style-type: none"> ➤ Project meeting in Budapest, Sep 2012 & 1st year review preparation in Rome, Oct 2012. Skype conference meetings with Work Package leaders in December 2012 and January 2013. 	
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none"> ➤ None 	
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none"> ➤ None 	

PP

Beneficiary:	ATHENA RC / Industrial Systems Institute
Work Package(s)	WP4 - SPD Network
Task(s)	Task 4.2 Distributed self-x models
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 4.2 Distributed self-x models: planned person months :
Effort actual or spent in this period:	Task 4.2 Distributed self-x models: 2,5
% of work completed at the end of the period (indicative):	Task 4.2 Distributed self-x models: achieved percentage : 35%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 4.2 <ul style="list-style-type: none"> ➤ 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. <p>The developed algorithms are being simulated in the OMNET++ environment in order for them to be adapted to the prototype under development.</p> 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ None 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Not applicable 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Project meeting in Budapest, Sep 2012. 1st year review preparation in Rome, Oct 2012. Skype conferences meetings with Work Package leaders in December 2012 and January 2013. 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ None 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

PP

D1.7

PP

Beneficiary:	ATHENA RC / Industrial Systems Institute
Work Package(s)	WP5 SPD Middleware & Overlay
Task(s)	Task 5.4: Adaptation of legacy systems Task 5.5 : Overlay monitoring and reacting system by security agents
Period:	1 st Sept 2012 – 29 st February 2013
Effort planned in this period:	Task 5.4: Adaptation of legacy systems Task 5.5 : Overlay monitoring and reacting system by security agents
Effort actual or spent in this period:	Task 5.4: Adaptation of legacy systems : 2 Task 5.5 : Overlay monitoring and reacting system by security agents:
% of work completed at the end of the period (indicative):	Task 5.4: Adaptation of legacy systems : 20% Task 5.5 : Overlay monitoring and reacting system by security agents:
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 5.4 <ul style="list-style-type: none"> ➤ Development of software adapters based on SLP protocol implementations, for discovering and registering legacy services. SW adapter was modelled and tested. 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ None 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Not applicable 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Project meeting in Budapest, Sep 2012. 1st year review preparation in Rome, Oct 2012. Skype conference meetings with Work Package leaders in December 2012, January 2013 and February 2013. 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ None 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

4.7.2 Hellenic Aerospace Industry

Beneficiary:	HAI
Work Package(s)	WP1 - Project Management
Task(s)	Task 1.1 – Project Management Task 1.2 – Liaisons
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 1.1 – Project Management, 2PM Task 1.2 – Liaisons, 0,5
Effort actual or spent in this period:	Task 1.1 – Project Management, 1PM Task 1.2 – Liaisons, 0PM
% of work completed at the end of the period (indicative):	Task 1.1 – Project Management, 2,5 PM (21% of total) Task 1.2 – Liaisons, 1 PM (33% of total)
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 1.1 <ul style="list-style-type: none"> ➤ HAI dedicated the aforementioned effort in project administration activities, participation in meetings and coordination of work and conferences 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ None 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Non applicable 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Organization of a teleconference, as a WP6 kick-off (14/02/2013) ➤ Participation in tactical (twice a month) meetings of the nSHIELD Task Force (phone calls) 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ None 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

Beneficiary:	HAI
Work Package(s)	WP2 - SPD Metrics, 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:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 2.1 - Multi-technology requirements & specification, 0 PM Task 2.2 - Multi-technology SPD metrics, 0 PM Task 2.3 - Multi-Technology Architectural Design, 0 PM
Effort actual or spent in this period:	Task 2.1 - Multi-technology requirements & specification, 1 PM Task 2.2 - Multi-technology SPD metrics, 1 PM Task 2.3 - Multi-Technology Architectural Design, 1 PM
% of work completed at the end of the period (indicative):	Task 2.1 - Multi-technology requirements & specification, 4 PM (80% of total) Task 2.2 - Multi-technology SPD metrics, 2 PM (40% of total) Task 2.3 - Multi-Technology Architectural Design, 9 PM (75% of total)
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • Task 2.1 <ul style="list-style-type: none"> ➤ HAI contributed in the efforts of consortium to update the content of requirements. More specifically HAI contributed in the discussion about: <ul style="list-style-type: none"> ○ Categorization of Requirements ○ Further classification of Requirements based on the 4 functional nSHIELD layers ○ Focus on Architecture related Requirements ○ Registration of Requirements in specific categories • Task 2.2 <ul style="list-style-type: none"> ➤ HAI contributed in this first stage of the definition of SPD Metrics for the overall nSHIELD system, in the following: <ul style="list-style-type: none"> ○ Assessment of candidate SPD Metrics ○ Review of first versions of D2.5 • Task 2.3 <ul style="list-style-type: none"> ➤ HAI coordinated efforts to finalize a formalized reference system Architecture, reflected in the work of D2.3 (internal) and D2.4 (public), both finalized in the reference period. The work included: <ul style="list-style-type: none"> ○ Definition of the methodology and design process ○ Proposal of an overall Architecture scheme 	

<ul style="list-style-type: none"> ○ 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
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none"> ➤ The finalization of nSHIELD reference Architecture was an achievement with implications and interactions throughout the project
<p>Corrective actions:</p> <ul style="list-style-type: none"> ➤ The Architecture will be finalized (M26), through a continuous cooperation between WP2 and the technical WPs (3-5), as well as the WPs involved in demonstration, system proof and incorporation of applications (WP6-7)
<p>Meetings performed during the period:</p> <p>None</p>
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none"> ➤ A small effort was spent during this period, although not planned, in order to finalize deliverables, in view of the first annual review meeting
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none"> ➤ None

PP

Beneficiary:	HAI
Work Package(s)	WP4 - SPD Network
Task(s)	Task 4.3 - Reputation-based resource management technologies
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 4.3 - Reputation-based resource management technologies, 3,5 PM
Effort actual or spent in this period:	Task 4.3 - Reputation-based resource management technologies, 3 PM
% of work completed at the end of the period (indicative):	Task 4.3 - Reputation-based resource management technologies, 4 PM (33% of total)
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 4.3 <ul style="list-style-type: none"> ➤ HAI has been working on Reputation-based resource management technologies and more specifically on trusted aware routing in Crossbow IRIS and Telosb sensor nodes 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ Algorithms for reputation based trusted routing are under development 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Not necessary 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ HAI had a teleconference (Skype) with the coordinator of the Task 4.2 (UNIGE) on 30/01/2013 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ No serious deviations between planned and actually spent effort 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

Beneficiary:	HAI
Work Package(s)	WP5 - SPD Middleware and Overlay
Task(s)	Task 5.1 – SPD driven Semantics Task 5.3 – Policy-based management Task 5.5 – Overlay monitoring and reacting system by security agents
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 5.1 – SPD driven Semantics, 1,5PM Task 5.3 – Policy-based management, 4 PM Task 5.5 – Overlay monitoring and reacting system by security agents, 1,5 PM
Effort actual or spent in this period:	Task 5.1 – SPD driven Semantics, 1PM Task 5.3 – Policy-based management, 4 PM Task 5.5 – Overlay monitoring and reacting system by security agents, 1 PM
% of work completed at the end of the period (indicative):	Task 5.1 – SPD driven Semantics, 1 PM (17% of total) Task 5.3 - Policy-based management, 4,5 PM (30% of total) Task 5.5 – Overlay monitoring and reacting system by security agents, 1PM (17% of total)
Description of the activities carried out during the period to reach specific objectives within the task/WP	
<ul style="list-style-type: none"> • Task 5.1 <ul style="list-style-type: none"> ➢ HAI conducted an assessment on UML diagrams, candidates for the nSHIELD semantic model • Task 5.3 <ul style="list-style-type: none"> ➢ 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 • Task 5.5 <ul style="list-style-type: none"> ➢ HAI has started working on the multi-layered Overlay Security Agent, in the direction of the design of abstracted and open user services 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➢ 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. 	
Corrective actions:	

PP

Meetings performed during the period:

- None

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

PP

Beneficiary:	HAI
Work Package(s)	WP6 - Platform integration, validation & demonstration
Task(s)	Task 6.3 – Lifecycle SPD Support
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 6.3 – Lifecycle SPD Support, 3 PM
Effort actual or spent in this period:	Task 6.3 – Lifecycle SPD Support, 1 PM
% of work completed at the end of the period (indicative):	Task 6.3 – Lifecycle SPD Support, 1 PM (17% of total)
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 6.3 <ul style="list-style-type: none"> ➤ HAI dedicated the aforementioned effort in forming SPD lifecycle procedures for nSHIELD, based mainly on the international standard ISO/IEC 12207 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ None 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Not applicable 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ Organization of a teleconference, as a WP6 kick-off (14/02/2013) 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ HAI used less than the planned effort, due to the preliminary nature of this introductory stage of WP6. HAI plans to use the remaining effort in the following (and more critical) steps of WP6. 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

PP

Beneficiary:	HAI
Work Package(s)	WP8 - Knowledge exchange and industrial validation
Task(s)	Task 8.1 – Dissemination Task 8.3 – Exploitation
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 8.1 – Dissemination, 0-0,5 PM Task 8.3 – Exploitation, 0-0,5 PM
Effort actual or spent in this period:	Task 8.1 – Dissemination, 1 PM Task 8.3 – Exploitation, 1 PM
% of work completed at the end of the period (indicative):	Task 8.1 – Dissemination, 1 PM (50% of total) Task 8.3 – Exploitation, 1 PM (25% of total)
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 8.1, 8.3 <ul style="list-style-type: none"> ➤ HAI dedicated the aforementioned effort in dissemination activities as well as in forming and describing the verification and testing plan for the first version of nSHIELD operational manual 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ None 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ Not applicable 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ None 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ None 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

4.7.3 Integrated Systems Development ISD

Beneficiary:	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:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 1.1 Project management - 0.5 PM Task 3.3 Power node - 12 PM Task 6.1 Multi-Technology System Integration – 0 PM Task 7.1 Railways security – 0 PM Task 7.2 Voice / facial recognition – 0 PM Task 7.4 Social mobility – 0 PM
Effort actual or spent in this period:	Task 1.1 Project management - 0.5 PM Task 3.3 Power node - 11.5 PM Task 6.1 Multi-Technology System Integration – 0 PM Task 7.1 Railways security – 0 PM Task 7.2 Voice / facial recognition – 0 PM Task 7.4 Social mobility – 0 PM
% of work completed at the end of the period (indicative):	Task 1.1 Project management - 25% Task 3.3 Power node - 28% Task 6.1 Multi-Technology System Integration – 0% Task 7.1 Railways security – 0% Task 7.2 Voice / facial recognition – 0% Task 7.4 Social mobility – 0%

<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none">➤ 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. More information can be found in the relevant section of D3.2.
<p>Description of criticalities met during the period:</p> <ul style="list-style-type: none">➤ None
<p>Corrective actions:</p> <ul style="list-style-type: none">➤ Not applicable
<p>Meetings performed during the period:</p> <ul style="list-style-type: none">➤ 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.
<p>Deviations between actual and planned person-months:</p> <ul style="list-style-type: none">➤ None
<p>Dissemination activities and exploitation perspectives:</p> <ul style="list-style-type: none">➤ None

4.7.4 Technical University of Crete TUC

Beneficiary:	TUC
Work Package(s)	WP2 – SPD Metric, requirements and system design
Task(s)	Task 2.2 Multi-technology SPD metrics
Period:	1 st September 2012 – 28 th February 2013
Effort planned in this period:	Task 2.2 Multi-technology SPD metrics, 0 PM
Effort actual or spent in this period:	Task 2.2 Multi-technology SPD metrics, 1.3 PM
% of work completed at the end of the period (indicative):	Task 2.2 Multi-technology SPD metrics, 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 2.2 <ul style="list-style-type: none"> ➤ Proposal of a novel dynamic and applicable formal methodology for evaluating the SPD composed metric. The new approach supports a dynamic choreographed modelling scheme. The scheme permits the modelling of legitimate/malicious behaviour, dynamic composition and setting of environment parameters and attack scenarios. To retain consistency with this new model, the original SPD metrics of D2.5 were re-classified in three categories (SPD metrics, security attributes and security properties). 	
Description of criticalities met during the period:	
<ul style="list-style-type: none"> ➤ All required contributions were sent in time and no deviations of the schedule defined by the respective WP/task leader have been observed. 	
Corrective actions:	
<ul style="list-style-type: none"> ➤ None 	
Meetings performed during the period:	
<ul style="list-style-type: none"> ➤ None 	
Deviations between actual and planned person-months:	
<ul style="list-style-type: none"> ➤ No deviations. 	
Dissemination activities and exploitation perspectives:	
<ul style="list-style-type: none"> ➤ None 	

Beneficiary:	TUC
Work Package(s)	WP3 - SPD Node
Task(s)	Task 3.1 Nano node Task 3.2 Micro/Personal node Task 3.3 (TUC not involved) Task 3.4 Dependable self-x Technologies Task 3.5 Cryptographic technologies
Period:	1 st September 2012 – 28 th February 2013
Effort planned in this period:	Task 3.1 Nano node, 1.8 PM Task 3.2 Micro/Personal node, 1.8 PM Task 3.4 Dependable self-x Technologies, 1.8 PM Task 3.5 Cryptographic technologies, 4.2 PM
Effort actual or spent in this period:	Task 3.1 Nano node, 1.8 PM Task 3.2 Micro/Personal node, 1.8 PM Task 3.4 Dependable self-x Technologies, 1.8 PM Task 3.5 Cryptographic technologies, 4.2 PM
% of work completed at the end of the period (indicative):	Task 3.1 Nano node, 100% Task 3.2 Micro/Personal node, 100% Task 3.4 Dependable self-x Technologies, 100% Task 3.5 Cryptographic technologies, 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> ➤ Task 3.1 <p>We conducted a survey for smartcard-based authentication protocols. Based on the knowledge acquired by this survey, we have designed an authentication protocol that uses symmetric keys stored in the smart cards. The proposed scheme is based on a symmetric “masterkey”, which can be stored on any kind of TPM, and is used to generate all the required sub-keys. In this way, we can enhance the trust among different nodes. We are considering integrating this scheme to the TUN interface described in WP5.</p> <ul style="list-style-type: none"> ➤ Task 3.2 <p>Well-known crypto libraries, like OpenSSL, target mainstream applications. Other libraries that are designed for embedded system applications contain redundant functionality, as they support a wide range of cryptographic primitives. For nSHIELD cryptographic technologies, we implement a compact crypto library for a subset of lightweight ciphers and compact implementations of standard ciphers. The library utilizes open-source implementations of known ciphers. We implement a common API for utilizing all of them with different parameters. In this first prototype, the library contains block and stream ciphers. For block ciphers, it supports AES, DES, PRESENT, LED and KATAN in ECB (Electronic CodeBook) mode of operation with zero padding. For stream ciphers, it supports the eSTREAM project finalists Salsa, Rabbit, HC, SOSEMANUK, Grain, Trivium and Mickey v2. The crypto library is implemented in C language. We will implement and test the library on BeagleBone and BeagleBoard devices.</p>	

➤ Task 3.4

An anonymizer component will be developed for nSHIELD applications where personal location privacy is to be preserved, while enabling the system to provide location monitoring services. After an extensive review of the state of the art, the TinyCasper scheme was chosen and will be implemented, aiming to preserve personal location privacy via the well-established k-anonymity privacy concept, while enabling the system to provide location monitoring services. The implemented scheme will offer two options: a resource-aware algorithm for applications, where it is essential to minimize communication and computational cost and a quality-aware algorithm, which minimizes the size of cloaked areas, in order to generate more accurate aggregate locations. Provisions will be made and original work will be extended in order to better match nSHIELD's architecture and hardware and to facilitate scenarios where the nodes are mobile. On the server side, a simple graphical interface will be used in order to setup the various parameters and monitor the system.

Contribution to D3.1 (SPD node technologies assessment) in Section 6 (Dependable self-x Technologies). Access control mechanisms are in charge of preventing non authorized/malicious entities to access the physical resources of embedded devices that can be reached over the network. Automatic access control is a technique where network entities use a lightweight mechanism to authenticate each other. For nSHIELD, we are developing an automatic access control protocol based on the Gossamer protocol. Gossamer is an ultra-lightweight protocol that provides mutual authentication and prevents DoS attacks on RFID systems. We are implementing the protocol in BeagleBones/BeagleBoards. A BeagleBoard will act as a server and a small number of BeagleBones will connect to the board and act as tags. The protocol will be used for node and network protection against DoS attacks.

➤ Task 3.5

Investigated secure protocols and methods for establishing cryptographic keys among communicating parties. Emphasis has been given on Identity Based Cryptography and its use in key agreement methods to benefit from the advantages this method offers. The aim is to provide an efficient scheme to establish keys that will be used to secure communications among resource-restricted nodes, in place of the expensive IKE protocol used in IPsec. This work is carried out in parallel with WP4, where the use of a light IPsec protocol for secure communications at network layer is being examined. The platforms to demonstrate the proposed schemes have been chosen together with the corresponding crypto libraries that will form the basis for this key agreement scheme, while development is underway.

Development of a lightweight, efficient, GPU accelerated hashing and hash lookup mechanism utilizing the CUDA GPGPU toolkit. The scheme will maintain a hash-table with the hash values of known files. Upon execution, it will compute the digest of input files using the same hash function and, depending on application, look for a match or a mismatch between pre-existing and calculated values. Possible applications of the mechanism include (but are not limited to) malware detection on local disks or network traffic and file integrity checks for pre- or post-installation audits. Work will include optimizations both in the hash calculation and lookup mechanisms, taking into consideration the highly parallel architecture of current GPUs. This scheme and its variations will further enhance the functionality and performance of the nSHIELD's power nodes, taking advantage of state-of-the art GPU-accelerated ARM-based systems (e.g. NVIDIA Carma platform).

Description of criticalities met during the period:

- All required contributions were sent in time and no deviations of the schedule defined by the respective WP/task leader have been observed.

Corrective actions:

- None

Meetings performed during the period:

- 2012-09-25: Skype conference among TUC members

PP

- 2013-01-17: Skype conference among TUC members

Deviations between actual and planned person-months:

- No deviations.

Dissemination activities and exploitation perspectives:

- Some more effort will be put in the results of the four surveyed SPDs, as well as of the relevant EU projects, in order to be sent for publication in related journals/conferences.

Beneficiary:	TUC
Work Package(s)	WP4 - SPD Network
Task(s)	Task 4.3 Reputation-based resource management technologies Task 4.4 Trusted and dependable connectivity
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 4.3 Reputation-based resource management technologies: 1.8 PMs Task 4.4 Trusted and dependable connectivity: 3.2 PMs
Effort actual or spent in this period:	Task 4.3 Reputation-based resource management technologies: 1.8 PMs Task 4.4 Trusted and dependable connectivity: 3.2 PMs
% of work completed at the end of the period (indicative):	Task 4.3 Reputation-based resource management technologies: 100% Task 4.4 Trusted and dependable connectivity: 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP:	
<ul style="list-style-type: none"> • Task 4.3 <ul style="list-style-type: none"> ➤ Contribution to D4.3 (Preliminary SPD network technologies prototype report) in Section () and D4.4 (SPD network technologies prototype) in section (). Design and implementation (in progress) of a prototype of a novel reputation and trust-based system for secure routing and intrusion detection. The concept was simulated in ns2 (network simulator 2) in C++. The system extends the Dynamic Source Routing (DSR) protocol by integrating reputation and trust information to the decision making process of DSR. The goal is to select short paths with well-reputed nodes and avoid the malicious ones. Our reputation-based scheme can act as a general-purpose scheme for a wide range of applications. We identify the basic components that are common in many relevant schemes and provide an abstract reputation-based framework. For each component we invoke a set of implementations, based on well-examined schemes. The network designer selects which components are active and the exact set of implementations. The design options range from ultra-lightweight protocols to heavily secure ones. In this demo, we only support the manipulation of direct knowledge. For calculating the reputation estimate, we implement simple summation and a reputation fading mechanism. For the grading of a transaction we support simple (+1/-1) and gradual (+1/-2) ranking. The designer can set the scope of reputation ranking (node, path or community of nodes). We support punishment policies for the malicious nodes based on routing and forwarding criteria. Also, we support automatic re-entrance policies for the punished nodes. Currently, we model the black-hole attack as an example of malicious behaviour scenario. A legitimate node can detect a malicious one and take countermeasures. • Task 4.4 <ul style="list-style-type: none"> ➤ After investigating the alternatives regarding the protection of messages during transmission while considering nodes' capabilities in terms of deploying expensive cryptographic computations, a network layer security approach was chosen and an IPsec based protocol was proposed for resource-constrained devices. Given the lack of a standardised IPsec scheme for such devices there is on-going research on this topic and published schemes are being examined. A prototype is being developed to investigate the pros and cons of our 	

proposed scheme compared to others. We collaborated with our partners to find a common agreement on the scheme that will be developed to ensure the required interoperability for the exchanged messages among different platforms.

Description of criticalities met during the period:

- Explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning
- 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
- Example: Some inputs are missing from the finalization of T x.y. This has introduced a delay in the formalization of some key concepts in task z.w...

Corrective actions:

- Example: A project extension could be enough to finalize the work, because...

Meetings performed during the period:

- 2012-11-21: WP4 PhC

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- None

PP

Beneficiary:	TUC
Work Package(s)	WP5 - SPD Middleware & Overlay
Task(s)	Task 5.2 Core SPD services & Adaptation of Legacy Systems Task 5.3 Policy-based management
Period:	1 st Sept 2012 – 28 th February 2013
Effort planned in this period:	Task 5.2 Core SPD services & Adaptation of Legacy Systems: 3.0 PMs Task 5.3 Policy-based management: 2.4 PMs
Effort actual or spent in this period:	Task 5.2 Core SPD services & Adaptation of Legacy Systems: 3.0 PMs Task 5.3 Policy-based management: 2.4 PMs
% of work completed at the end of the period (indicative):	Task 5.2 Core SPD services & Adaptation of Legacy Systems: 100% Task 5.3 Policy-based management: 100%
<p>Description of the activities carried out during the period to reach specific objectives within the task/WP:</p> <ul style="list-style-type: none"> • Task 5.2 <ul style="list-style-type: none"> ➤ 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. Identified appropriate technologies and successfully setup existing nSHIELD OSGi framework (Knopflerfish) where identified technologies will be integrated. ➤ Collaborated with partners to identify and address interoperability issues between interfaces and between said interfaces and the nSHIELD platform. Also collaborated with partners to identify 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”. 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. • Task 5.3 <ul style="list-style-type: none"> ➤ 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. ➤ 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. ➤ Work on finalizing the aim and outline of the demonstration scenario for the proposed framework. 	

PP

D1.7

Description of criticalities met during the period: <ul style="list-style-type: none">➤ Explain the reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning➤ 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➤ Example: Some inputs are missing from the finalization of T x.y. This has introduced a delay in the formalization of some key concepts in task z.w...
Corrective actions: <ul style="list-style-type: none">➤
Meetings performed during the period: <ul style="list-style-type: none">➤ 2012-12-19: WP5 PhC (Skype)➤ 2013-01-16: WP5 PhC (Skype)➤ 2013-02-06: WP5 PhC - D5.2 - D5.3 (Skype)
Deviations between actual and planned person-months: <ul style="list-style-type: none">➤ None
Dissemination activities and exploitation perspectives: <ul style="list-style-type: none">➤ None

PP

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	PP	3	Yes	June 2013	The deliverable has been rejected by the reviewer. It seemed already re-submitted in November, but it needs additional improvements.
D8.4	Build Secure Embedded Systems with nSHIELD v1	8	MGEP	R	PU	12	No	June 2013	
D1.6	Quality Control Report 1	1	SES	R	PU	15	No	June 2013	
D1.7	Periodic Management Report	1	SES	R	PP	18	No	May 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	

PP

D1.7

PP

D4.2	Preliminary SPD network technologies prototype	4	SES	P,O	RE	18	No	May 2013	
D4.3	Preliminary SPD network technologies prototype report	4	SES	R	PU	18	Yes	May 2013	
D5.2	Preliminary SPD middleware and overlay technologies prototype	5	UNIROMA1	P,O	RE	18	No	May 2013	
D5.3	Preliminary SPD middleware and overlay technologies prototype report	5	SES	R	PU	18	No	May 2013	
D6.1	Lifecycle and SPD Support Plan	6	TECNALIA	R	CO	18	No	May 2013	

Table 8: Deliverables

PP

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		M18	No	May 2013	Reasons for the delay are in Para. 6.2

Table 9: Milestones

PP

D1.7

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 really first short transition period.

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

The document has been well defined in terms of requirements; however it needed some details concerning the architecture and their elements, including (i) ontologies on security, (ii) ontology for system description, (iii) metrics, (iv) reasoning and (v) execution. Additionally the formal description of security and the system of systems could be included in the D8.4. This wasn't taken into consideration in the TA and could be considered the principal cause of the delay.

Action on D5.3 (Preliminary SPD middleware and overlay technologies prototype)

The D5.3 will document the integration of innovative codes into the platform developed for the pilot project, pSHIELD: several partners were no part of the pSHIELD consortium and they needed to be guided into the development of additional modules. This development has been already started. Additionally, the definition of the Policy has also started a little late because of the need to mature application scenarios where policies are strictly dependent.

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.

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

Selex ES will cover the effort and the activities of Selex SG and Selex ES from January 2013 to the end of the project.

From the activities point of view, the third half has been split in two separated part. From the 1st of September to the 31st of December the beneficiary report and the related activities have been reported by Selex SG and Selex ES separately. Form the 1st of January to the 28th of February the beneficiary report and the related activities are associated to Selex ES.

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 ESIS

ESIS announced in Q1.2012 to leave the project and left the consortium in June 2012. Formal communication was given on July 2012 via email. ESIS has been deleted from the project beneficiary report session of this document.

6.3.4 NOOM

NOOM announced in Q1.2012 to leave the project and left the consortium in June 2012. Formal communication was given on July 2012 via email. NOOM has been deleted from the project beneficiary report session of this document.

6.4 Project meetings

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 held and a set of amendments was collected
- Many meetings related to Work Package activities were held via Phone Conferences
- Meeting between JU and the Selex ES new contact point was held in Brussels (20/02/2013)

Minutes of Meetings as well as corresponding documents are stored at the project official repository and Collaborative Tool (<http://nshield.unik.no>).

Information is also available at the nSHIELD website.

	Date	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

	Date	Phone
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 3: Project meetings

6.5 Project planning and status

Some deliverable has been delivered with delay. However this delay is not impacting the project. All the partners agreed and no objections were raised.

Some of the reasons of this delay are explained at Para 6.2. Additional reasons for this delay are:

- the D4.2, D4.3, D5.2 and 5.3 required more participation from partners. The GANTT in the TA, for this reason, shows dates not realistic.
- One of the most involved partners has not contributed in the project as expected and required by the TA.

Activities from M18 are not affected from any additional delay. The plan described in the Technical Annex can be considered valid and do not need to change at the moment (M18).

6.6 Impact of deviations

After one year and half the project is running on track, with no major deviations and no negative impacts on the project. All the delays are 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.

6.8 Project website

- nSHIELD project website is 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 available at address: <http://nshield.unik.no>
The access to repository is limited only to authorized persons. 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 D8.2.

6.10 Co-ordination activities

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

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 SECURED.

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.

PP

Contract N. 269317 Acronym: nSHIELD Period: 01.09.2011 - 28.02.2013		MAS	ASTS	AT	A THENA	SE	TECNALIA	ALFA	ETH	HAI	ISL	ISD	SG	MGEF	S-LAB	SESM	SICS	TZD	TELC	THYA	TUC	UNIGE	UNIUD	UNIROMA1	SES
Workpackage 1:	Actual WP total:	0	2	4,4	0	11	3	0	0,5	3,5	4,2	0,5	17,1	1,5	0	0	0	0	0	1,5	0	0	1,5	2,17	3,5
Project Management	Planned WP total:	0,00	3,00	9,00	3,00	11,00	5,00	0,00	1,00	15,00	10,00	2,00	17,30	3,00	0,00	0,00	0,00	0,00	0,00	13,00	4,00	0,00	3,00	3,00	34,70
	%	0	67%	49%	0	100%	60%	0	50%	23%	42%	25%	99%	50%	0	0	0	0	0	12%	0	0	50%	72%	10%
Workpackage 2:	Actual WP total:	0	10	5,9	2	11,9	22,34	0	1,5	15	0	0	6,46	0	8,93	0	5	7,6	0	11,5	8,5	0	3	0	2
SPD Metric, requirements and system design	Planned WP total:	0,00	11,00	8,00	6,00	11,90	12,00	0,00	2,00	22,00	0,00	0,00	6,46	0,00	10,00	0,00	6,00	10,00	0,00	20,00	10,00	0,00	3,00	0,00	4,64
	%	0	91%	74%	33%	100%	186%	0	75%	68%	0	0	100%	0	89%	0	83%	76%	0	58%	85%	0	100%	0	43%
Workpackage 3:	Actual WP total:	0	0	13,3	5	2,6	9	0	24	0	0	16,5	7,64	0	7,1	6	7	0	3,1	4	23,6	21,5	8	0	0,7
SPD Node	Planned WP total:	0,00	0,00	22,00	8,00	2,60	6,00	0,00	25,00	4,00	0,00	58,00	7,54	0,00	12,00	15,00	20,00	26,00	6,00	30,00	37,00	30,00	12,00	0,00	14,46
	%	0	0	60%	63%	100%	150%	0	96%	0	0	28%	101%	0	59%	40%	35%	0	52%	13%	64%	72%	67%	0	5%
Workpackage 4:	Actual WP total:	0	0	0	3,5	35	18	0	0	4	22,5	0	5,64	8,5	0	0	0	0	0	2	9,8	9,5	7	0	5,4
SPD Network	Planned WP total:	0,00	0,00	0,00	10,00	35,00	14,00	0,00	0,00	15,00	34,00	0,00	5,64	20,00	0,00	0,00	0,00	0,00	0,00	12,00	14,00	25,00	12,00	0,00	53,36
	%	0	0	0	35%	100%	129%	0	0	27%	66%	0	100%	43%	0	0	0	0	0	17%	70%	38%	58%	0	10%
Workpackage 5:	Actual WP total:	0	0	0	2	15,7	15,5	0	0	6,5	10,5	0	5,34	6,5	13,26	0	0	0	0	3	11,7	0	0	24,1	4,9
SPD Middleware & Overlay	Planned WP total:	0,00	0,00	0,00	14,00	15,70	20,00	0,00	0,00	27,00	18,00	0,00	5,34	8,00	28,00	0,00	0,00	0,00	0,00	19,00	18,00	0,00	0,00	41,00	31,96
	%	0	0	0	14%	100%	78%	0	0	24%	58%	0	100%	81%	47%	0	0	0	0	16%	65%	0	0	59%	15%
Workpackage 6:	Actual WP total:	0,00	0,00	0,00	0,00	0,10	7,00	0,00	0,00	1,00	5,50	0,00	1,30	0,00	0,90	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,20
Platform integration, validation & demonstration	Planned WP total:	7,00	8,00	19,00	21,00	0,10	15,00	4,00	3,00	32,00	24,00	6,00	1,30	3,00	29,00	0,00	0,00	0,00	0,00	12,00	0,00	0,00	6,00	4,00	34,60
	%	0	0	0	0	100%	47%	0	0	3%	23%	0	100%	0	3%	0	0	0	0	0	0	0	0	0	1%
Workpackage 7:	Actual WP total:	2	6,02	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0
SPD Applications	Planned WP total:	8,00	21,00	2,00	0,00	0,00	8,00	13,00	18,00	23,00	0,00	6,00	0,00	0,00	24,00	16,00	0,00	0,00	3,00	32,00	9,00	5,00	0,00	0,00	40,00
	%	25%	29%	0	0	0	0	0	0	0	0	0	0	0	0	13%	0	0	0	0	0	0	0	0	0
Workpackage 8:	Actual WP total:	1	3	1,4	0	0	2,51	1	0,7	2	3,4	0	3,93	3,4	0	0	0	0	0	0	1,1	0	0	0	0,4
Knowledge exchange and industrial validation	Planned WP total:	3,00	6,00	4,00	4,00	0,00	8,00	1,00	1,00	6,00	14,00	0,00	3,93	11,00	5,00	0,00	0,00	0,00	0,00	5,00	5,00	0,00	0,00	0,00	9,07
	%	33%	50%	35%	0	0	31%	100%	70%	33%	24%	0	100%	31%	0	0	0	0	0	0	22%	0	0	0	4%
Total Project PM	Actual total:	3,00	21,02	25,00	12,50	76,30	77,35	1,00	26,70	32,00	46,10	17,00	47,41	19,90	30,19	8,00	12,00	7,60	3,10	22,00	54,70	31,00	19,50	26,27	17,10
	Planned total:	18,00	49,00	64,00	66,00	76,30	88,00	18,00	50,00	144,00	100,00	72,00	47,51	45,00	108,00	31,00	26,00	36,00	9,00	143,00	97,00	60,00	36,00	48,00	222,79
	%	17%	43%	39%	19%	100%	88%	6%	53%	22%	46%	24%	100%	44%	28%	26%	46%	21%	34%	15%	56%	52%	54%	55%	8%

Table 10: Person-Month Status

Note: the contribution from partners from Norway was 11.5 PM, but reported too late, thus not included here

7.1 MAS

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY MOVATION FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs ⁵		45000		45000	
	Subcontracting					
	Travel		2000		2000	
	Remaining direct costs					
TOTAL DIRECT COSTS ²			47000		47000	
TOTAL INDIRECT COSTS ²						

Table 11: MAS Cost

Note: the reporting period in Norway is different from the nSHIELD report, numbers are indicative

⁵ **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 ANSALDO STS FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		32.297,3	9772,07	42069,37	
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS			32.297,3	9772,07	42069,37	
TOTAL INDIRECT COSTS			16.148,65	4886,04	21034,69	<i>Rate 50% of personnel costs</i>

Table 12: ASTS Cost

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

7.3 AT

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ACORDE TECHNOLOGIES FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3,8	Personnel costs	0	1.850,00 €	21.579,87 €	23.429,87 €	Salaries of project manager and project engineers
	Subcontracting	0	0	0	0	
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS		0	1.850,00 €	21.579,87 €	23.429,87 €	
TOTAL INDIRECT COSTS		0	370,00 €	4.315,97 €	4.685,97 €	

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 1/9/12 – 28/2/13						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP3, WP4, WP5	Personnel costs		20000		20000	
	Subcontracting					
WP3, WP4, WP5	Travelling Expenses		3218		3218	
WP3, wP4, WP5	Research Equipment		1333		1333	
	Remaining direct costs		625		625	
TOTAL DIRECT COSTS			25176		25176	
TOTAL INDIRECT COSTS			5035		5035	

Table 14: ATHENA Cost

7.5 SE

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR SE FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 2, 3, 4, 5	Personnel costs	145.285,00			145.285,00	<i>Salaries of 3 engineer and 2 lab technician for ~24,7 months total</i>
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS		145.285,00			145.285,00	
TOTAL INDIRECT COSTS		72.643,00			72.643,00	

Table 15: SE Cost

7.6 TECNALIA

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR TECNALIA Y FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2, WP3, WP4, WP5 WP6, WP8, WP1	Personnel costs		130.990,29		130.990,29	Salaries for 34,51 p/m
	Remaining direct costs					
TOTAL DIRECT COSTS			130.990,29		130.990,29	
TOTAL INDIRECT COSTS			26.198,06		26.198,06	

Table 16: TECNALIA Cost

7.7 ETH

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ETH FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3	Personnel costs	0 €	27200 €	0 €	27200 €	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 €	
TOTAL DIRECT COSTS		0 €	27200 €	0 €	27200 €	
TOTAL INDIRECT COSTS		0 €	13600 €	0 €	13600 €	Overhead for personnel costs (rate 50%)

Table 17: ETH Cost

7.8 HAI

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR HAI Y FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,4,5,6,8	Personnel costs		104.768,89 €			Salaries for 1 PM (WP1) Salaries for 3PMs (WP2) Salaries for 3 PMs (WP4) Salaries for 6 PMs (WP5) Salaries for 1 PM (WP6) Salaries for 2 PM (WP8)
	Subcontracting					
	Equipment		1951,00€			Doors licence
	Travel		961,70€			Participation in Plenary meeting (Budapest, 10 September 2012)
	Remaining direct costs					
TOTAL DIRECT COSTS			107.681,59 €			
TOTAL INDIRECT COSTS			5.500 €			

Table 18: HAI Cost

7.9 ISL

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR ISL Y FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,4,5,6,8	Personnel costs		143306€			Salaries for one Director, 2 experts and 2 senior engineers for five months each approximately
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS			171967€			
TOTAL INDIRECT COSTS			28661€			<i>overhead rate 20% of personnel costs</i>

Table 19: ISL Cost

7.10ISD

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ISD FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs					
	Subcontracting					
	Travel					
	Remaining direct costs					
TOTAL DIRECT COSTS						
TOTAL INDIRECT COSTS						

Table 20: 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.

7.11 SG

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR SG FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,3,4,5,6,8	Personnel costs	64.615,3			64.615,3	<i>Salaries of 1,5 engineer and 1,5 lab technician for ~11,5 months total</i>
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS		64.615,3			64.615,3	
TOTAL INDIRECT COSTS		32.307,7			32.307,7	

Table 21: SG Cost

7.12 MGEP

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR MGEP Y FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		€52250,22		€52250,22	Salaries of personnel
	Subcontracting					
	Zolertia Professional Pack Platinum		€1308,95		€1308,95	WSN development platform
	Audit		€900		€900	Audit costs
	Remaining direct costs					
TOTAL DIRECT COSTS			€54459,17		€54459,17	
TOTAL INDIRECT COSTS			€10450,04		€10450,04	Overhead rate 20% of personnel costs

Table 22: MGEP Cost

7.13 SLAB

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR SEARCH-LAB Y FOR THE PERIOD 1ST SEPT 2012 – 28ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2	Personnel costs		5 468 EUR		5 468 EUR	1.96MMs
WP3	Personnel costs		6 835 EUR		6 835 EUR	2.45MMs
WP5	Personnel costs		20 170 EUR		20 170 EUR	7.23MMs
WP6	Personnel costs		2 511 EUR		2 511 EUR	0.9MMs
All	Total Personnel costs		34 984 EUR		34 984 EUR	12.54MMs
	Subcontracting					
all	Travel costs		1 226 EUR		1 226 EUR	Project meetings
	Remaining direct costs					
TOTAL DIRECT COSTS			36 210 EUR		36 210 EUR	
TOTAL INDIRECT COSTS			3 621 EUR		3 621 EUR	

Table 23: SEARCH-LAB Cost

The fluctuation of the exchange rate between EUR and HUF could cause the final reported costs differ even more than 10%

7.14 SESM

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SESM FOR THE PERIOD 01/09/2012 – 28/02/2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs		16800		16800	3 PMs
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					Travel costs are not reimbursed according to national agreement.
TOTAL DIRECT COSTS			16800		16800	
TOTAL INDIRECT COSTS			8064		8064	Indirect costs calculated on 2011 balance sheet were 48%

Table 24: SESM Cost

7.15 SICS

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SICS FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2	Personnel costs	9000€			9000€	System requirements and architecture work.
WP3	Personnel costs	1000€			1000€	Swedish node work coordination.
WP3	Personnel costs			10760€	10760€	SICS hypervisor Global Platform design and Linux porting design work.
WP3	Subcontracting			15500	15500	SICS hypervisor Linux porting work.
TOTAL DIRECT COSTS		10000€		26260€	36260€	
TOTAL INDIRECT COSTS		5500€		5918€	11418€	55% overhead costs.

Table 25: SICS Cost

7.16T2D

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY T2D FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2	Personnel costs			7000€	7000€	System requirements and architecture work.
WP3	Personnel costs				1000€	Swedish node work coordination.
WP3	Personnel costs			9000€	9000€	Implementation of prototype firmware
TOTAL DIRECT COSTS					17000€	
TOTAL INDIRECT COSTS					3000€	overhead

Table 26: T2D Cost

7.17 TELC

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TELC FOR THE PERIOD 1ST SEPT 2012 – 28ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs					
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS			680			
TOTAL INDIRECT COSTS			374			Overhead 55% of personnel cost. Includes travel.

Table 27: TELC Cost

7.18 THYIA

No activities have been reported from THYIA.

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY THYIA FOR THE PERIOD 1 ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs ⁶					
	Subcontracting					
	Travel					
	Remaining direct costs					
TOTAL DIRECT COSTS						
TOTAL INDIRECT COSTS						

Table 28: THYIA Cost

7.19TUC

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TUC FOR THE PERIOD 1ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2, WP3 WP4 WP5	Personnel costs	84.664,00			84.664,00	Salaries of full-time and part-time personnel, plus 8 PhD students at Technical University of Crete.
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS						
TOTAL INDIRECT COSTS						

Table 29: TUC Cost

PLEASE NOTE: NO ACTUAL PAYMENTS TO PERSONNEL HAVE BEEN MADE SO FAR BECAUSE TUC HAS NOT YET SIGNED CONTRACTS WITH THE RELEVANT GREEK AUTHORITIES.

7.20 UNIGE

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIGE FOR THE PERIOD 1ST SEPT 2012 – 28ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3	Personnel costs	48.000 €	0 €	0 €	48.000 €	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:
4		48.652,20 €	0 €	0 €	48.652,20 €	4 PM Junior Researcher 6 PM Full Professor 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: 7 PM Full Professor 5 PM Assistant Professor
TOTAL DIRECT COSTS		96.652,20 €	0 €	0 €	96.652,20 €	
TOTAL INDIRECT COSTS		37.694,36 €	0 €	0 €	37.694,36 €	overhead rate 39% of personnel costs

Table 30: UNIGE Cost

7.21 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	54.686,35 €	0	0	54,686,35 €	Salaries for 1 Full Professor (0.5 PM)
3						Salaries for 2 Full Professors (1 PM each) + 1 Associate Professor (1 PM) and 1 Assistant Professor (1 PM)
3						Salaries for 1 Full Professors (1 PM each) + 1 Associate Professor (2 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		54.686,35 €	0	0	54.686,35 €	
TOTAL INDIRECT COSTS		10.937,27 €	0	0	10.937,27 €	Overhead: 20% of personnel cost

Table 31: UNIUD Cost

7.22 UNIROMA1

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIROMA1 FOR THE PERIOD 1ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 5	Personnel costs		71600 €		71600 €	n. 11 PM (5 professors & 6 researchers)
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS			71600 €		71600 €	
TOTAL INDIRECT COSTS			35800 €		35800 €	

Table 32: UNIROMA1 Cost

7.23 SES

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SES FOR THE PERIOD 1ST SEPT 2012 – 28ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3, 4,5,6,8	Personnel costs	107.476,40			107.476,40	<i>Salaries of 4 engineer and 4 lab technician for ~17 months total</i>
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS		107.476,40			107.476,40	
TOTAL INDIRECT COSTS		53.738,20			53.738,20	

Table 33: SES Cost

7.24 Alfatroll

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ALFATROLL FOR THE PERIOD 1ST SEPT 2012 – 28 ST FEBRUARY 2013						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
	Personnel costs		15000		15000	
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y'					
	Remaining direct costs					
TOTAL DIRECT COSTS ⁷			15000 €		15000	
TOTAL INDIRECT COSTS						

Table 34: Alfatroll Cost

Note: the reporting period in Norway is different from the nSHIELD report, numbers are indicative

⁷ All costs reported are indicative, and subject to acceptance of the Research Council of Norway.

8 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.

9 Certificates

For this intermediate report no certificate is required, in accordance with Article IV.4.3 of the Grant Agreement.