PROJECT PERIODIC REPORT

JU Grant Agreement number: ***100204***

Project acronym: ***PSHIELD***

Project title: ***pilot 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 01.01.2011 to 30.06.2011

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

Dr. Josef Noll (SESM)

Tel: +47 9083 8066

E-mail: josef.noll@movation.no

Project website[2] address: http://www.pshield.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: http://www.artemis-ju.eu. The area of activity of the project should also be mentioned.

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

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

- The attached periodic report represents an accurate description of the work carried out in this project for this reporting period;

- The project (tick as appropriate):

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

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

  □ has failed to achieve critical objectives and/or is not at all on schedule[4].

- The public website is up to date, if applicable.

- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status. Any changes have been reported under section 5 (Project Management) in accordance with Article III.2.f and IV.1.f of the JU Grant Agreement.

Name of administrative representative of the Coordinator[1]: Dr. Josef Noll

Date: 16/09/2011

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

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

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

Project no: 100204

p-SHIELD

pilot embedded Systems architecture for multi-Layer Dependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems (including RAILWAYS)

D1.1.3: Management Report Report

Due date of deliverable: 31st August 2011
Actual submission date: 16th September 2011

Start date of project: 1st June 2010 Duration: 12 months

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		
Francesca Matarese	SESM	16/09/2011	
All partners contribute			
Reviewed by			
Name	Company		
Approved by			
Name	Company		
Josef Noll	MOVATION	16/09/2011	

Modification History		
Issue	Date (DD/MM//YY)	Description

Contents

1 PUBLISHABLE SUMMARY 11

1.1 Summary 11

1.2 Main results achieved 13

CLEARLY SIGNIFICANT AND TANGIBLE RESULTS ARE: 13

CLEARLY SIGNIFICANT AND TANGIBLE RESULTS ARE: 14

CLEARLY SIGNIFICANT AND TANGIBLE RESULTS ARE: 15

1.2.1. Measures on how pSHIELD has reached the scope 18

1.2.2. Overall project impact 20

1.3 Dissemination 20

1.3.1 Internal dissemination to project partners 21

1.3.2 Targeted industrial dissemination 21

1.3.3 Scientific dissemination 23

1.3.4 Contribution to workshops and exhibitions 24

2 PROJECT OBJECTIVES FOR THE PERIOD 25

3 WORK PROGRESS AND ACHIEVEMENTS DURING THE PERIOD 27

3.1 WP2 SPD Metrics Requirements and System Design 28

3.1.1 Progress towards objectives 28

3.1.2 Significant and tangible results 28

3.2 WP 3 SPD Node 30

3.3.1 Progress towards objectives 30

3.3.2 Significant and tangible results 30

Status of the deliverables: 31

3.3 WP4 SPD Network 33

3.3.1. Progress towards objectives 33

3.3.2. Significant and tangible results 33

WP4 SPD NETWORK (LEADER: SCOM) IS DIVIDED INTO 2 TASKS. IN ALL OF THEM ARE CONDUCTED STUDIES, ANALYSIS AND R&D ACTIVITIES BASED OF THE D2.1.1, D2.2.1, AND D2.3.1 REQUIREMENTS AND SPECIFICATIONS. 33

3.4 WP5 SPD Middleware & Overlay 37

3.4.1. Progress towards objectives 37
3.4.2. Significant and tangible results 37

3.5 WP6 Platform integration, validation & demonstration 39
3.5.1. Progress towards objectives 39
3.5.2. Significant and tangible results 39

3.6 WP7 Knowledge exchange & industrial validation 40
3.6.1. Progress towards objectives 40
3.6.2. Significant and tangible results 40

3.7 Italy 46
3.7.1. SESM 46
3.7.2. Ansaldo ASTS 50
3.7.3. Elsag Datamat 51
3.7.4. Eurotech 55
3.7.5. Selex Communications 58
3.7.6. Tecnologie delle Reti e dei Sistemi 60
3.7.7. Università degli Studi di Genova 62
3.7.8. Università degli Studi di Roma “La Sapienza” 64

3.8 Spain 68
3.8.1 Acorde Seguridad 68
3.8.2 European Software Institute/Tecnalia 70
3.8.3 Mondragon Goi Eskola Politecnikoa 72

3.9 Greece 74
3.9.1 ATHENA 74
3.9.2 Hellenic Aerospace Industry 76
3.9.3 Integrated Systems Development 78

3.10 Norway 78
3.10.1 Centre for Wireless Innovation 80
3.10.2 Movation AS 84

3.11 Slovenia 88
3.11.1 THYIA Tehonlogije (Coordinator) 88

3.12 Portugal 94
3.12.1. Critical Software 94

4 DELIVERABLES AND MILESTONES TABLES 103

4.1 Deliverables (excluding the periodic and final reports) 103

4.2 Milestones 104

5 PROJECT MANAGEMENT 105

5.1 Consortium management tasks and achievements 105

5.2 Encountered problems 105

5.3 Changes in the consortium 105

5.4 Project meetings 105

5.5 Project planning and status 106

5.6 Impact of deviations 106

5.7 Changes to the legal status 107

5.8 Project website 107

5.9 Dissemination and exploitation activities 107

5.10 Co-ordination activities 107

6 EXPLANATION OF THE USE OF THE RESOURCES 108

7 BENEFICIARIES WITHOUT A CORRESPONDING NATIONAL GRANT AGREEMENT FINANCIAL STATEMENTS – FORM C AND SUMMARY FINANCIAL REPORT 118

7.1 Certificates 118

Figures

Figure 1 Dissemination has an own standing on the pSHIELD wiki, same as the description of the Demonstrator 21
Figure 2 - View of the pSHIELD embedded system as provided to the Telenor Innovation Fair...........22

Tables

Table 1 – Project meetings 106
Table 3 – Person-Month Status Table 109
Tables 3.1 – Personnel, Subcontracting And Other Major Direct Cost Items 110

Acronyms

ESs	Embedded Systems
SPD	Security Privacy Dependability
ESNs	Embedded System Networks
ESD	Embedded System device
KETs	Key Enabling Technologies
WP	Work Package
PPR	Project Periodic Report
HW	Hardware
SW	Software
SotA	State of the Art
CR	Cognitive Radio
SDR	Software Defined Radio

1 Publishable summary

1.1 Summary

pSHIELD is a pilot project co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) within the context of Embedded Systems.

The SHIELD consortium proposes a pilot project (pSHIELD) which is a reduced R&D project addressing the core concepts of SHIELD, participated by the core/key partners and extended to a new group of partners coming from Norway and Portugal.

The pilot is foreseen to be an initial investigation to be enhanced with R&D activities that will be proposed in the future ARTEMIS Calls.

pSHIELD wants to investigate and validate a reduced but still consistent and coherent set of innovative concepts behind the SHIELD project, in a restricted scenario, with a rearranged consortium tailored on the pilot's scope.

The pSHIELD project aims at addressing Security, Privacy and Dependability (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.

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 available ones within a solid base that will become the reference milestone for a new generation of "SPD-ready" ESs. pSHIELD will approach SPD at 4 different levels: node, network, middleware and overlay. For each level, the state of the art within SPD of single technologies and solutions will be improved and integrated (hardware and communication technologies, cryptography, middleware, smart SPD applications, etc.). The SPD technologies will be enhanced with composable functionality, in order to fit in with the pSHIELD architectural framework.

The composability of the pSHIELD 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 within the pSHIELD framework will have impact on the development cycles of SPD in ESs because the qualification, (re-)certification and (re-)validation process of a pSHIELD framework instance will be faster, easier and more 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 the design, operational and maintenance phases. The pSHIELD approach is based on **modularity and expandability**, and can be adopted to bring built-in SPD solutions into the whole of the strategic sector of ARTEMIS, such as transportation, communication, health, energy and manufacturing.

To achieve these challenging goals the project aims to create 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, guaranteeing their maintenance and evolution in time.

In order to verify these important achievements, the project will **validate the pSHIELD integrated system by means of an application scenario**: monitoring of freight trains transporting hazardous material.

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 standardised SPD certificability, it is possible to estimate an overall 30% cost reduction for a full pSHIELD oriented design methodology.

To fulfil these challenging goals a European consortium has been set-up accounting major industries in the field of SPD in ESs. The high involvement of specialized SMEs, skilled universities and research centres makes the research team complete in order to make SHIELD a successful project.

The pSHIELD project will be focused on:

1. **Demonstrate composability**: The main novelty is the composability of SPD functionality at different layers among different technologies. The mechanism behind the composability could be investigated as well in this pilot project, at least limited to the design level.
2. **New technologies:** A sub-set of the previous SHIELD technologies will be used to be the very first significant example of SPD composability.
3. **Modularity and expandability:** As well as SHIELD, pSHIELD will maintain the same features, by preserving the work breakdown structure proposed in SHIELD.
4. **Innovative, modular, composable, expandable and high-dependable architectural framework:** the pilot project will be in charge of designing the core of this architectural framework, thus leaving to a future project its refinement and development
5. **Metrics:** metrics are the other novelty in the SHIELD project. They can be investigated in the pSHIELD project and used to validate the first basic functionalities of the framework.
6. **Validate the SHIELD integrated system in one application scenario:** the pilot project will validate the architectural framework by means of a specific application scenario.

1.2 Main results achieved

For the second reporting period of pSHIELD project (01.01.2011-30.06.2011) some intermediate objectives for the project were planned. An official request of seven months of extension has been sent to the Project Officer in April 2011.

pSHIELD is structured in work packages and main results are related to them.

The objectives for the **WP2 Scenarios, requirements and system design** are:

1. The definition of the SPD requirements and specifications of each layer, as well as of the overall system on the basis of the application scenario;
2. The definition of proper SPD metrics to assess the achieved SPD level of each layer, as well as of the overall system;
3. The definition of SHIELD system architecture. Identification of the SPD layers functionalities, their intra and inter layer interfaces and relationships.

The results of the first objective have been reported in D2.1.1. Results of the other two objectives have been reported in D2.2.1 and D2.3.1. D2.1.2, D2.2.2. and D2.3.2 are under finalisation.

Clearly significant and tangible results are:

- Top-level requirements specification for the application scenario
- High-level pSHIELD system requirements specification
- High-level SPD requirements specification for Node, Network, Middleware and Overlay Functional Layer
- High-level requirements specification for the SPD metrics
- High-level pSHIELD reference system architecture requirements specification
- High-level SPD Node, Network, Middleware and Overlay architecture requirements specification

The objectives for the **WP3 SPD Node** are:

1. Select a representative set of SPD technologies at Node level;
2. Develop appropriate composability mechanisms at such level;
3. Deliver a SPD node prototype.

The results of these objectives were partially planned within the period of this report. The activities performed are on-going and preliminary results brought to D3.1 and draft version of D3.2 and D3.2.

Clearly significant and tangible results are:

- A final first version D3.1 is developed.
- Embedded System security based on the whole design pyramid is investigated (protocol, algorithm, architecture, micro-architecture and circuit level)
- Potential architecture for SPD core module that include both TPM and MTM features
- Secure firmware, secure boot and bootstrapping with key management is investigated

- An architectural solution of nano node analysed for 3D integration technology is considered as first choice that can be also modelled by conceptual models.
- An architectural solution for micro/personal node is analysed as a possible upgrade of Contiki and Hydra OS solutions
- SPD conceptual models are proposed for sensor node based on the IEEE 802.11, IEEE 802.15.4 standards
- SotA solutions in the field of secondary power supply source to guarantee the correct system operation
- Studies of SotA node hardware and software available on market.
- Identification and description of hardware and software power nodes platforms.
- Development of hardware and software demonstrating selected pSHIELD node capabilities described by node architecture in D2.3.1.
- Design of a mobile and rugged high performance embedded node, the Power Node, with SPD intrinsic functionalities.
- Power Node board design.
- Power Node rugged enclosure design.
- Power node thermal studies.
- Design and implementation of board firmware.
- Operating system identification.
- Preliminary analysis of Power Node SDK.
- Results: Power Node PCB Layout design terminated. Operating system selection oriented in favour of Red Hat, CentOs or Scientific Linux.
- Research of the SotA within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.
- Evaluation of asymmetric cryptography algorithms and their suitability to pSHIELD.
- Evaluation of symmetric cryptography algorithms and their suitability to pSHIELD.
- Evaluation of message authentication codes algorithms and their suitability to pSHIELD.
- Results: The results of Task 3.3 activities are formalised within Deliverable 3.4 “SPD self-x and cryptographic technologies”, available at pSHIELD BSCW Server.
- Due to AES Rijndael being the cipher selected to be integrated into the nodes, some studies, about the original definition of the protocol, have been made to propose several code optimisations that let improve the efficient of the system.

The objectives for the **WP4 SPD Network** are:

1. Improve SPD technologies at Network level;
2. Develop potential prototype to be integrated in the demonstrator

The results of these objectives were partially planned within the period of this report. The activities performed are on-going and preliminary results brought to D4.1 and D4.2.

Clearly significant and tangible results are:

- Proposed new technologies enabling smart SPD driven transmissions.

- Performance analysis of various waveforms has been completed to select best candidates for the foreseen applications, both at the physical and MAC layer
- Realization and adaptation of HW and SW of multicore platform for the cognitive algorithm validation on embedded system
- Identification of spectrum sensing features for Cognitive Radio analysis
- Adaptation of sensing part of the Cognitive Radio simulator for pSHIELD
- Study of the different IDS approaches (misuse vs anomaly detection, and architecture) taking into account the requirements of sensor networks.
- Study the real resource footprint of wireless communication protocols (energy consumption among them) and its impact on performance on some commercially available devices.
- Study of anomaly detection systems.
- Transmission parameters smart adaptation according to radio resources observation towards trusted and dependable connectivity implementation.
- Implementation of a Cognitive Radio Node software simulator that is able to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly.
- Research relating to the state-of-the-art technology within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.
- Preliminary studies and discussions regarding the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices

The objectives for the **WP5 Middleware & Overlay** are:

1. Define a common semantic to describe the SPD interfaces and functionalities;
2. Introduce the Overlay concepts and functionalities;
3. Develop a prototype to be integrated in the demonstrators.

The results of these objectives were partially planned within the period of this report. The activities performed are on-going and preliminary results brought D5.1 and D5.2.

Clearly significant and tangible results are:

- Identification of pSHIELD semantic technologies;
- Semantic models to enable the pSHIELD seamless approach definition of main services at middleware layer;
- Prototypes of ontologies;
- Prototypes of semantic patterns of SPD composition;
- Experimental semantic engine for SPD composition;
- Analysis of the OSGI Knoplerfish platform as technological candidate for pSHIELD
- WP5 Middleware demonstrator;

- Service Oriented technology selection to address the seamless approach and interoperability requirements;
- High level design of the pSHIELD Middleware Architecture;
- High level design of a secure service discovery for pSHIELD Middleware;
- Analysis of semantic based access system and suggestion for semantically supported attribute-based access system
- Analysis of the SoA in Policy-based management architectures and protocols;
- Modelling of an Embedded System with Hybrid Automata;
- Design of the closed-loop control algorithms to enable the Composability functionality;
- Formalisation of a static procedure to model the composability of Embedded Systems by means of Hybrid Automata;
- Matlab-Simulink overlay models and simulations.

The WP5 work has been organised affording at the beginning three main tasks identified: semantic model, core services and overlay.

The semantic model has been analysed among the other involved partners and a good collaboration brought at the end of the period to a first proposal for the pSHIELD ontology.

The issue of middleware and overlay has been analysed from an architectural point of view and some alternative proposal have been studied and discussed between partners.

A Service Oriented approach has been investigated and selected as the one that would satisfy the seamless requirements of pSHIELD innovative features. This kind of approach is moreover suitable to develop all main functionalities, decoupling the technological details of the infrastructural layers (node and network) from the middleware and overlay layers.

The middleware has been identified as the broker between the high level functionalities exposed by core services and the overlay, and the node and network functional components. In this matter it will be important to exchange information between the other technical WPs (3,4) to detail the appropriate interfacing between the functional layers.

The Core Services realised by the middleware has been analysed and identified as the main functionality needed by the control system (implemented by the Overlay layer) in order to demonstrate the composability features of pSHIELD.

Research activities has been brought to a first modelling of the Overlay layer from a control perspective and some models have been proposed and verified through simulations.

The objectives for **WP6 Platform integration, validation & demonstration** are:

1. Integration of software components;
2. Validation of implemented solution through an iterative and incremental process;
3. Demonstration of the proposed architecture with a pilot demonstrator.

WP6 is at its initiating stage and practically out of the reporting period. According to Technical Annex and the prolongation the project received, **Task 6.4 Multi-Tecnology Demonstration** started on July, whereas the other tasks start from September 2011 and on. These tasks are **Task 6.1**

Multi-Technology System Integration, **Task 6.2 Multi-Technology Validation & Verification** and **Task 6.3 Lifecycle SPD Support**.

No deliverables were requested for the reference period concerning the current report. The development of discrete demonstrational prototypes from several partners can be considered as the first step of WP6 and the process of synthesizing a representative pSHIELD demonstrator, composed from integrated parts. These prototypes will be presented in the second review meeting in Oslo, where also the work plan and time schedule for WP6 will be detailed.

The objectives for **WP7 Knowledge exchange and industrial validation** are:

1. Industrial Dissemination,
2. Industrial Exploitation of results.

Industrial dissemination activities play an essential role, from an ARTEMIS perspective, in the validation of research results in the industrial sector. Therefore, such activities are considered as integral part of the project both in terms of industrial research and experimental development. Several partners have been involved in dissemination activities and results are reported in §1 of this report.

Clearly significant and tangible results are listed below:

pSHIELD established three dedicated Web spaces for users, internal and external to pSHIELD. These are as follows:

- *pSHIELD Web site* for pubic information, news and promotion of pSHIELD project. SESM is currently maintaining this site.
- *BSCW Server* for clean document exchange within the project internal users. THYIA is currently providing this facility.
- *pSHIELD semantic media wiki* platform for internal collaboration, visualization and day-to-day work support. CWIN is maintaining the wiki.

Following are the significant results achieved within this period for dissemination:

- A dedicated internal dissemination session has been arranged to improve knowledge sharing, cooperation and synergy.
- Four scientific articles published in high quality conferences and one journals have been published in this period, making in total seven scientific publications from pSHIELD.
- A PhD thesis is expected to be submitted by the end of this year.
- A PhD thesis was successfully discussed in April 2011 (PhD candidate Luca Bixio). Part of the research carried out during this work is strongly related to pSHIELD concepts.
- Industrial dissemination has identified necessary players to establish an ecosystem for industrial applications of pSHIELD. Besides the Telecom industry represented through Telenor contacts have been established to ABB, one of the leading power automation companies.

- Dissemination activities are currently collected on the pSHIELD wiki, and will be transferred from there to the public Web page and the D7.1.2 report

Industrial exploitation of pSHIELD results are currently under discussion. Areas for exploitation are:

- Sensor platform,
- Semantic middleware, and the
- Encrypted communication hardware.

The pSHIELD sensor platform was already deployed in the ESIS electrical motorbike and the measurement vehicle of the Norwegian Rail Authority (JBV). However, an extension to an industrial platform would require a.o. Dashboard functionality, GUI, user interface, End-to-end security, including encryption, and access control. Thus we currently favour another phase of developments together with the telecom and power industry in order to develop closer to actual industrial needs.

Following are the significant results achieved within this period for exploitation:

- The draft Exploitation plan has been circulated among the consortium members for feedback, suggestions and contributions. Only high-level feedback was given. We envisage to detail the feedback through dedicated phone conferences.

1.2.1. Measures on how pSHIELD has reached the scope

The initial evaluation summarized in the table below shows that pSHIELD has received good results. Only two areas have not sufficiently outlined the achievements, while 5 areas are identified as areas for improvement. The scope has been sufficiently outlined in a majority of 10 areas. In the remaining period of pSHIELD we will work with the results from this preliminary analysis.

Aspect of scope	Achieved (-,o,+)	Comment
411A) Has the project delivered a suitable architecture in the early phase of the project?	o	The architecture was outlined only after the first review
411B) Have suitable APIs been defined to ensure interworking?	o	The selected semantic approach for interworking allows handling of heterogeneous components
421A) Have the performed R&D approaches received the result?	+	Technology developments are well under-way,
421B) Are the results well in line with the state-of-the-art in research?	+	yes
421C) Does the prototypical development demonstrate the key features?	O, +	Some areas as the middleware clearly address the key features of pSHIELD, others still need to demonstrate SPD.
431A) Is a map of the business ecosystem established?	-	The map has not been explicitly drawn, but key players have been identified
431B) Does the map of the ecosystem contain the identification of playmakers?	+	Key players are partners in the project, and others outside of the project have been identified.
431C) Have initial contacts with playmakers and with a similar projects been established?	+, o	Initial contact with key players is established to the degree which can be expected for a pilot project. Contacts to other project needs still to be improved
441A) Are key players identified?	+	Yes, ranging from both security domain, energy automation and communication
441B) Is (initial) contact established?	+	yes
441C) Is the scientific dissemination being taken towards both conferences and journals?	+	Yes, papers have been submitted to both conferences and journals
441D) Is the feedback from the scientific dissemination documented?	-	Though feedback was given it is not yet documented
441E) Did internal dissemination take place, and did it include hand on experience?	+	Yes, internal dissemination is part of the physical meetings
441F) Does the project have a solid base of basic information through Web pages and public documents?	o	As a pilot project pSHIELD has initial documentation available. Work on public deliverables is ongoing.
441G) Does the project supports collaborative approaches?	+	The project has established a well-functioning collaborative platform, and is using phone conferences to a good extend.

1.2.2. Overall project impact

pSHIELD has been conceived as first phase (pilot) in the development of the overall SHIELD project. In this respect, when all the foreseen SHIELD functionalities will be deployed and exploited, impact on the market and its innovation will be the same highlighted in the SHIELD proposal.

The **current technological situation** for the ES solutions within the area of security, privacy and dependability are ad-hoc designed, implemented and deployed for each specific system pursuing sub-optimised performances and incompatibility at higher costs while the growing number and quality of treats are emphasising new challenges towards secure, dependable ES that will be operative in the augmented complexity scenarios of the future.

Lack in well defined SPD metrics constitutes, furthermore, big obstacles for a fast-validation and certification of the ES for many industrial applications where security, privacy, and dependability are with high priorities.

To resolve this situation, **the ES market** urgently **needs** an holistic built-in approach for a fast, flexible and standardised development of SPD solutions taking advantages from reusing previously validated results, adopting reference parameters to evaluate the product and deploying after standard and easier certification procedures.

During dissemination events mentioned below it was noted that the European industry in the ES is gaining a large momentum in terms of investments, stringent collaboration between academy and industry, governmental support, and development of significant competitive advantages with SPD type technologies. By proposing to realise embedded SPD via standardised design methods mainly based on *frameworks of composable technologies* to be settled within a specific industrial solution, a *set of on new SPD metrics* which allow fast, standard validations and certification as well as *methods and mechanism to easily design and keep SPD level compliance the whole of the system's lifetime*, the SHIELD project aims to **drastically improve SPD quality of ES** addressing the above mentioned industrial requirements.

1.3 Dissemination

PSHIELD project has been promoted through:

- internal dissemination to project partners,
- targeted industrial dissemination
- scientific dissemination
- contribution to workshops and exhibitions.

1.3.1 Internal dissemination to project partners

Internal dissemination has been arranged to share knowledge among the consortium partners and present the latest status and developed pSHIELD results. Such session has been envisioned to enhance cooperation and synergy. A project assembly had been held during 12-13. July 2011 in Rome and WP7 arranged a dedicated internal dissemination session for that. The agenda of this session has been distributed through an internal wiki page:
http://pshield.unik.no/wiki/PA_Rome_20110712-13#Dissemination_session_.2F_partners_prototypes_presentation

We collected all available pilot prototype developments and explained the goals of each prototype. A detailed discussion on the middleware followed, including the envisaged path for integration of the prototypes. As focus is on developments rather than tedious integration work, the project decided to go for specific demonstrators in the areas:

- a demonstration of composability of SPD functionality,
- integration across heterogeneous platforms,
- hardware prototypical implementations of specific layers,

Details of these prototypical demonstrators are listed on Web, and will be presented during the Review Meeting in September 2011.

Figure 1 Dissemination has an own standing on the pSHIELD wiki, same as the description of the Demonstrator

Another way of dissemination is through the intensive use of the semantic MediaWiki, which was specially developed for this project. The semantic MediaWiki can be seen as a quality control instrument, because all events within the project are captured through this tool. Details of the functionality of the semantic MediaWiki were described in the deliverable D1.1.1, and thus can you left out here.

Through the use of semantic technologies we ensure that we have consistent information, and that related information is "not longer away than two clicks". The usage of the wiki has shown a high usability for phone conferences and meetings, while the day-to-day work documentation on the wiki is rather an exception. Most partners prefer the traditional file format information.

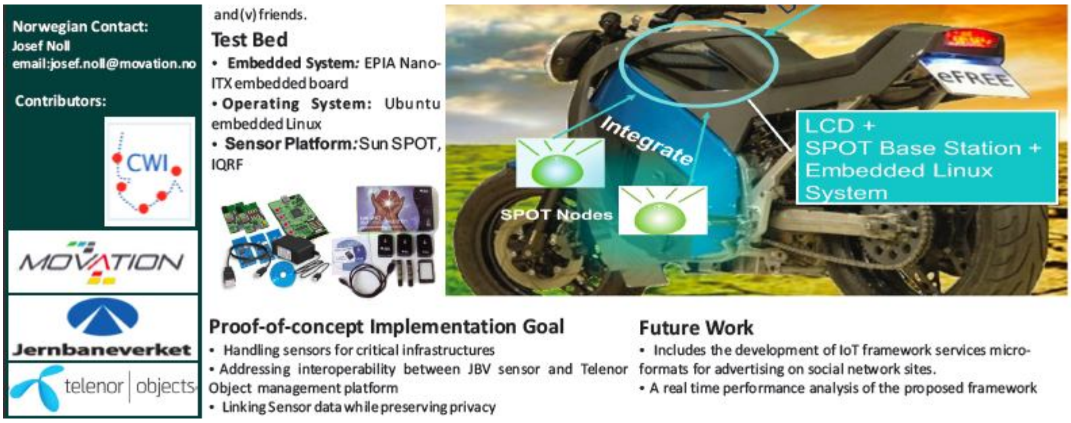
1.3.2 Targeted industrial dissemination

As the main goal of the shield is to generate impact in this area, the main focus has been on the dissemination of prototypical results to targeted industries. The 2nd focus has been to establish an ecosystem such that the solution developed by pSHIELD will be ready for the market in a relatively short timeframe. With this respect we collaborate with the telecom industry to ensure standardisation of communication and SPD features through heterogeneous platforms.

Targeted industrial dissemination in pSHIELD concentrates on the areas of hardware development for embedded systems and integration of pSHIELD embedded systems into standardised machine-to-machine or machine-to-business to business environment. Within the area of hardware development, the prototypical developments aren't yet ready to come into the market, thus they are only demonstrated to selected partners. In this area we have 3 main demonstrations being a components for secure, medication such as encryption off radio interfaces, platforms for embedded systems, and mattresses and middleware for SPD is functionality.
Establishing an ecosystem for pSHIELD means collaborating with relevant partners. As communication from the embedded systems towards end customers is seen as a major part, pSHIELD collaborated with the Telecom industry, in this case Telenor. Through this collaboration we ensure that results will be ready for standardisation in ETSI, the European Telecommunication Standards Institute. We have identified ETSI TS102.690, the Functional architecture for an M2M platform" as a promising starting point. However, this standard currently concentrates on the signalling and communication from a sensor system to the M2M platform and further to other entities, and does not envisage the SPD requirements on the embedded system.

During the reporting period pSHIELD engaged in the following targeted dissemination:

- A prototype of the pSHIELD personal node platform (embedded Linux) was provided to ESIS Norway and Telenor Objects, who used the platform within the electrical motorcycle of ESIS. This motorbike is part of the Telenor Innovation Fair at Fornebu, Norway (see Fig 7.2).


Norwegian Contact:
Josef Noll
email:josef.noll@movation.no

Contributors:

and (v) friends.

Test Bed
- Embedded System: EPIA Nano-ITX embedded board
- Operating System: Ubuntu embedded Linux
- Sensor Platform: Sun SPOT, IQRF

Proof-of-concept Implementation Goal
- Handling sensors for critical infrastructures
- Addressing interoperability between JBV sensor and Telenor Object management platform
- Linking Sensor data while preserving privacy

Future Work
- Includes the development of IoT framework services micro-formats for advertising on social network sites.
- A real time performance analysis of the proposed framework

Figure 2 - View of the pSHIELD embedded system as provided to the Telenor Innovation Fair

- Contact to the National Hospital "Rikshospitalet" was established. A presentation of "Security, Privacy and Dependability" of embedded systems was provided in spring 2011, with the goal of elaborating the applicability of pSHIELD integrated sensors for eHealth purposes, together with Telenor Objects. The feedback is documented on the wiki: http://pshield.unik.no/wiki/PSHIELD_Dissemination, mainly stating the lack of standards in this area.

- Another target company was Simlink, providing a SIM card with a WLAN beacon. Such a card will allow to have security options with OTA (over the air application install) and controlling of devices. We identified Simlink as an interesting technology for micro- and personal-nodes, being able to provide several sensor applications in the market.
- The first installation of the embedded system in the measurement vehicle of the Norwegian Rail Authority showed the need for an autonomous system. Most of the "of-the-shelf" products used in this integration did not support the autonomous operation, causing the installation on the train to be delayed to Q3.2011.
- Installation of a pSHIELD Sensor Network is underway with the Italian Railway provider, expecting the installation to take place in Q3.2011
- Further industrial actors are identified, namely ABB and the Norwegian Defence Research Establishment (FFI). Workshops are planned for Q3.2011 to establish the potential for pSHIELD results.

1.3.3 Scientific dissemination

Scientific dissemination of projects such as pSHIELD have a starting phase of 6 to 9 months prior to the first publications, and most of the publications come within the second and third year from the beginning of a project. pSHIELD is different, focussing on knowledge being present in the companies, and bringing these knowledge both to the scientific audience and the targeted industrial partners. Already during the first six months pSHIELD partners published two scientific papers and educated one master student. This second period shows an increase of the scientific dissemination with in total eight papers, out of which one paper was accepted as a Journal Paper.

The following scientific articles has been published (or accepted for publication) –

- Iñaki Garitano, Roberto Uribeetxeberria and Urko Zurutuza, "Review of SCADA Anomaly Detection Systems", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447
- Urko Zurutuza , Enaitz Ezpeleta, Álvaro Herrero and Emilio Corchado "Visualization of Misuse-based Intrusion Detection: Application to Honeynet Data", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447
- Ekhiotz Jon Vergara, Simin Nadjm-Tehrani, Mikael Asplund and Urko Zurutuza, "Resource Footprint of a Manycast Protocol Implementation on Multiple Mobile Platforms", Fifth International Conference on Next Generation Mobile Applications, Services and Technologies,NGMAST 2011, Cardiff, Wales, UK, 14-16 September 2011.

- Fiaschetti A., Lavorato F., Suraci V., Palo A., Taglialatela A., Morgagni A., Baldelli A., Flammini F., “On the use of semantic technologies to model and control Security, Privacy and Dependability in complex systems” Proc. Of 30th International Conference on. Computer Safety, Reliability and Security (SAFECOMP’11), Sep. 2011. Naples, Italy

- Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, "Interoperability of Security-enabled Internet of Things", to appear in Wireless Personal Communication Special Issue on "Internet of Things and Future Applications", Springer-Netherland, 2011.

- Mohammad M. R. Chowdhury, Josef Noll, "Securing Critical Infrastructure: A Semantically Enhanced Sensor Based Approach", 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic System Technology, WiRELESS ViTAE 2011, Chennai, India, Feb. 28-Mar. 2011.

- L. Bixio, M. Ottonello, M. Raffetto, and C.S. Regazzoni, “Comparison among Cognitive Radio Architectures for Spectrum Sensing,” EURASIP Journal on Wireless Communications and Networking, vol. 2011, Article ID 749891, 18 pages, 2011. doi:10.1155/2011/749891

- L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C. S. Regazzoni, Sk. S. Alam and C. Armani, “A Transmit Beamforming Technique for MIMO Cognitive Radios,”, Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, SDR'11 - WInnComm - Europe, Brussels, Belgium, June 22-24, 201

In total six PhD students have dedicated their research work to pSHIELD. The following PhD thesis where the majority of the works has been done as a part of pSHIELD scientific tasks is scheduled to finish by the end of this year.

- Sarfraz Alam, “Secure interworking of sensor systems in heterogeneous business environments” (tentative title), PhD thesis, to be finished in Q4.2011

- Sk. Shariful Alam, “Opportunistic Spectrum Sensing and Transmissions in Cognitive Radio” (tentative title), PhD thesis, to be finished in Q4.2013

1.3.4 Contribution to workshops and exhibitions

Besides pSHIELD has planned to participate the following events:

- ARTEMIS and ITEA Co-Summit in Helsinki, Finland on 25-26. October 2011. pSHIELD is expected to demonstrate the latest results of the project through a live prototype.

2 Project objectives for the period

Within the first reporting period of the pSHIELD project (01.01.2011-30.06.2011) some intermediate objectives for the project were planned as described within the previous section. In August 2010 the Coordinator SESM reported the causes for three month delay (agreed by the Project Assembly). A final delay was reported by THYIA (as Coordinator from December 2011) to the Project Officer by e-emails before the end of the reporting period and an official request of seven months of extension has been sent to JU Artemis on the 29 of March 2011.

The objectives for the **WP2 Scenarios, requirements and system design** are:

1. The definition of the SPD requirements and specifications of each layer, as well as of the overall system on the basis of the application scenario;
2. The definition of proper SPD metrics to assess the achieved SPD level of each layer, as well as of the overall system;
3. The definition of SHIELD system architecture. Identification of the SPD layers functionalities, their intra and inter layer interfaces and relationships.

The results of the objectives have been reported in **D2.1.1, D2.2.1 and D2.3.1**. Other deliverables (D2.1.2, D2.2.2. and D2.3.2, which aims at completing preliminary versions of activities reported in D2.1.1, D2.2.1 and D2.3.1) are under finalisation.

The objectives for the **WP3 SPD Node** are:

1. Select a representative set of SPD technologies at Node level;
2. Develop appropriate composability mechanisms at such level;
3. Deliver a SPD node prototype.

The results of these objectives were planned to be partially ready within the period of this report. The activities performed are on-going and preliminary results brought to **D3.1** SPD Node technologies prototype.

The objectives for the **WP4 SPD Network** are:

1. Improve SPD technologies at Network level;
2. Develop potential prototype to be integrated in the demonstrator

The results of these objectives were planned to be partially ready within the period of this report. The activities performed are reported in **D4.1** SPD Network technologies prototype and **D4.2** SPD network technologies prototype report (on-going).

The objectives for the **WP5 Middleware & Overlay** are:

1. Define a common semantic to describe the SPD interfaces and functionalities;
2. Introduce the Overlay concepts and functionalities;
3. Develop a prototype to be integrated in the demonstrators.

The results of these objectives were planned to be partially ready within the period of this report. The activities performed are on-going and preliminary results brought to **D5.1** pSHIELD Semantic model and **D5.2** SPD middleware and overlay functionalities prototype.

WP6 is at its initiating stage and practically out of the reporting period. According to Technical Annex and the prolongation the project received, **Task 6.4 Multi-Technology Demonstration** started on July, whereas the other tasks start from September 2011. No deliverables were requested for the reference period concerning the current report.

The objectives for **WP7 Knowledge exchange and industrial validation** are:

1. Industrial Dissemination,
2. Industrial Exploitation of results.

Industrial dissemination activities play an essential role, from an ARTEMIS perspective, in the validation of research results in the industrial sector. Therefore, such activities are considered as integral part of the project both in terms of industrial research and experimental development. Several partners have been involved in dissemination activities and results are reported in §1 of this report.

Industrial exploitation of pSHIELD results are currently under discussion. Areas for exploitation are:

- Sensor platform,
- Semantic middleware, and the
- Encrypted communication hardware.

The pSHIELD sensor platform was already deployed in the ESIS electrical motorbike and the measurement vehicle of the Norwegian Rail Authority (JBV). However, an extension to an industrial platform would require a.o. Dashboard functionality, GUI, user interface, End-to-end security, including encryption, and access control. Thus we currently favour another phase of developments together with the telecom and power industry in order to develop closer to actual industrial needs.

3 Work progress and achievements during the period

For Work Package

3.1 WP2 SPD Metrics Requirements and System Design

3.1.1 Progress towards objectives

WP2 (THYIA Leader) R&D activities are partitioned in three tasks, i.e., Task 2.1 (ASTS Leader), Task 2.2 (ESI Leader), and Task 2.3 (HAI Leader).

From these tasks the outcome in the Period 1 are three deliverables D2.1.1 (M3), D2.2.1 (M6), and D2.3.1(M6). Since a delayed was reported it was not expected a completion of D2.2.1 and D2.3.1 for the first period.

The partners contributing in WP2 are: SESM (9PMs), ASTS (14PMs), ATHENA (3PMs), CS (3PMs), CWIN (4PMs), ED (8PMs), ESI (2PMs), ETH (12PMs), HAI (9PMs), SCOM (1PM) and THYIA (11PMs).

Their main contributions were related to the following key objectives in pSHIELD: SESM (T2.1 & T2.3, SPD nodes), ASTS (T2.1, T2.2, Application scenario), ATHENA (T2.2, T2.3, network), CS(T2.1, T2.2, T2.3) CWIN (T2.1, T2.2, T2.3), ED(T2.1, T2.2, T2.3, middleware), ESI(T2.2, SPD metrics), ETH(T2.1, T2.2, T2.3, SPD nodes), HAI (T2.3, SPD layers, system, and network), SCOM (2.3, reviewer), THYIA (T2.1, T2.2, T2.3, involved almost in all targeted objectives).

Overall summary for WP2:

- Targeted objectives for D2.1.1 are reached up to 90%. Refinement will be done with respect to the new plane for M10 (now shifted for 7 months)
- Targeted objectives for D2.2.1 are reached up to 70%. Refinement will be done with respect to the new plane for M10 (now shifted for 7 months)
- Targeted objectives for D2.1.1 are reached up to 80%. Refinement will be done with respect to the new plane for M10 (now shifted for 7 months)
  - As major achievements in this task:
    - ✓ High-level pSHIELD reference system architecture requirements specification
    - ✓ High-level SPD Node, Network, Middleware and Overlay architecture requirements specification

D2.2.1 and D2.3.1 requirements specifications will be refined and aligned to D2.1.1 for the next review in September 2011.

3.1.2 Significant and tangible results

Clearly significant and tangible results are:

- Top-level requirements specification for the application scenario
- High-level pSHIELD system requirements specification
- High-level SPD requirements specification for Node, Network, Middleware and Overlay Functional Layer
- High-level requirements specification for the SPD metrics
- High-level pSHIELD reference system architecture requirements specification

- High-level SPD Node, Network, Middleware and Overlay architecture requirements specification

Based on these tangible results the consortium implemented these requirements specification in two additional documents for mid-term review: “Formalised Conceptual Models for the Key pSHIELD Concepts” and “Aggregation of SPD metrics during composition” in which appropriate conceptual models are developed to support development of detailed requirements and specifications for WP3, WP4, WP5 and WP6.

Related project taken in considerations are: **CESAR** (pSHIELD participants: ASTS, CS, ED, HAI, and ATHENA), **EMMON** (pSHIELD participants: CS and SESM), **IMSK** (pSHIELD participants: SCOM, THYIA), **SMART** (pSHIELD participants: HAI), **ECRYPT II.**

Liaison with the related projects in which we have 8 participants are contributing for dissemination of the R&D activities and results especially on the security, privacy and dependability issues for the future embedded systems. The exploitation prospective are huge if we take in consideration overlap with the business segments covered in CESAR, EMMON, SMART and IMSK project. With respect to the extension of this project, i.e. nSHIELD where we have an additional three scenarios, the range of possible market place is growing rapidly. Overall the exploitation of the pSHIELD project results has a solid foundation within the selected application scenario since the European rail transportation will go through a significant technology breakthrough where the new generation Embedded Systems for safety critical applications will play the key role.

3.2 WP 3 SPD Node

3.3.1 Progress towards objectives

Work Package 3 according to initial Technical Annex starts from month 1 till month 11 of the project. Due to reported delay mentioned in the beginning of this section the work started with a delay of 3-6 months with respect to the partners' contributions. In new project schedule with extension of 7 months work package 3 ends in month 17, that is in the end of October 2011.

WP3 SPD Node (Leader: SESM based on the PA decision taken in October 2010) is divided into 3 tasks: T3.1, T3.2, and T3.3. In all of them are conducted studies, analysis and R&D activities based of the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications.

3.3.2 Significant and tangible results

Task 3.1 Nano, Micro/Personal node (Task Leader: THYIA)

- A final first version D3.2 is developed.
- Embedded System security based on the whole design pyramid is investigated (protocol, algorithm, architecture, micro-architecture and circuit level)
- Potential architecture for SPD core module that include TPM and MTM features
- Secure firmware, secure boot and bootstrapping with key management is investigated
- An architectural solution of nano node analysed for 3D integration technology is considered as first choice that can be also modelled by conceptual models.
- An architectural solution for micro/personal node is analysed as a possible upgrade of Contiki and Hydra OS solutions
- SPD conceptual models are proposed for sensor node based on the IEEE 802.11, IEEE 802.15.4 standards
- SotA solutions in the field of "Energy Storage Systems" to guarantee the correct system operation
- SotA solutions in the field of "Power Harvesting Methods" to improve the autonomy of the power supply.
- Design of a protection circuit for a power supply (DC)

Task 3.2 Power node (Task Leader: ETH)

ETH works:

- Studies of SotA node hardware and software available on market.
- Identification and description of hardware and software power nodes platforms.
- Development of hardware and software demonstrating selected pSHIELD node capabilities described by node architecture in D2.3.1.
- Design of a mobile and rugged high performance embedded node, the Power Node, with SPD intrinsic functionalities.
- Power Node board design.
- Power Node rugged enclosure design.
- Power node thermal studies.
- Design and implementation of board firmware.

- Operating system identification.
- Preliminary analysis of Power Node SDK.
- Results: Power Node PCB Layout design terminated. Operating system selection oriented in favour of Red Hat, CentOs or Scientific Linux.

SESM works:

- Works based on D2.3.1 requirements and specification and D2.3.1 architecture.
- Updated works based on endorsed M0.1 and M0.2 documents.
- Based on developed conceptual pSHIELD SPD Node Layer model: design of Power Node Prototype.
- Development of SW/HW framework based on Xilinx development board.
- Implementation of pSHIELD Node Layer blocks in VHDL and C language code.
- Implementation of pSHIELD Node Adapter blocks: pSHIELD Interface and SPD Node Status.
- Implementation of pSHIELD Node Adapter block: Security and Privacy based on hardware data encryption/decryption.
- Implementation of pSHIELD Node Adapter block: Dependability based reconfigurable application bit-stream.
- Development and implementation of application: A-FSK Demodulator code.
- Design and development of DAQ Adapter hardware board.

AS works:

- SotA solutions in the field of secondary power supply source to guarantee the correct system operation.
- SotA solutions in the field of "Power Harvesting Methods" to improve the autonomy of the power supply.
- Design of a protection circuit for a power supply (AC)

Task 3.3 Dependable self-x and cryptographic technologies (Task Leader: AS)

- Research of the SotA within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.
- Evaluation of asymmetric cryptography algorithms and their suitability to pSHIELD.
- Evaluation of symmetric cryptography algorithms and their suitability to pSHIELD.
- Evaluation of message authentication codes algorithms and their suitability to pSHIELD.
- Results: The results of Task 3.3 activities are formalised within Deliverable 3.4 "SPD self-x and cryptographic technologies", available at pSHIELD BSCW Server.
- Due to AES Rijndael is the cipher selected to be integrated in the nodes, some studies, about the original definition of the protocol, have been made to propose several code optimisations that let improve the efficient of the system.

Status of the deliverables:

- D3.1 SPD node technologies prototypes (internal M15) – The draft version with chapter structure assigned to tasks is available at BSCW server. Works in tasks are in progress. The contribution from CWIN and MAS is 80% ready.

- D3.2 SPD nano, micro/personal node technologies prototype report (public M16) – draft document is available at BSCW Server.

- D3.3 SPD power node technologies prototype report (public M17) – The draft version with chapter structure agreed by task partners is available at BSCW server. Partners works are in progress. SESM contribution is 50% ready.

- D3.4 SPD self-x and cryptographic technologies prototype report (public M16) – draft deliverable is available at BSCW Server, it is 30% ready with main task partner CS contribution included.

3.3 WP4 SPD Network

3.3.1. Progress towards objectives

According to T4.1 objectives SCOM and UNIGE have proposed new technologies enabling smart SPD driven transmissions. In particular, the cognitive radio (CR) paradigm, which is usually based on Software Defined Radio (SDR), has been proposed to deal with such transmissions. CR is composable and expandable and modular by definition. In fact, it has been designed to accommodate these features.

Issues related to programmable radio platforms, both HW and SW, have been investigated in order to optimize the architecture of proposed CR.

Performance analysis of various waveforms has been completed to select best candidates for the foreseen applications, both at the physical and MAC layer.

Particular attention has been devoted in the definition of MAC and forwarding protocols capable to support mesh operation with minimum overhead in term of bandwidth and delay.

Moreover, the modules of a cognitive radio which enable the required smart SPD driven transmissions and trusted and dependable connectivity have been analyzed. In particular, the security threats related to these modules in reaching the goals have been discussed and some solutions to overcome such limitations have been identified. SCOM will use the remaining PMs to study the effectiveness of the identified solutions to address the open issues, through simulation models of the proposed algorithms.

3.3.2. Significant and tangible results

WP4 SPD Network (Leader: SCOM) is divided into 2 tasks. In all of them are conducted studies, analysis and R&D activities based of the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications.

In this period, SCOM provided some results on the benefits which can be obtained by introducing the considered new technologies for smart SPD transmissions and trustable and dependable connectivity. At the moment SCOM has spent about 70% of the effort and it is planning to spend the rest of the PMs to achieve the objectives according to the pSHIELD technical annex.

Task	Partner	Progress	Indicators
4.1	SCOM	Proposed new technologies enabling smart SPD driven transmissions.	Internal report
4.1	SCOM	Performance analysis of various waveforms has been completed to select best candidates for the foreseen applications, both at the physical and MAC layer	Internal report
4.1	SCOM	Realization and adaptation of HW and SW of multicore platform for the cognitive algorithm validation on embedded system	Internal report
4.1	UNIGE	Identification of spectrum sensing features for Cognitive Radio analysis	Publication

4.1	UNIGE	Adaptation of sensing part of the Cognitive Radio simulator for pSHIELD	Publication

The implemented Cognitive Radio Node is able to receive radio parameters from moving hosts and automatically detect possible threats. The internal architecture of the Node learns typical safe environments features thus detecting the presence of external attackers by analysing radio parameters.

In a considered scenario, the cognitive node always updates the radio parameters (SNR, BER and Transmitter Power, PTX) for the self-awareness purposes. There are some specific provisions considered to design this kind of simulator used for the Security, Privacy and Dependability (SPD) in the context of integrated and interoperating heterogeneous applications.

When an agent enters the scene, the cognitive node becomes aware of the radio parameters of the agent either by using the spectrum sensing technique or from a direct communication from the agent itself. In this way the node can update its radio information for using the radio resources efficiently and securely. The cognitive node has an internal knowledge of all the radio parameters which would be considered in the selected environment and their respective variation models. The node knows itself from a configuration database what frequencies are used by which agent and which frequencies are free to use. If a new agent enters in the scene while continuing communication, the cognitive node sense the radio parameters of the agent and is able to modify and adapt agents radio parameters when necessary.

In the presence of a jammer of specific frequency in a cluster, the cognitive node sends a message to the agents to adjust the radio parameters properly, i.e., by changing either the frequency or the transmission power (spread spectrum or noise based data transmission of signals).

Moving agents in the scene and the presence of jammers are dynamically created through a specific simulator that was built to this aim. The simulator sends to the cognitive node is the positioning data, namely the trajectories of the agents (like a tracker) and radio data on the situation. More specifically, each agent is controlled by the cognitive mobile node, considered as an entity, after the registration process in the area under observation, periodically sends information on the quality of communication.

Task	Partner	Progress	Indicators
4.2	MGEP	Study of the different IDS approaches (misuse vs anomaly detection, and architecture) taking into account the requirements of sensor networks.	Internal report
4.2	MGEP	Study the real resource footprint of wireless communication protocols (energy consumption among them) and its impact on performance on some commercially available devices.	Publication
4.2	MGEP	Study of anomaly detection systems.	Publication
4.2	UNIGE	Transmission parameters smart adaptation according to radio resources observation towards trusted and dependable connectivity implementation.	Publication
4.2	UNIGE	Implementation of a Cognitive Radio Node software simulator that is able	Publication

		to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly.	
4.2	CS	Research relating to the state-of-the-art technology within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.	Deliverable
4.2	CS	Preliminary studies and discussions regarding the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices	Deliverable

The main activity of MGEP in pSHIELD is on the study of the requirements for lightweight link-layer secure communication in wireless sensor network scenarios and the design and development of proper schemes focusing on confidentiality. More specifically, intrusion detection systems (IDS) have been studied.

Misuse detection based IDS monitors the activities of a system and compares them with signatures of attacks that are stored in a database. This kind of IDS have high accuracy rates, however, due to the high increase of new attacks and the continuous variants of them it is extremely difficult to have an updated set of rules. On the other hand, anomaly detection depends greatly on the supposition that users and networks behave in a sufficiently regular way and therefore, any significant deviation from such behaviour could be considered as an evidence of an intrusion. **Hybrid IDS, where the system is based in anomaly and misuse techniques best fit in WSN.** However, there are application areas, such as SCADA systems, where anomaly detection performs better than in traditional information and communications technology (ICT) networks. SCADA communications are deterministic, and their operation model is often cyclical. Based on this premise, modelling normal behaviour by mining specific features sets gets feasible and efficient.

Another important issue is the architecture deployed for the IDS. Attacks can be detected locally in nodes, centralized in a main processing node or even through the collaboration of global and local agents integrated in the application layer of nodes. Although it may result in an increase in the resource requirements of a sensor node, **the global security level that gives distributed intrusion detection is considered more reliable** than the centralized one.

The centralized architecture could not detect as many attacks, due to the low data rate of wireless communication and energy constraints of sensor nodes that could not afford the transmission of massive audit data to a base station. However, in a distributed intrusion detection system, no node is trustful, due to potential inside attackers. For that reason is necessary to propose an agent able to detect anomalies in its host neighbours. The protection of the nodes is also necessary so it is high recommended to implement a local agent for the nodes able to analyse possible local feature changes.

Other activities of T4.2 are concerned to the design of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks, aiming to reduce the vulnerability to attacks depleting communication resources and node energy.

As Confidentiality, Data Integrity and Service Availability are also addressed by security systems in wired networks Energy is unique to the wireless sensor networks due to the resource limitation constraint. Regarding energy there is a necessity to asses the existing protocols and applications in different real situations as they are initially designed and studied in a simulation environment. We have studied the **resource footprint (energy consumption among them) and its impact on performance on some commercially available devices**. We could see both how different aspects of the communications protocol contributes to the footprint and how this in turn affects the performance. The methodologies used can be applied to other protocols and applications, aiding in future optimisations. Vulnerabilities in the communications protocol could lead to greater energy consumption and eventually to a DoS attack.

In accordance with CS's contribution shown within the Technical Annex, CSW's main contribution to pSHIELD is within the areas of "Cryptography for low cost nodes" and "Dependable authentic key distribution mechanisms". These activities have been planned according to three main phases: Research, Selection and Integration.

The activities performed by CS in this task are being performed in parallel with the work on Task 3.3. The main activity undertaken was the research relating to the state-of-the-art technology within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.

Within this second period, the main activities have involved studies of SotA cryptography libraries available for resource constraint devices, according to outcome of first period research studies and pSHIELD's application scenario, a complementary study to test the respective algorithms implementation on the hardware of a possible micro (TelosB mote) and power (Linux based computer) node, and the selection and description of cryptographic libraries to be used in the third phase of CSW activities.

After the research studies and evaluations performed in the first period, in this second period the main activities in this task concerned preliminary studies and discussions regarding the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices (pSHIELD application scenario)

The results of Task 4.2 activities are formalised in Deliverable 4.2 "SPD network technologies prototypes report", available at the pSHIELD BSCW Server

3.4 WP5 SPD Middleware & Overlay

3.4.1. Progress towards objectives

WP5 (SELEXELSAG Leader) R&D activities are partitioned in four tasks, i.e., Task 5.1 SPD driven Semantics (TRS Leader), Task 5.2 Core SPD services (THYIA Leader), Task 5.3 Policy-based management (ESI ED Leader), and Task 5.4 Overlay monitoring and reacting system by security agents (ED Leader).

Here below the list of the deliverables for WP5 (delivery month definition):

Deliverables

- Public
  - ➢ D5.3 pSHIELD semantic models report (M18)
  - ➢ D5.4 SPD middleware and overlay functionalities report (M18)
- Internal
  - ➢ D5.1 pSHIELD semantic models (M15)
  - ➢ D5.2 SPD middleware and overlay functionalities prototype (M15)

Moreover WP5 Partners have participated to definition of Mid-term review additional deliverables:

- Internal
  - ➢ M0.1: Formalized conceptual models of the key pSHIELD concepts (M13)
  - ➢ M0.5: The pSHIELD focus areas, key innovations and project outputs (M13)

The partners contributing in WP5 are: SE (37PMs), UNIROMA1 (22PMs), CS (20PMs), ATHENA
(4PMs), CWIN (7PMs), TECNALIA (1PMs), TRS (14PMs), and THYIA (11PMs).

Overall summary for WP5:

- Targeted objectives for D5.1 are reached up to 75% (at the moment 100%)
- Targeted objectives for D5.2 are reached up to 75% (at the moment 100%)
- Targeted objectives for D5.3 are reached up to 30% (at the moment 50%)
- Targeted objectives for D5.4 are reached up to 30% (at the moment 50%)

3.4.2. Significant and tangible results

- – Identification of pSHIELD semantic technologies;
- – Semantic models to enable the pSHIELD seamless approach definition of main services at middleware layer;
- – Prototypes of ontologies;
- – Prototypes of semantic patterns of SPD composition;
- – Experimental semantic engine for SPD composition;
- – Analysis of the OSGI Knoplerfish platform as technological candidate for pSHIELD
- – WP5 Middleware demonstrator;
- – Service Oriented technology selection to address the seamless approach and

interoperability requirements;

- High level design of the pSHIELD Middleware Architecture;
- High level design of a secure service discovery for pSHIELD Middleware;
- Analysis of semantic based access system and suggestion for semantically supported attribute-based access system
- Analysis of the SoA in Policy-based management architectures and protocols;
- Modelling of an Embedded System with Hybrid Automata;
- design of the closed-loop control algorithms to enable the Composability functionality;
- Formalisation of a static procedure to model the composability of Embedded Systems by means of Hybrid Automata;
- Matlab-Simulink overlay models and simulations.

The WP5 work has been organised affording at the beginning three main tasks identified: semantic model, core services and overlay.

The semantic model has been analysed among the other involved partners and a good collaboration brought at the end of the period to a first proposal for the pSHIELD ontology.

The issue on middleware and overlay has been analysed from an architectural point of view and some alternative proposal have been studied and discussed between partners.

A Service Oriented approach has been investigated and selected as the one that would satisfy the seamless requirements of pSHIELD innovative features. This kind of approach is moreover suitable to develop all main functionalities decoupling the technological details of the infrastructural layers (node and network) from the middleware and overlay layers.

The middleware has been identified as the broker between the high level functionalities exposed by core services and the overlay, and the node and network functional components. In this matter will be important to exchange information between the other technical WPs (3,4) to detail the appropriate interfacing between the functional layers.

The Core Services realised by the middleware have been analysed and identified as the main functionality needed by the control system (implemented by the Overlay layer) in order to demonstrate the composability features of pSHIELD.

Research activities have been brought to a first modelling of the Overlay layer from a control perspective and some models has been proposed and verified through simulations.

3.5 WP6 Platform integration, validation & demonstration

3.5.1. Progress towards objectives

Work Package 6 is at its initiating stage and practically out of the reporting period. According to Technical Annex and the prolongation the project received, **Task 6.4 Multi-Tecnology Demonstration** started on July, whereas the other tasks start from September 2011 and on. These tasks are **Task 6.1 Multi-Technology System Integration**, **Task 6.2 Multi-Technology Validation & Verification** and **Task 6.3 Lifecycle SPD Support**. No deliverables were requested for the reference period concerning the current report. The development of discrete demonstrational prototypes from several partners can be considered as the first step of WP6 and the process of synthesizing a representative pSHIELD demonstrator, composed from integrated parts. These prototypes will be presented in the second review meeting in Oslo, where also the work plan and time schedule for WP6 will be detailed.

3.5.2. Significant and tangible results

N/A.

3.6 WP7 Knowledge exchange & industrial validation

3.6.1. Progress towards objectives

WP7 consists of two tasks, Dissemination and Exploitation. This report describes the outcomes of both tasks.

3.6.2. Significant and tangible results

The performed and on-going activities at each task are summarized as follows mentioning *measurable indicators*, and *significant* and *tangible results*:

T7.1 – Dissemination (Leader: SESM)

PSHIELD project has been promoted through:

- internal dissemination to project partners,
- targeted industrial dissemination
- scientific dissemination
- contribution to workshops and exhibitions.

Internal dissemination to project partners

Internal dissemination has been arranged to share knowledge among the consortium partners and present the latest status and developed pSHIELD results. Such session has been envisioned to enhance cooperation and synergy. A project assembly had been held during 12-13. July 2011 in Rome and WP7 arranged a dedicated internal dissemination session for that. The agenda of this session has been distributed through an internal wiki page:
http://pshield.unik.no/wiki/PA_Rome_20110712-13#Dissemination_session_.2F_partners_prototypes_presentation

We collected all available pilot prototype developments and explained the goals of each prototype. A detailed discussion on the middleware followed, including the envisaged path for integration of the prototypes. As focus is on developments rather than tedious integration work, the project decided to go for specific demonstrators in the areas:

- a demonstration of composability of SPD functionality,
- integration across heterogeneous platforms,
- hardware prototypical implementations of specific layers,

Details of these prototypical demonstrators are listed on Web, and will be presented during the Review Meeting in September 2011.

Another way of dissemination is through the intensive use of the semantic MediaWiki, which was specially developed for this project. The semantic MediaWiki can be seen as a quality control instrument, because all events within the project are captured through this tool. Details of the functionality of the semantic MediaWiki were described in the deliverable D1.1.1, and thus can you left out here.

Through the use of semantic technologies we ensure that we have consistent information, and that related information is "not longer away than two clicks". The usage of the wiki has shown a high usability for phone conferences and meetings, while the day-to-day work documentation on the wiki is rather an exception. Most partners prefer the traditional file format information.

Targeted industrial dissemination

As the main goal of the shield is to generate impact in this area, the main focus has been on the dissemination of prototypical results to targeted industries. The 2nd focus has been to establish an ecosystem such that the solution developed by pSHIELD will be ready for the market in a relatively short timeframe. With this respect we collaborate with the telecom industry to ensure standardisation of communication and SPD features through heterogeneous platforms.

Targeted industrial dissemination in pSHIELD concentrates on the areas of hardware development for embedded systems and integration of pSHIELD embedded systems into standardised machine-to-machine or machine-to-business to business environment. Within the area of hardware development, the prototypical developments aren't yet ready to come into the market, thus they are only demonstrated to selected partners. In this area we have 3 main demonstrations being a components for secure, medication such as encryption off radio interfaces, platforms for embedded systems, and mattresses and middleware for SPD is functionality.

Establishing an ecosystem for pSHIELD means collaborating with relevant partners. As communication from the embedded systems towards end customers is seen as a major part, pSHIELD collaborated with the Telecom industry, in this case Telenor. Through this collaboration we ensure that results will be ready for standardisation in ETSI, the European Telecommunication Standards Institute. We have identified ETSI TS102.690, the Functional architecture for an M2M platform" as a promising starting point. However, this standard currently concentrates on the signalling and communication from a sensor system to the M2M platform and further to other entities, and does not envisage the SPD requirements on the embedded system.

During the reporting period pSHIELD engaged in the following targeted dissemination:

- A prototype of the pSHIELD personal node platform (embedded Linux) was provided to ESIS Norway and Telenor Objects, who used the platform within the electrical motorcycle of ESIS. This motorbike is part of the Telenor Innovation Fair at Fornebu, Norway (see Fig 7.2).

- Contact to the National Hospital “Rikshospitalet” was established. A presentation of "Security, Privacy and Dependability" of embedded systems was provided in spring 2011, with the goal of elaborating the applicability of pSHIELD integrated sensors for eHealth purposes, together with Telenor Objects. The feedback is documented on the wiki: http://pshield.unik.no/wiki/PSHIELD_Dissemination, mainly stating the lack of standards in this area.

- Another target company was Simlink, providing a SIM card with a WLAN beacon.

Such a card will allow to have security options with OTA (over the air application install) and controlling of devices. We identified Simlink as an interesting technology for micro- and personal-nodes, being able to provide several sensor applications in the market.

- The first installation of the embedded system in the measurement vehicle of the Norwegian Rail Authority showed the need for an autonomous system. Most of the “of-the-shelf” products used in this integration did not support the autonomous operation, causing the installation on the train to be delayed to Q3.2011.
- Installation of a pSHIELD Sensor Network is underway with the Italian Railway provider, expecting the installation to take place in Q3.2011
- Further industrial actors are identified, namely ABB and the Norwegian Defence Research Establishment (FFI). Workshops are planned for Q3.2011 to establish the potential for pSHIELD results.

Scientific dissemination

Scientific dissemination of projects such as pSHIELD have a starting phase of 6 to 9 months prior to the first publications, and most of the publications come within the second and third year from the beginning of a project. pSHIELD is different, focussing on knowledge being present in the companies, and bringing these knowledge both to the scientific audience and the targeted industrial partners. Already during the first six months pSHIELD partners published two scientific papers and educated one master student. This second period shows an increase of the scientific dissemination with in total eight papers, out of which one paper was accepted as a Journal Paper.

The following scientific articles has been published (or accepted for publication);

- Iñaki Garitano, Roberto Uribeetxeberria and Urko Zurutuza, “Review of SCADA Anomaly Detection Systems”, Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447
- Urko Zurutuza , Enaitz Ezpeleta, Álvaro Herrero and Emilio Corchado “Visualization of Misuse-based Intrusion Detection: Application to Honeynet Data”, Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447
- Ekhiotz Jon Vergara, Simin Nadjm-Tehrani, Mikael Asplund and Urko Zurutuza, “Resource Footprint of a Manycast Protocol Implementation on Multiple Mobile Platforms”, Fifth International Conference on Next Generation Mobile Applications, Services and Technologies,NGMAST 2011, Cardiff, Wales, UK, 14-16 September 2011.
- Fiaschetti A., Lavorato F., Suraci V., Palo A., Taglialatela A., Morgagni A., Baldelli A., Flammini F., “On the use of semantic technologies to model and control Security,

Privacy and Dependability in complex systems" Proc. Of 30th International Conference on. Computer Safety, Reliability and Security (SAFECOMP'11), Sep. 2011. Naples, Italy

- Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, "Interoperability of Security-enabled Internet of Things", to appear in Wireless Personal Communication Special Issue on "Internet of Things and Future Applications", Springer-Netherland, 2011.
- Mohammad M. R. Chowdhury, Josef Noll, "Securing Critical Infrastructure: A Semantically Enhanced Sensor Based Approach", 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic System Technology, WiRELESS ViTAE 2011, Chennai, India, Feb. 28-Mar. 2011.
- L. Bixio, M. Ottonello, M. Raffetto, and C.S. Regazzoni, "Comparison among Cognitive Radio Architectures for Spectrum Sensing," EURASIP Journal on Wireless Communications and Networking, vol. 2011, Article ID 749891, 18 pages, 2011. doi:10.1155/2011/749891
- L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C. S. Regazzoni, Sk. S. Alam and C. Armani, "A Transmit Beamforming Technique for MIMO Cognitive Radios,", Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, SDR'11 - WInnComm - Europe, Brussels, Belgium, June 22-24, 201

In total six PhD students have dedicated their research work to pSHIELD. The following PhD thesis where the majority of the works has been done as a part of pSHIELD scientific tasks is scheduled to finish by the end of this year.

- Sarfraz Alam, "Secure interworking of sensor systems in heterogeneous business environments" (tentative title), PhD thesis, to be finished in Q4.2011
- Sk. Shariful Alam, "Opportunistic Spectrum Sensing and Transmissions in Cognitive Radio" (tentative title), PhD thesis, to be finished in Q4.2013

Contribution to workshops and exhibitions

Besides pSHIELD has planned to participate the following events:

- ARTEMIS and ITEA Co-Summit in Helsinki, Finland on 25-26. October 2011. pSHIELD is expected to demonstrate the latest results of the project through a live prototype.

Significant outcomes:

- A dedicated internal dissemination session has been arranged to improve knowledge sharing, cooperation and synergy.

- Four scientific articles published in high quality conferences and one journals have been published in this period, making in total seven scientific publications from pSHIELD.
- A PhD thesis is expected to be submitted by the end of this year.
- A PhD thesis was successfully discussed in April 2011 (PhD candidate Luca Bixio). Part of the research carried out during this work is strongly related to pSHIELD concepts.
- Industrial dissemination has identified necessary players to establish an ecosystem for industrial applications of pSHIELD. Besides the Telecom industry represented through Telenor contacts have been established to ABB, one of the leading power automation companies.
- Dissemination activities are currently collected on the pSHIELD wiki, and will be transferred from there to the public Web page and the D7.1.2 report

T7.2 – Exploitation (Leader: CWIN)

Industrial exploitation of pSHIELD results are currently under discussion. Areas for exploitation are:

- ➢ Sensor platform,
- ➢ Semantic middleware, and the
- ➢ Encrypted communication hardware.

The pSHIELD sensor platform was already deployed in the ESIS electrical motorbike and the measurement vehicle of the Norwegian Rail Authority (JBV). However, an extension to an industrial platform would require a.o. Dashboard functionality, GUI, user interface, End-to-end security, including encryption, and access control. Thus we currently favour another phase of developments together with the telecom and power industry in order to develop closer to actual industrial needs.

Significant outcomes:

- The draft Exploitation plan has been circulated among the consortium members for feedback, suggestions and contributions. Only high-level feedback was given. We envisage to detail the feedback through dedicated phone conferences.

Status of the deliverables:

- D7.1.1 Web site – The project Web site was up online according to schedule on month 2 and thus WP7 achieved the milestone M1. The deliverable D7.1.1 was accepted during the mid-term review meeting (22. March 2011).

- D7.1.2 Dissemination report – The preliminary table of contents has been already been proposed and we are on course to achieve the deadline
- D7.2.1 Exploitation plan – The preliminary table of contents & responsible partners have been proposed.

For Partner (grouped by Country)

The following tables resume the work progress and achievements during the reporting period.

3.7 Italy

3.7.1. SESM

Beneficiary5:	SESM
Work Package(s)	WP16 – Project management (total 36PM) WP2 – SPD metric, requirements and system design (total 9PM) WP3 – SPD node (total 29PM) WP6 – Platform integration, validation & demonstration (total 9PM) WP7 – Knowledge exchange and industrial validation (total 6PM)
Task(s)	Task 1.1 Project management Task 1.2 Liaisons Task 2.1 Multi-technology requirements & specification Task 2.3 Multi-technology architectural design Task 3.2 Power node Task 6.2 Multi-Technology Validation & Verification Task 6.3 Lifecycle SPD Support Task 7.1 Dissemination
Period:	1st January 2011 – 30st June 2011
Effort planned in this period:	Task 1.1 Project management – 8PM Task 1.2 Liaisons – 7PM Task 2.1 Multi-technology requirements & specification – 1PM Task 2.3 Multi-technology architectural design – 2PM Task 3.2 Power node – 15PM Task 6.2 Multi-Technology Validation & Verification – 1PM Task 6.3 Lifecycle SPD Support – 1PM Task 7.1 Dissemination – 1PM
Effort actual or spent in this period:	Task 1.1 Project management – 5PM Task 1.2 Liaisons – 5PM Task 2.1 Multi-technology requirements & specification – 1PM Task 2.3 Multi-technology architectural design – 1PM Task 3.2 Power node – 10PM Task 6.2 Multi-Technology Validation & Verification – 0PM Task 6.3 Lifecycle SPD Support – 0PM Task 7.1 Dissemination – 1PM

[5] This report is per Beneficiary, and it provides as many as WPs in which it is involved each Beneficiary (see as PPR - Project Periodic Report, section 1.2.7.)

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

% of work completed at the end of the period (indicative):	Task 1.1 Project management – 62,5% Task 1.2 Liaisons – 71,43% Task 2.1 Multi-technology requirements & specification – 100% Task 2.3 Multi-technology architectural design – 50% Task 3.2 Power node – 66,66% Task 6.2 Multi-Technology Validation & Verification – 0% Task 6.3 Lifecycle SPD Support – 0% Task 7.1 Dissemination – 100%

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

- Task 1.1 Project management
  - Role of Technical Project Coordinator (TCM) during the period.
  - Role of WP3 Leader, after withdraw of previous WP leader.
- Task 1.2 Liaisons
  - Continuous studies on projects concerning topics related to pSHIELD.
- Task 2.1 Multi-technology requirements & specification
  - Extensive analysis of TA (Annex I) described goals in node layer area.
  - Analysis of relevance to Sub-Programme 6 Priority, Industry Priorities and Artemis Targets.
  - Definition of Nodes requirements following above goals.
  - Node requirements contributed to deliverable D2.1.1 chapter 8 "Node Requirements and Specifications" with subchapters containing detailed references to Annex I.
  - Continuous studies on requirements that are used in Tasks 2.3 and 3.2.
  - Refinement of requirements to be updated in next revision of D2.3.1 and in D2.3.2.
- Task 2.3 Multi-technology architectural design
  - Continuous studies of SotA technologies available on market.
  - Development of pSHIELD generic node architecture on the base of previously prepared for D2.1.1 node requirements and specifications.
  - Works on pSHIELD SPD Node Architecture based on endorsed by consortium documents M0.1 and M0.2.
  - Design of generic conceptual model of a pSHIELD node for all node types, which can be implemented in different architectures, providing different functionalities, different SPD compliance levels and different services, depending on the type of node and application field. Three node types represent very different devices but they share the same conceptual model, enabling a seamless composability. Contributed to D2.3.1 (Node section).
- Task 3.2 Power node
  - Continuous studies of SotA node hardware and software available on market.
  - Development of hardware and software demonstrating selected pSHIELD node capabilities described by node architecture in D2.3.1.
  - Result:
    - Works based on D2.3.1 requirements and specification and D2.3.1 architecture.
    - Updated works based on endorsed M0.1 and M0.2 documents.
    - Based on developed conceptual pSHIELD SPD Node Layer model: design of Power Node Prototype.
    - Development of SW/HW framework based on Xilinx development board.
    - Implementation of pSHIELD Node Layer blocks in VHDL and C language code.
    - Implementation of pSHIELD Node Adapter blocks: pSHIELD Interface and SPD Node Status.
    - Implementation of pSHIELD Node Adapter block: Security and Privacy based on hardware

data encryption/decryption.
    - Implementation of pSHIELD Node Adapter block: Dependability based reconfigurable application bit-stream.
    - Development and implementation of application: A-FSK Demodulator code.
    - Design and development of DAQ Adapter hardware board.

- Task 6.2 Multi-Technology Validation & Verification
  - ➢ Works with WP5 partners leading to development of common data interface for exchange of information with middleware layer.
- Task 6.3 Lifecycle SPD Support
  - ➢ Works not yet started due to delays in project
- Task 7.1 Dissemination
  - ➢ Exchange of informative materials on the project subject.
  - ➢ Preparation and presentation of pSHIELD project at Embedded World 2011 exhibition in Nuremberg (with MAS).
  - ➢ Results: Presentation of project at exhibition, making it recognized by governments and industry representatives.

A summary progress towards objectives.

During the second period of the project, SESM was involved in actions on several different management levels.

- SESM acts as Technical Project Coordinator. Due to lack of national agreement project consortium decided in October 2010 to move coordinator role to another partner. The change entered in force in December 2010. From that moment SESM took technical coordinator role of TCM.
- SESM acts as a WP3 leader, after decision of previous leader to withdraw, and acceptance of project consortium in October 2010.
- SESM also takes part in 8 tasks as a partner or leader.

During described period in SESM we took necessary steps to realise our project aims. After analysis of Annex I and relevance to Sub-Programme 6 Priority, Industry Priorities and Artemis Targets, we defined Nodes requirements following above goals. They are contributed to deliverable D2.1.1 chapter 8 "Node Requirements and Specifications".

Based on that we developed and proposed in D2.3.1 a pSHIELD generic node architecture. Proposed generic conceptual model of a pSHIELD node for all node types, can be implemented in different architectures, providing different functionalities, different SPD compliance levels and different services, depending on the type of node and application field. Three node types represent very different devices but they share the same conceptual model, enabling a seamless composability.

Then in April 2011 after Mid-term review new deliverables M0.1 and M0.2 were committed by consortium. Architecture and conceptual model of pSHIELD SPD Node Layer were updated accordingly to stay inline with ideas contained in new documents. Also works on implementation of pSHIELD SPD PowerNode were updated and in-lined with committed deliverables.

The first necessary step was to identify a development platform. Due to availability of the board in early stage of development Xilinx Virtex5 FPGA based board (XDB) was selected. Based on selected board development of SW/HW framework started. Step by step elements of pSHIELD Node Layer were implemented in VHDL and C language code. Following blocks of pSHIELD Node Adapter (D2.3.1) were implemented: pSHIELD Interface, SPD Node Status, Security and Privacy (based on hardware data encryption/decryption) and Dependability (based reconfigurable application bit-stream). As a use-case and application of prototype an A-FSK Demodulator was selected. Necessary works on implementation of A-FSK Demodulator are on-going. As a part of prototype DAQ Adapter hardware board was designed and developed.

Clearly significant and tangible results

- Development of extensive set of Node requirements that exactly follow goals of Annex I. Results contributed to deliverable D2.1.1 chapter 8 "Node Requirements and Specifications" with subchapters containing detailed references to Annex I.
- Design of generic conceptual model of a pSHIELD node for all node types, which can be implemented in different architectures, providing different functionalities, different SPD compliance levels and different services, depending on the type of node and application field. Three node types represent very different devices but they share the same conceptual model, enabling a seamless composability. Contributed to D2.3.1 (Node section) and to new deliverable M0.1.
- The first version of pSHIELD Power Node prototype was developed and presented during Consortium Meeting in Rome 12-13.07.2011.

Use of resources

The delay in the project had as a consequence that the deploy of resources has been postponed.

Dissemination activities and exploitation perspectives

- SESM (together with MAS) prepared informative materials on pSHIELD project and presented them at Embedded World 2011 exhibition in Nuremberg at ARTEMIS stand.

Corrective actions

- Close collaboration between partners was enforced after Mid-term review.
- The new deliverables requested by Project Officer were prepared in short time in close collaboration of all the consortium confirmed by commitment M0.3.
- Partners collaboration was intensified by means of frequent phone conferences at different levels of project and by means of on-line collaboration based on pSHIELD Wiki.
- The Consortium Meeting in Rome 12-13.07.2011 was organized to answer the main project question: how to proceed to succeed pSHIELD.

3.7.2. Ansaldo ASTS

Beneficiary7:	Ansaldo STS
Work Package(s)	WP1 - Project Management WP2 - Scenarios, user requirements and architecture design WP6 - Platform Integration, validation & demonstration WP7 - Dissemination
Task(s)	Task 1.1 Project management Task 2.2 Multi-technology SPD metrics Task 6.1 Multi-Technology System Integration Task 6.2 Multi-Technology Validation & Verification Task 6.4 Multi-Technology Demonstration Task 7.1 Dissemination
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 Project management: 1 PM Task 2.2 Multi-technology SPD metrics: 10 PM Task 6.1 Multi-Technology System Integration: 6 PM Task 6.2 Multi-Technology Validation & Verification: 9 PM Task 6.4 Multi-Technology Demonstration: 24 PM Task 7.1 Dissemination: 2 PM
Effort actual or spent in this period:	Task 1.1 Project management: 1 PM Task 2.2 Multi-technology SPD metrics: 9 PM Task 6.1 Multi-Technology System Integration: 4 PM Task 6.2 Multi-Technology Validation & Verification: 4,5 PM Task 6.4 Multi-Technology Demonstration: 12,25 PM Task 7.1 Dissemination: 2 PM
% 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 6.1 Multi-Technology System Integration: 60% Task 6.2 Multi-Technology Validation & Verification: 50% Task 6.4 Multi-Technology Demonstration: 50% Task 7.1 Dissemination: 100%

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

- Task 1.1
  - ➢ Coordination activities with the Technical Management Committee (TMC);
- Task 2.2
  - ➢ Revision and checking of D2.2.1 document;
  - ➢ Drafting of the sections in charge of ASTS within D2.2.1 document.
  - ➢ Results: support the identification of metrics required for the SPD measurements, also according to the proposed scenario considered in Task 6.4;
- Task 6.1
  - ➢ Preliminary analysis on the components of the architecture for the testbed, in order to address the

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

SPD concerns; • Task 6.2 ➢ Preliminary considerations on the integration of different components included in the prototype; • Task 6.4 ➢ Coordination activities with the partners to collect the inputs required to define the platform for the demonstrator, consisting in the monitoring of freight trains transporting hazardous material; ➢ Identification of the physical asset on which to assemble the testbed; ➢ Identification of HW resources in order to monitor car integrity and warn about possible leaking of hazardous material; • Task 7.1 ➢ The proposal of an advanced monitoring and surveillance system to protect freight trains transporting hazardous material was disseminated through the production of a scientific publication;
Description of criticalities met during the period: ➢
Corrective actions: ➢
Meetings performed during the period: ➢ Line up with the other reports
Deviations between actual and planned person-months: ➢ Due to the obtained project extension, some activities regarding WP2 and WP6 will be postponed. In particular the final check of the consistence of the outputs provided in the WP2 will be completed after reaching a more advanced status on WP6. Similarly, the further planned effort in the WP1, WP6 and WP7 will be spent later.
Dissemination activities and exploitation perspectives: ➢ Further dissemination activities regarding the results of project are planned. The research issues will be promoted through the participation in conferences and workshops on the topics of the project.

3.7.3. Elsag Datamat

Beneficiary[8]:	SELEX ELSAG (ex ELSAG DATAMAT)
Work Package(s)	WP1 - Project Management WP2 - SPD Metric, requirements and system design WP5 - SPD Middleware & Overlay WP6 - Platform integration, validation & demonstration WP7 - Knowledge exchange and industrial validation
Task(s)	Task 1.1 - Project Management Task 2.1 - Multi-technology requirements & specification

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

	Task 2.2 - Multi-technology SPD metrics Task 2.3 - Multi-technology architectural design Task 5.1 - SPD driven Semantics Task 5.2 - Core SPD services Task 5.3 - Policy-based management Task 5.4 - Overlay monitoring and reacting system by security agents Task 6.2 - Multi-technology Validation & Verification Task 7.2 – Exploitation
Period:	1st January 2011 – 30st June 2011
Effort planned for the period:	**WP1 – 3,0 PM** Task 1.1 – 3,0 PM **WP2 – 8 PM** Task 2.1 – 2,0 PM Task 2.2 – 2,0 PM Task 2.3 – 4,0 PM **WP5 – 26,5 PM** Task 5.1 – 7,0 PM Task 5.2 – 6,5 PM Task 5.3 – 6,5 PM Task 5.4 – 6,5 PM **WP6 – 8 PM** Task 6.2 – 8,0 PM **WP7 – 2 PM** Task 7.2 – 1,0 PM
Effort actual or spent in this period:	**WP1 – 2,4 PM** Task 1.1 – 2,4 PM **WP2 – 8,0 PM** Task 2.1 – 2,0 PM Task 2.2 – 2,0 PM Task 2.3 – 4,0 PM **WP5 – 24,10 PM** Task 5.1 – 7,5 PM Task 5.2 – 6,5 PM Task 5.3 – 4,6 PM Task 5.4 – 5,5 PM **WP6 – 5,0 PM** Task 6.2 – 5,0 PM **WP7 – 1,0 PM** Task 7.2 – 1,0 PM
% of work completed at the end of the period (indicative):	**WP1 – 80,0%** Task 1.1 – 80,0% **WP2 – 100,0%** Task 2.1 – 100,00% Task 2.2 – 100,00% Task 2.3 – 100,00%

	WP5 – 65,14% Task 5.1 – 75,00% Task 5.2 – 72,22% Task 5.3 – 51,11% Task 5.4 – 61,11% **WP6 – 38,46% PM** Task 6.2 – 38,46PM **WP7 – 50,0% PM** Task 7.2 – 50.00% PM

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

- **Task 1.1**
  - Technical management activities and support to the coordinator;
  - Project scheduling and achievements control;
  - Progress reports about involved resources and other expenditure;
  - Coordination of the leaded WPs and tasks technical activities;
  - Participation to physical meetings and phone conferences;
  - Organization of physical meetings and phone conferences.

Objectives: manage the project

- **Task 2.1**
  - Analysis of SPD requirements on Middleware and Overlay layers;
  - Analysis of standard methodologies on SPD requirements definition;
  - Contribution to the D2.1.1 "System Requirements and Specification" defining the requirements of Middleware and Overlay functionalities;
  - Contribution to the internal review of D2.1.1.

Objectives: defining the requirement of the pSHIELD framework driven by the use case
Results: inputs to the D2.1.1 deliverables and proposition of a standard methodology

- **Task 2.2**
  - Study of metrics for SPD multilayer approach and analysis of methodologies for metrics gathering;
  - Analysis of the state of the art of the existing metrics on SPD;
  - Analysis and study in depth of Common Criteria standard;
  - Analysys of SoA of existing composability approach;
  - Analysis and proposal of Quantitative Measurement of Metrics;
  - Contribution to the D2.2.1 "Preliminary SPD Metrics Specification".

Objectives: defining the SPD metrics of the pSHIELD framework
Results: inputs to the D2.2.1 deliverables and proposition of a conceptual model approach on metrics

- **Task 2.3**
  - Analysis of the SoA of Middleware architecture;
  - Proposition of a Service Oriented architecture to address the seamless approach and interoperability

requirements;

- Contribution to the D2.3.1 “Preliminary System Architecture Design”.

Objectives: defining the pSHIELD framework architecture
Results: inputs to the D2.3.1 deliverables on overall high level and middleware/overlay architecture

Progress towards objectives

WP5 (SELEXELSAG Leader) R&D activities are partitioned in four tasks, i.e., Task 5.1 SPD driven Semantics (TRS Leader), Task 5.2 Core SPD services (THYIA Leader), Task 5.3 Policy-based management (ESI ED Leader), and Task 5.4 Overlay monitoring and reacting system by security agents (ED Leader).

Here below the list of the deliverables for WP5 (delivery month definition):
Deliverables

- Public
  - D5.3 pSHIELD semantic models report (M18)
  - D5.4 SPD middleware and overlay functionalities report (M18)
- Internal
  - D5.1 pSHIELD semantic models (M15)
  - D5.2 SPD middleware and overlay functionalities prototype (M15)

Moreover WP5 Partners have participated to definition of Mid-term review additional deliverables:

- Internal
  - M0.1: Formalized conceptual models of the key pSHIELD concepts (M13)
  - M0.5: The pSHIELD focus areas, key innovations and project outputs (M13)

The partners contributing in WP5 are: SE (37PMs), UNIROMA1 (22PMs), CS (20PMs), ATHENA (4PMs), CWIN (7PMs), TECNALIA (1PMs), TRS (14PMs), and THYIA (11PMs).

Overall summary for WP5

- Targeted objectives for D5.1 are reached up to 75% (at the moment 100%)
- Targeted objectives for D5.2 are reached up to 75% (at the moment 100%)
- Targeted objectives for D5.3 are reached up to 30% (at the moment 50%)
- Targeted objectives for D5.4 are reached up to 30% (at the moment 50%)

Significant and tangible results

- Identification of pSHIELD semantic technologies;
- Semantic models to enable the pSHIELD seamless approach definition of main services at middleware layer;
- Prototypes of ontologies;
- Prototypes of semantic patterns of SPD composition;
- Experimental semantic engine for SPD composition;
- Analysis of the OSGI Knoplerfish platform as technological candidate for pSHIELD

• WP5 Middleware demonstrator; • Service Oriented technology selection to address the seamless approach and interoperability requirements; • High level design of the pSHIELD Middleware Architecture; • High level design of a secure service discovery for pSHIELD Middleware; • Analysis of semantic based access system and suggestion for semantically supported attribute-based access system • Analysis of the SoA in Policy-based management architectures and protocols; • Modelling of an Embedded System with Hybrid Automata; • design of the closed-loop control algorithms to enable the Composability functionality; • Formalisation of a static procedure to model the composability of Embedded Systems by means of Hybrid Automata; • Matlab-Simulink overlay models and simulations.
Corrective actions: ➢ No corrective actions are needed. The activities were carried out according to the technical annex with a specific effort indicated.
Meetings performed during the period: ➢ 14th January: WP2.3/WP4.1 meeting ➢ 13th May: WP4.1 meeting ➢ 1st June: phone call ➢ 16th June: phone call ➢ 24th June: phone call

3.7.4. Eurotech

Beneficiary[9]:	ETH
Work Package(s)	WP1 - SPD metric, requirements and system design WP3 – SPD node
Task(s)	Task 1.1 Project management Task 2.1 Multi-technology requirements & specification Task 2.2 Multi-technology SPD metrics Task 2.3 Multi-technology architectural design Task 3.2 Power node Task 6.4 Multi-Tecnology Demonstration
Period:	1st January 2011 – 30st June 2011

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

Effort planned in this period:	Task 1.1 Project management: 2MM Task 2.1 Multi-technology requirements & specification: 4MM Task 2.2 Multi-technology SPD metrics: 2MM Task 2.3 Multi-technology architectural design: 6MM Task 3.2 Power node: 42MM Task 6.4 Multi-Tecnology Demonstration: 4MM
Effort actual or spent in this period:	Task 1.1 Project management: 1,5MM Task 2.1 Multi-technology requirements & specification: 4MM Task 2.2 Multi-technology SPD metrics: 2MM Task 2.3 Multi-technology architectural design: 6MM Task 3.2 Power node: 33MM Task 6.4 Multi-Tecnology Demonstration: 2MM
% of work completed at the end of the period (indicative):	Task 1.1 Project management: 75% Task 2.1 Multi-technology requirements & specification: 100% Task 2.2 Multi-technology SPD metrics: 100% Task 2.3 Multi-technology architectural design: 100% Task 3.2 Power node: 78% Task 6.4 Multi-Tecnology Demonstration: 50%

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

- Task 1.1
  - ➢ Management activities required by the project: financial and technical planning, research activities control, reporting activities, review meeting preparation. Contribution to M0.6.
- Task 2.1
  - ➢ Identification of pSHIELD system requirements and specifications: contribution to the final version of D2.1.1.
- Task 2.2
  - ➢ Examination of the SPD metrics that can be used to evaluate the prototype.
  - ➢ Results: SPD metrics examination.
- Task 2.3
  - ➢ pShield system architecture definition and design.
  - ➢ Power Node architecture definition and design.
  - ➢ Results: contribution to D2.1.3, related to Power Node architecture. Contribution to M0.1.
- Task 3.2
  - ➢ Design of the Power Node, a mobile and rugged high performance embedded node with SPD intrinsic functionalities.
  - ➢ Power Node board design and development (2nd release).
  - ➢ Power Node rugged enclosure design and development.
  - ➢ Finalization of power node thermal studies.
  - ➢ Design and implementation of board firmware (2nd release).
  - ➢ Linux operating system porting.
  - ➢ Power Node support tools.
  - ➢ Results: test of the first release of the Power Node prototype completed. Bugs, corrections and improvements for the second/final version identified. Second release of the Power Node planned for the end of July. Thermal studies and rugged enclosure design completed. First prototype of Power Node cold-plate based cooling system. Porting of Linux operating system completed.

- Task 6.4
  - Use-case and scenario identification, demonstrator definition (in collaboration with SESM). Contribution to final pShield pilot definition and implementation.

Summary[10] of progress by beneficiary no. & name

A summary progress towards objectives

The Power Node represents an important element of pShield hardware infrastructure. The hardware infrastructure is the basement on which every other layer will rely. The infrastructure will be partially developed in pShield project and partially in nSHield project. The Power Node provides to pShield system an element with high computing power, and offers the possibility to customize its SPD functionalities with a high performance FPGA. The possibility to reconfigure the FPGA at run time represents a fundamental feature of the node in terms of SPD and it is the main topic of the final demonstrator in which the Power Node is involved. The first phase of Power Node design and development is completed: it consisted in the identification of requirements and specifications, definition of the node architecture, design, development and test of the first version of the prototype. The test activities allowed the identification of bugs and technical issues that, in turn, suggested improvements for the second version of the Power Node. The second phase, consisting in the design and development of the second version of the prototype, has started and will produce the second release of the Power Node at the end of July 2011. This version will be involved in the final pilot. The design and development of the cooling system and of the rugged enclosure is progressing: the first version of the prototype of the cold-plate based liquid cooling system is available. At software level, the Linux operating system porting has been completed and the library/development tools are available.

Highlight clearly significant and tangible results

The most important results achieved in the first reporting period are:

- test of the first release of the Power Node prototype complete.
- Bugs, corrections and improvements for the second/final version identified.
- Second release of the Power Node prototype available for the end of July 2011.
- Analysis of ruggedized enclosure completed.
- Analysis of the cooling concept in combination with a cold-plate based cooling system completed.
- First prototype of the cold-plate based cooling system available.
- Porting of Linux operating system.
- Power node development tools and library.

Deviations from Annex I and their impact on other tasks

Tasks in Workpackage 2 have been subjected to a delay that influenced the other activities. Workpackage 3 has been only partially influenced by this delay because the activities in this Workpackage are fully aligned with the company internal research plan and have been performed anyway.

[10] Summary means all actual beneficiary's WP s (the first table above) summarised together with the beneificiary explanations, remarks, conclusions, etc).

Use of resources

Resources have been used according to the activities plan, with some deviations in Task 3.2 due to the delay accumulated in Workpackage 2.

Dissemination activities and exploitation perspectives

Promotion within Eurotech Group and FinMeccanica Group: internal seminar and presentations, periodical reports to Eurotech Group technical board. Promotion with customers.

Corrective Actions

No corrective actions are needed. The activities will proceed with a rescheduling and will progress according to the technical annex.

3.7.5. Selex Communications

Beneficiary[11]:	SCOM
Work Package(s)	WP1 – Project Management (4MM) WP2 – Metrics, Requirements & System Design (1MM) WP4 – SPD Network (18MM) WP6 – Platform integration, validation & demonstration (1MM) WP7 – Knowledge exchange & industrial validation (1MM)
Task(s)	Task 1.1/2 Project Management/Liaisons Task 2.3 Multi Technology Architectural Design Task 4.1 Smart SPD driven transmission Task 6.1 Multi Technology System Integration Task 7.2 Exploitation
Period:	1st January 2010 – 30th June 2011
Effort planned in this period:	Task 1.1/2 Project Management/Liaisons - 1.5MM Task 2.3 Multi Technology Architectural Design – 0,3MM Task 4.1 Smart SPD driven transmission – 9.0MM Task 6.1 Multi Technology System Integration – 0.5MM Task 7.2 Exploitation – 0.0MM
Effort actual or spent in this period:	Task 1.1/2 Project Management/Liaisons – 1.5MM Task 2.3 Multi Technology Architectural Design – 0.3MM Task 4.1 Smart SPD driven transmission – 10.5MM Task 6.1 Multi Technology System Integration – 0.5MM Task 7.2 Exploitation – 0.0MM

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

% of work completed at the end of the period (indicative) [12]**:**	Task 1.1/2 Project Management/Liaisons – 87.5% Task 2.3 Multi Technology Architectural Design - 100 % Task4.1 Smart SPD driven transmission - 88% Task 6.1 Multi Technology System Integration – 50% Task 7.2 Exploitation – 0%

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

- Task 2.3
  - ➢ Study of the metrics for the SPD classification related to the architectural design

- Task 4.1
  - ➢ Study and motivation of the main features needed for making the pSHIELD SPD-Based Radio System working
  - ➢ Identification and study of the reconfigurable radio components with waveform parameters (frequency, bandwidth, …) allowing SPD transmissions
  - ➢ Identification and study of spectrum sensing features for Cognitive Radio analysis and the available/used resources
  - ➢ Study and implementation of SPD-based transmission techniques capable of guaranteeing a low probability of interception.
  - ➢ Adaptation of the sensing part of the Cognitive Radio simulator for pSHIELD
  - ➢ Realization and adaptation of a multi-core based embedded platform for the study and the validation of the cognitive algorithms on an embedded system.

Description of criticalities met during the period:

- ➢ Part of the study and validation of the cognitive algorithms is performed on a real embedded platform instead of using simulation.
- ➢ An embedded platform with multi-core processor and FPGA was realized and adapted, in terms of Hardware and Operative System, in order to be used in pSHIELD.

Corrective actions:

- ➢ No corrective actions are needed. The activities were carried out according to the technical annex with a specific effort for setting up a Cognitive Radio Node demonstrator, as previously specified.

Meetings performed during the period:

- ➢ 14th January: WP2.3/WP4.1 meeting
- ➢ 13th May: WP4.1 meeting
- ➢ 1st June: phone call
- ➢ 16th June: phone call
- ➢ 24th June: phone call

Deviations between actual and planned person-months:

- ➢ With respect to the proposed PM breakdown a little deviation is occurred. Actually we have spent 21.5PM. A few PM belonging to personnel not initially considered for participating in the project have been allocated to better manage and perform project activities. The total costs remain inside the declared amount. We plan a total of 27.5PM instead of 25 for the overall project duration.

[12] Z% = (PMs planned-PMs spent)/PMs planned x 100. This must correspond to Table 3.1

3.7.6. Tecnologie delle Reti e dei Sistemi

Beneficiary[13]:	TRS
Work Package(s)	WP1 - Project Management WP5 - SPD Middleware & Overlay
Task(s)	Task 1.1 - Project Management Task 5.1 - SPD driven Semantics
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 - Project Management – 0,25 PM Task 5.1 - SPD driven Semantics – 5,5 PM
Effort actual or spent in this period:	Task 1.1 - Project Management – 0,25 PM Task 5.1 - SPD driven Semantics – 5,5 PM
% of work completed at the end of the period (indicative):	Task 1.1 - Project Management – 75% Task 5.1 - SPD driven Semantics – 75%

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

- Task 1.1
  - Controlling project scheduling and achievements
  - Reporting of progress and resource expenditure
  - Coordination of technical activities inside the task

- Task 5.1
  - Analysis of semantic SPD composition patterns
  - Prototyping of ontology models
  - Prototyping of semantic – rule based inference for SPD composition

Additional Information:

N.A.

A summary progress towards objectives

The activities carried out in this time-frame are based on the outcomes from the previous period, mostly concerning:

[13] This report is per Beneficiary, and it provides as many as WPs in which it is involved each Beneficiary (see as PPR - Project Periodic Report, section 1.2.7.)

(1) The building of (ontological) models, compliant to the proposed formal methodology of ontology building.

(2) The conceptualization of semantic patterns of SPD composition

(3) The prototyping of inferential engines in order to support semantic SPD composition

Task (1) has been carried out by going through requirements, analysis and design workflows of the methodology, achieving incremental and iterative outcomes made up of a domain lexicon, a glossary, and ultimately a semantically annotated model of Embedde Systems concepts and relations among them (ontology)

In Task (2), the SPD functionalities are modeled according to the pSHIELD proposal for SPD metric aggregations. In this task, we undertake a novel approach in which composition is modeled after analogous Composite Processes in OWL for services (OWL-S). We draw analogies between the models, and propose a concept of Connector that provides a specification of the structure of the composition, by means of basic "control constructs" (whose names are reminiscent of control structures in programming languages).

Moreover, we introduce an analytical specification of the algorithm that composes the SPD status values of contributing SPD functionalities into the overall SPD status value

Outcomes of Tasks (1) and (2) enable Task (3) , in which we exploit semantic (inferential) engines, enabled by SPD ontologies, to carry out a number of basic functionalities supporting composability based on SPD metric in the pSHIELD framework. In this novel approach to the determination of semantic enabled SPD composition, an automatic reasoner can infer the overall level of SPD metrics resting upon model axioms and declarative rules. In this Task we test an experimental implementation in order to support synthesis actions: at run time (online), changes in the state of the system trigger the semantic engine to devise new compositions, based on knowledge of modules that at the moment are active in the system (possibly discovered at run time), in order to guarantee the prearranged overall SPD level.

Clearly significant and tangible results

Tangible outcomes, provided as contributions to deliverable D5.1, include:

- Prototypes of ontologies
- Prototypes of semantic patterns of SPD composition
- Experimental semantic engine for SPD composition

Reasons for deviations from Annex I and their impact on other tasks as well as on available resources and planning

N.A.

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

TRS's contribution is reasonably in line with respect to the new project schedule, taking into account the approved extension to the project.

We identify as a critical situation any delay in the definition of the technologies involved in the testbed, since the actual instance models and inference rules must be tailored depending on a concrete demonstration scenario.

Use of resources The redevelopment of the schedule of activities has necessarily considered an effective distribution of residual budget to fit the extension needed by the overall project.
Dissemination activities and exploitation perspectives Advancements in semantic technologies expected in pSHIELD project have already been introduced during the "Workshop on Semantic Technologies applied to Requirements Management" held in SELEX SI in july 2010. A proposal submission for a paper is expected for the 4th Interop Vlab Workshop – October 6-7th – Rome (Italy) Application and further development of such technologies are planned in a number of oncoming research projects in TRS.
Corrective actions N.A.

3.7.7. Università degli Studi di Genova

Beneficiary[14]:	UNIGE
Work Package(s)	WP4 – SPD Network
Task(s)	Task 4.1 Smart SPD driven transmission Task 4.2 Trusted and dependable Connectivity
Period:	1st Jan 2011 – 30th June 2011
Effort planned in this period:	Task 4.1 Smart SPD driven transmission – PM 2 (Effectively needed 4) Task 4.2 Trusted and dependable Connectivity – PM 1 (Effectively needed 3)
Effort actual or spent in this period:	Task 4.1 Smart SPD driven transmission – PM 4 Task 4.2 Trusted and dependable Connectivity – PM 3

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

% of work completed at the end of the period (indicative):	Task4.1 Smart SPD driven transmission - 95% Task 4.2 Trusted and dependable Connectivity – 95%

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

- Task 4.1
  - ➢ Identification of spectrum sensing features for Cognitive Radio analysis
  - ➢ Adaptation of sensing part of the Cognitive Radio simulator for pSHIELD
- Task 4.2
  - ➢ Transmission parameters smart adaptation according to radio resources observation towards trusted and dependable connectivity implementation
  - ➢ Implementation of a Cognitive Radio Node software simulator that is able to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly

According to T4.1 and T4.2 objectives UNIGE has proposed new technologies enabling smart SPD driven transmissions. In particular, the cognitive radio (CR) paradigm, which is usually based on Software Defined Radio (SDR), has been proposed to deal with such transmissions. CR is composable and expandable and modular by definition. In fact, it has been designed to accommodate these features.
The implemented Cognitive Radio Node is able to receive radio parameters from moving hosts and automatically detect possible threats. The internal architecture of the Node learns typical safe environments features thus detecting the presence of external attackers by analysing radio parameters.
In a considered scenario, the cognitive node always updates the radio parameters (SNR, BER and Transmitter Power, PTX) for the self-awareness purposes. There are some specific provisions considered to design this kind of simulator used for the Security, Privacy and Dependability (SPD) in the context of integrated and interoperating heterogeneous applications.

When an agent enters the scene, the cognitive node becomes aware of the radio parameters of the agent either by using the spectrum sensing technique or from a direct communication from the agent itself. In this way the node can update its radio information for using the radio resources efficiently and securely. The cognitive node has an internal knowledge of all the radio parameters which would be considered in the selected environment and their respective variation models. The node knows itself from a configuration database what frequencies are used by which agent and which frequencies are free to use. If a new agent enters in the scene while continuing communication, the cognitive node sense the radio parameters of the agent and is able to modify and adapt agents radio parameters when necessary.

In the presence of a jammer of specific frequency in a cluster, the cognitive node sends a message to the agents to adjust the radio parameters properly, i.e., by changing either the frequency or the transmission power (spread spectrum or noise based data transmission of signals).

Moving agents in the scene and the presence of jammers are dynamically created through a specific simulator that was built to this aim. The simulator sends to the cognitive node is the positioning data, namely the trajectories of the agents (like a tracker) and radio data on the situation. More specifically, each agent is controlled by the cognitive mobile node, considered as an entity, after the registration process in the area under observation, periodically sends information on the quality of communication.

Description of criticalities met during the period:

- As previously explicitly asked by the WP leader, main efforts of the research unit during this last part of the pSHIELD project were devoted to the implementation of a real Cognitive Radio Node.
- Some inputs from the WP leader have been considered as typical measured quantities from Cognitive Node sensing subsystems.

Corrective actions:

- No corrective actions are needed. The activities were carried out according to the technical annex with a specific effort for setting up a Cognitive Radio Node demonstrator, as previously specified.

Meetings performed during the period:

- 1st June: phone call
- 16th June: phone call
- 24th June: phone call

Deviations between actual and planned person-months:

- With respect to the proposed PM breakdown a little deviation is occurred. Actually we have spent 7 PM. A few PM belonging to personnel not initially considered for participating in the project have been allocated to better manage and perform project activities. However we have kept the total declared costs at the same amount involving more staff with a lower income and avoiding the contribution of staff with an higher income according to the need of more effort to better address project needs and to cope with issues deriving from delays in the overall project development. We plan a total of 16 PM instead of 12 for the overall project duration.

Dissemination activities and exploitation perspectives:

- In order to disseminate the results achieved during project-related activities, the research unit has participated to international conferences and forums where part of the work performed in pSHIELD has been discussed.
- pSHIELD related publications:
    - L. Bixio, M. Ottonello, M. Raffetto, and C.S. Regazzoni, "Comparison among Cognitive Radio Architectures for Spectrum Sensing," EURASIP Journal on Wireless Communications and Networking, vol. 2011, Article ID 749891, 18 pages, 2011. doi:10.1155/2011/749891
    - L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C. S. Regazzoni, Sk. S. Alam and C. Armani, "A Transmit Beamforming Technique for MIMO Cognitive Radios,", Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, SDR'11 - WInnComm - Europe, Brussels, Belgium, June 22-24, 201
    - S. S. Alam, L. Marcenaro and C. Regazzoni, "Opportunistic Spectrum Sensing and Transmissions", submitted for publication

3.7.8. Università degli Studi di Roma "La Sapienza"

Beneficiary[15]:	UNIROMA1
Work Package(s)	WP1 - Project management
Task(s)	Task 1.1 - Project management

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

Period:	1st January 2011 – 30th June 2011
Effort planned for the whole project:	**WP1 – 2,0 PM** Task 1.1 – 2,0 PM
Effort actual or spent in this period:	**WP1 – 1,2 PM** Task 1.1 – 1,2 PM
% of work completed at the end of the period (indicative):	**WP1 – 75,0%** Task 1.1 – 75,0%

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

- **T1.1:**
  - Support to the technical manager and the technical coordinator in the organization of meetings and in the collection of documents, especially for WP5 related issues.

Objectives: manage the project

Description of criticalities met during the period:

- In order to ease the project management, it should be better identified the responsibility of each coordinator (technical and administrative).

Corrective actions:

- Correct the TA section about management.

Meetings performed during the period:

- 20th January, SESM: Consortium Phone Call
- 8th Februay SESM: Consortium Phone Call
- 21st March, THYIA: pre-meeting for mid-term review preparation – ALL
- 22nd March, THYIA: mid-term review meeting - ALL
- 1st June, SESM: Consortium Phone Call – ALL

Deviations between actual and planned person-months:

--

Dissemination activities and exploitation perspectives:

--

Beneficiary[16]:	UNIROMA1
Work Package(s)	WP5 - SPD Middleware & Overlay
Task(s)	Task 5.1 - SPD driven Semantics Task 5.2 - Core SPD services Task 5.4 - Overlay monitoring and reacting system by security agents
Period:	1st January 2011 – 30th June 2011
Effort planned for the whole project:	**WP5 – 22,0 PM** Task 5.1 – 5,0 PM Task 5.2 – 9,0 PM

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

	Task 5.4 – 8,0 PM
Effort actual or spent in this period:	**WP5 – 11,6 PM** Task 5.1 – 1,6 PM Task 5.2 – 7,3 PM Task 5.4 – 2,7 PM
% of work completed at the end of the period (indicative):	**WP5 –101,0%** Task 5.1 – 104,0% Task 5.2 – 106,0% Task 5.4 – 95,0%

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

- **T5.1 - SPD driven Semantics**
  - Enrichment of the preliminary pSHIELD Ontology with the translation of the “metrics quantification” and “medieval castle” concepts introduced in WP2, in order to improve the SPD composability power of the metamodel.
  - The final prototype of OWL ontology to model the pSHIELD system, as well as SPD functionalities has been developed with the Protegè tool and documented.
  - Some additional work has been performed in the scope of WP2 to contribute and review the D2.x deliverables with respect to the sections that have direct impact on WP5.
  - A great effort has been put to provide inputs to document M0.1 with respect to Semantic technologies issues

Objectives: provide semantic models to enable the pSHIELD seamless approach

Tangible Results: consistent inputs to deliverable 5.1 (including OWL prototypes). Deliverable M0.1

- **T5.2 - Core SPD services**
  - Consolidation of the high level design of the pSHIELD Middleware Architecture.
  - Mapping and implementation of the pSHIELD Middleware core services into the OSGI Knoplerfish platform that will be delivered as part of WP5 prototypes.
  - Some additional work has been performed in the scope of WP2 to contribute and review the D2.x deliverables with respect to the sections that have direct impact on WP5
  - A great effort has been put to provide inputs to document M0.1 with respect to Core SPD Services and middleware architecture

Objectives: define the basic services at middleware layer in the multilayered approach; provide the Overlay with the (secure) discovery functionality

Tangible Results: consistent inputs to deliverable 5.2 (including preliminary OSGI prototype). Deliverable M0.1

- **T5.4 - Overlay monitoring and reacting system by security agents**
  - Refinement of the model of an Embedded System with Hybrid Automata.
  - Introduction of the model of a network of Embedded Systems with Hybrid Automata
  - Consolidation of the procedure to model the composability of Embedded Systems by means of Hybrid Automata.

- Further simulations of the Overlay behaviour in a very simple scenario by means of Matlab-Simulink tool, in order to demonstrate the composability.
- Preliminary studies on Model Predictive Control as potential control algorithm for composability
- Analysis of inferential engine and rules (like Jena) as control algorithm to drive SPD aware composability (in conjunction with Task 5.1)
- Additional work has been performed in the scope of WP2 to contribute and review the D2.x deliverables with respect to the sections that have direct impact on WP5
- A great effort has been put to provide inputs to document M0.1 with respect to composability issues and overlay architecture
-

Objectives: design and develop the Overlay; design the closed-loop control algorithms to enable the Composability functionality

Tangible Results: some inputs to deliverable 5.2 (including preliminary Matlab-Simulink models and simulations). Deliverable M0.1

Description of criticalities met during the period:

--

Corrective actions:

--

Meetings performed during the period:

- 21st January, ElsagDatamat: meeting with TRS and ED
- 15th Februay THYIA: Project Assembly Phone Call
- 25th February, ElsagDatamat: phone call WP5 – ALL
- 9th March, ElsagDatamat: phone call for mid-term review preparation – ALL
- 16th March, SESM: phone call for mid-term review preparation – ALL
- 29th March, SESM: Technical Phone Call – ALL
- 1st April, SESM: Technical Phone Call – ALL
- 5st April, CWIN: Technical Phone Call – ALL
- 12st April, ED: Technical Phone Call – ALL
- 11th May, SESM: WP5 Meeting – WP5 Core Team
- 24th June, SESM: Consortium Phone Call – ALL

Deviations between actual and planned person-months:

- None

Dissemination activities and exploitation perspectives:

- The pSHIELD concepts have been subject of Master Thesis: - Francesco Lavorato, “Study and development of a semantic framework to model and control security, privacy and dependability in Emebedded Systems”, May 2011.
- Some achievements in semantic technologies development have been presented in the paper accepted in the SafeComp 2011 (The 30th International Conference on Computer Safety, Reliability and Security Naples, Italy): "On the use of semantic technologies to model and control Security, Privacy and Dependability in complex systems". (Authors - Andrea Fiaschetti, Francesco Lavorato, Vincenzo Suraci, Andi Palo, Andrea Taglialatela, Andrea Morgagni, Renato Baldelli, Francesco

Flammini)

3.8 Spain

3.8.1 Acorde Seguridad

Beneficiary[17]:	AS
Work Package(s)	WP1 - Project Management
Task(s)	Task 1.1 Project management
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 Project management 0.5 PM
Effort actual or spent in this period:	Task 1.1 Project management 0.5 PM
% of work completed at the end of the period (indicative):	Task 1.1 Project management 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP: • Task 1.1 ➢ General administrative project issues ➢ Coordination of Spanish team	

Beneficiary[18]:	AS
Work Package(s)	WP3 - SPD Node
Task(s)	Task 3.1 Nano, Micro/Personal node Task 3.2 Power Node Task 3.3 Dependable self-x and cryptographic technologies
Period:	1st January 2011 – 30th June 2011

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

Effort planned in this period:	Task 3.1 Nano, Micro/Personal node 3.5 PM Task 3.2 Power Node 3 PM Task 3.3 Dependable self-x and cryptographic technologies 0.5 PM
Effort actual or spent in this period:	Task 3.1 Nano, Micro/Personal node 4 PM Task 3.2 Power Node 3.5 PM Task 3.3 Dependable self-x and cryptographic technologies 1 PM
% of work completed at the end of the period (indicative):	Task 3.1 Nano, Micro/Personal node 114% Task 3.2 Power Node 116% Task 3.3 Dependable self-x and cryptographic technologies 200%

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

- Task 3.1 and Task 3.2
  - ➢ Studies of the SotA solutions in the field of “Energy Storage Systems” to guarantee the correct system operation. Some commercial solutions have been included in order to identify the ones with a good value for money.
  - ➢ Studies of the SotA solutions in the field of “Power Harvesting Methods” to improve the autonomy of the power supply.
  - ➢ Design of circuit protection devices to prevent damages originated in the power system. The design includes protections from equipment overload, short-circuits and overvoltage conditions (Transient voltage spikes).

The studies are made taking into account the power consumption of commercial solutions that can be considered as nano, micro, personal and power nodes.

Description of criticalities met during the period:

- ➢ The delay in the first months of the project has influenced the schedule in the period covered by this report. An extra effort was needed to prepare the Mid-Term review and to solve the open points within a short period of time.

Corrective actions:

- ➢ The approved extension of the project will allow finalizing all the intended work with success. No further corrective actions are required.

Meetings performed during the period:

- ➢ PhC: 20th January
- ➢ PhC: 8th February
- ➢ PhC: 15th February
- ➢ PhC: 25th February
- ➢ PhC: 16th March
- ➢ PhC: 28th March
- ➢ PhC: 29th March
- ➢ PhC: 1st April
- ➢ PhC: 12th April
- ➢ PhC: 18th April
- ➢ PhC: 24th May

- PhC: 1st June - PhC: 24th June - PhC: 18th July
Deviations between actual and planned person-months: - ACORDE has spent slightly more PM that initially planned. This is mainly due to the realignment of objectives for different tasks in order to increase the added value of the research performed. - At the same time, ACORDE has not spend the initially planned amount for consumables, without prejudice of the execution of the technical tasks. Thus, the deviation in PM will not economically influence the budget.
Dissemination activities and exploitation perspectives: - Many of today's ES, such as wireless and portable devices rely heavily on the limited power supply. ACORDE, as company specialized in the development of RF equipment, satellite communications systems, monitoring and control integrated systems, and location & positioning systems, is really interested in increasing its knowledge in power supply design, due to is the base to design autonomous wireless systems which can compete in market.

3.8.2 European Software Institute/Tecnalia

Beneficiary[19]:	Tecnalia
Work Package(s)	WP2[20] - SPD Metrics, Requirements and System Design WP4 – SPD Network WP7 - Knowledge exchange and industrial validation
Task(s)	Task 2.2 Multi Technology specification and metrics Task 2.3 Multi technology architectural design Task 4.2 Trusted and dependable Connectivity Task 7.1 Dissemination
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 2.2 Multi Technology specification and metrics 2 PM Task 2.3 Multi technology architectural design 0,3 PM Task 4.2 Trusted and dependable Connectivity 0,1 PM Task 7.1 Dissemination 0,2 PM
Effort actual or spent in this period:	Task 2.2 Multi Technology specification and metrics 2 PM Task 2.3 Multi technology architectural design 0,3 PM Task 4.2 Trusted and dependable Connectivity 0,1 PM Task 7.1 Dissemination 0,2 PM

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

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

% of work completed at the end of the period (indicative):	Task 2.2 Multi Technology specification and metrics 70% Task 2.3 Multi technology architectural design 90% Task 4.2 Trusted and dependable Connectivity 90% Task 7.1 Dissemination 80%

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

- Task 2.2
  - Definition of SPD metrics in a quantitative way
  - Managing SPD metrics contributions from each partner
  - Refinement of SPM preliminary metrics for pSHIELD project
  - Development of SPD metrics paper for EUROMED conference (accepted) (this is also a task of dissemination)
- Task 2.3
  - Contribution for SPD multi technology architectural design taking into account the SPD metrics
- Task 4.2
  - Contribution for trusted and dependable connectivity
- Task 7.1
  - A paper was presented and accepted by Tecnalia and Ansaldo

Description of criticalities met during the period:

- Due to recommendations of last review SPD preliminary focus has changed in order to show more quantitative methods. This made an impact in WP6 (platform development) making that some platform requirements had changed.
  - Results have been achieved in this sense: a quantitative method has been defined and implemented within this task
  - This task should be refined for last deliverable: final SPD metrics

Corrective actions:

- The project extension could be enough to finalize the task of SPD metrics because once the method is chosen it is easy to move forward, implement it and deploy it to the system

Meetings performed during the period:

- 24th June: phone call (Task 2.2)
- 21st June: phone call (Task 2.2)
- 31st June: phone call (Task 2.2)
- 29th April: phone call (Task 2.2)
- 2nd March: phone call (Task 2.2)
- 4th February: phone call (Task 2.2)
- Periodic meeting as well for the rest of the tasks

Deviations between actual and planned person-months:

- No major deviations need to be mentioned. The resources have been redistributed according the schedule in the appendix

Dissemination activities and exploitation perspectives:

- SPD metrics in critical infrastructure for EUROMED conference (paper accepted).

3.8.3 Mondragon Goi Eskola Politecnikoa

Beneficiary[21]:	MGEP – Mondragon Goi Eskola Politeknikoa
Work Package(s)	WP1[22] - Project Management WP4 – SPD Network WP7 - Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project management Task 4.2 Trusted and dependable Connectivity Task 7.1Dissemination
Period:	1st Jan 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 Project management – PM: 0.13 Task 4.2 Trusted and dependable Connectivity – PM 2 Task 7.1Dissemination - PM: 0.25
Effort actual or spent in this period:	Task 1.1 Project management – PM:0.13 Task 4.2 Trusted and dependable Connectivity – PM 3 Task 7.1 Dissemination - PM: 0.4
% of work completed at the end of the period (indicative):	Task 1.1 Project management – 60%[23] Task 4.2 Trusted and dependable Connectivity – 90% Task 7.1 Dissemination - 90 %

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

- Task 1.1
  - Project management: Reporting of progress and resource expenditure, production of deliverables.
- Task 4.2
  - Study of the different IDS approaches (misuse vs anomaly detection, and architecture) taking into account the requirements of sensor networks.
  - Study the real resource footprint of wireless communication protocols (energy consumption among them) and its impact on performance on some commercially available devices.
  - Study of anomaly detection systems.
- Task 7.1
  - Three papers were presented by the research group.

The main activity of MGEP in pSHIELD is on the study of the requirements for lightweight link-layer secure communication in wireless sensor network scenarios and the design and development of proper schemes focusing on confidentiality. More specifically, intrusion detection systems (IDS) have been studied.

Misuse detection based IDS monitors the activities of a system and compares them with signatures of attacks that are stored in a database. This kind of IDS have high accuracy rates, however, due to the high

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

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

[23] Z% = PMs spent/PMs planned x 100. This must correspond to Table 3.1

increase of new attacks and the continuous variants of them it is extremely difficult to have an updated set of rules. On the other hand, anomaly detection depends greatly on the supposition that users and networks behave in a sufficiently regular way and therefore, any significant deviation from such behaviour could be considered as an evidence of an intrusion. Hybrid IDS, where the system is based in anomaly and misuse techniques best fit in WSN. However, there are application areas, such as SCADA systems, where anomaly detection performs better than in traditional information and communications technology (ICT) networks. SCADA communications are deterministic, and their operation model is often cyclical. Based on this premise, modelling normal behaviour by mining specific features sets gets feasible and efficient.

Another important issue is the architecture deployed for the IDS. Attacks can be detected locally in nodes, centralized in a main processing node or even through the collaboration of global and local agents integrated in the application layer of nodes. Although it may result in an increase in the resource requirements of a sensor node, the global security level that gives distributed intrusion detection is considered more reliable than the centralized one.

The centralized architecture could not detect as many attacks, due to the low data rate of wireless communication and energy constraints of sensor nodes that could not afford the transmission of massive audit data to a base station. However, in a distributed intrusion detection system, no node is trustful, due to potential inside attackers. For that reason is necessary to propose an agent able to detect anomalies in its host neighbours. The protection of the nodes is also necessary so it is high recommended to implement a local agent for the nodes able to analyse possible local feature changes.

Other activities of T4.2are concerned to the design of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks, aiming to reduce the vulnerability to attacks depleting communication resources and node energy.

As Confidentiality, Data Integrity and Service Availability are also addressed by security systems in wired networks Energy is unique to the wireless sensor networks due to the resource limitation constraint. Regarding energy there is a necessity to asses the existing protocols and applications in different real situations as they are initially designed and studied in a simulation environment. We have studied the resource footprint (energy consumption among them) and its impact on performance on some commercially available devices. We could see both how different aspects of the communications protocol contributes to the footprint and how this in turn affects the performance. The methodologies used can be applied to other protocols and applications, aiding in future optimisations. Vulnerabilities in the communications protocol could lead to greater energy consumption and eventually to a DoS attack.

Description of criticalities met during the period:

- The main efforts of the research group during this last part of the pSHIELD project were devoted to the study of the different IDS approaches and architectures to propose the most suitable for WSN.
- A study of the real resource footprint of wireless communication protocols and its impact on performance on some commercially available devices has also been carried out.

Corrective actions:

- No corrective actions are needed. The activities were carried out according to the technical annex.

Meetings performed during the period:

➢ Periodic phone calls
Deviations between actual and planned person-months: ➢ No major deviations need to be mentioned. The resources have been redistributed according the schedule in the appendix. Most of dissemination work has been carried out in this period expending more resources than planned but little contributions are expected for the remaining time.
Dissemination activities and exploitation perspectives: ➢ The security group of MGEP has participated in international conferences and forums where results relevant to pSHIELD were presented. ➢ pSHIELD related publications: o Iñaki Garitano, Roberto Uribeetxeberria and Urko Zurutuza, "Review of SCADA Anomaly Detection Systems", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447 o Urko Zurutuza , Enaitz Ezpeleta, Álvaro Herrero and Emilio Corchado "Visualization of Misuse-based Intrusion Detection: Application to Honeynet Data", Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Salamanca (Spain) in April, 2011, ISBN 9783642196447 o Ekhiotz Jon Vergara, Simin Nadjm-Tehrani, Mikael Asplund and Urko Zurutuza, "Resource Footprint of a Manycast Protocol Implementation on Multiple Mobile Platforms", Fifth International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST 2011, Cardiff, Wales, UK, 14-16 September 2011.

3.9 Greece

3.9.1 ATHENA

Beneficiary[24]:	ATHENA
Work Package(s)	WP2 - SPD metrics, requirements and system design WP3 - SPD Node WP4 - SPD Network
Task(s)	Task 2.1 - Multi-technology requirements & specification Task 2.3 – Multi-technology architectural design Task 3.3 - Dependable self-x and cryptographic technologies Task 4.2 - Trusted and dependable connectivity
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 2.1 - Multi-technology requirements & specification – 1 PM Task 2.3 – Multi-technology architectural design - 2 PM Task 3.3 - Dependable self-x & cryptographic techn. – 2 PM Task 4.2 - Trusted and dependable connectivity – 0,5 PM

[24] This report is per Beneficiary, and it provides as many as WPs in which it is involved each Beneficiary (see as PPR - Project Periodic Report, section 1.2.7.)

Effort actual or spent in this period:	Task 2.1 - Multi-technology requirements & specification – 0 PM Task 2.3 – Multi-technology architectural design - 0 PM Task 3.3 - Dependable self-x & cryptographic techn. – 0 PM Task 4.2 - Trusted and dependable connectivity – 0 PM
% of work completed at the end of the period (indicative):	Task 2.1 - Multi-technology requirements & specification – 0% Task 2.3 –Multi-technology architectural design - 0% Task 3.3 - Dependable self-x & cryptographic techn. – 0% Task 4.2 - Trusted and dependable connectivity – 0%

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

- Task 2.1
  - ➢ Identification of the requirements of the application scenarios
  - ➢ Description of the specifications of the overall system

- Task 2.3
  - ➢ Analysis of the fundamental concepts of Security, Privacy
  - ➢ Analysis of the fundamental concepts of Dependability
  - ➢ Analysis of security aspects in embedded systems

- Task 3.3
  - ➢ Working on novel cryptographic key exchange algorithm (Controlled Randomness)
    - Less frequent key exchanges
    - Lower control channel utilization
    - Higher security vs. Cryptanalysis
    - Multiple valid keys per time frame
    - Low (to zero) processing overhead
- Task 4.2
  - ➢ Assessment of a number of defence mechanisms against DDoS attacks
    - Ingress/Egress filtering, Packet Marking/Logging, Self reconfiguration and sustainability, Deep packet inspection
    - Integration of the mechanisms inside the SPD network architecture
    - Evaluation and redesign of the mechanisms with regard to the node classes defined in wp3

Additional Information:-

A summary progress towards objectives

➢ WP2

- ➢ Analysis of the fundamental concepts of Security, Privacy:
  - Principles : Confidentiality, Integrity, Availability
  - Mechanisms : Authentication, Authorisation, Intrusion detection/prevention, Policies
  - Domains : System, Network, Operations, Physical
- ➢ Analysis of the fundamental concepts of Dependability:
  - Threats : Faults, Errors, Failures
  - Attributes : Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability
  - Means : Fault Prevention, Tolerance, Removal
- ➢ Analysis of security aspects in embedded systems

- System Design
- Application design and implementation
- Physical Security and side channel attacks

- WP3
  - Adoption of proven methodologies against distributed denial of service attacks and their applicability on a resource limited environment such as the one of SPD embedded systems. Deployment, adaptation and measurement of the performance of packet marking and deep packet inspection methodologies that enable a node to mitigate an ongoing DDoS attack through reconfiguration of the node operation characteristics as well as the network ones. This subtask will be implemented in close cooperation with WP4 (Network layer) since most of these methodologies affect the node as well as its connectivity with the backbone network or the neighbouring nodes, depending on the deployment strategy.
  - Deploying and measuring the efficiency both in terms of performance and security of different cryptographic frameworks that offer PKI capabilities as well as symmetric cryptographic operations. Implementation and deployment of a new cryptographic key exchange algorithm called “Controlled Randomness” that limits the need of frequent key exchange between the communicating parties, thus boosting the robustness of the underlying cryptographic operations against cryptanalysis, while keeping the performance cost in acceptable, and in some cases favourable, levels.

3.9.2 Hellenic Aerospace Industry

Beneficiary[25]:	HAI
Work Package(s)	WP2 - SPD Metrics, Requirements and System Design
Task(s)	Task 2.3 - Multi-Technology Architectural Design
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 2.3 - Multi-Technology Architectural Design, 3 PM
Effort actual or spent in this period:	Task 2.3 - Multi-Technology Architectural Design, 3 PM

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

% of work completed at the end of the period (indicative):	Task 2.3 - Multi-Technology Architectural Design, 89% PM[2] (8/9)

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

- Task 2.3
  - ➢ The objective of finalizing a preliminary multi-technology Architecture description has encompassed the following activities:
    - ✓ HAI contributed in the mid-term review follow up document M0.5, about pSHIELD focus areas and especially on validating pSHIELD
    - ✓ Based on the recommendations from the first project review, specifically stated for D2.3.1, the team worked on highlighting and augmenting the positive remarks and eliminating the negative ones
    - ✓ Two dedicated to T2.3 phone conferences and 4 document updates (preceded by corresponding rounds of contributions from partners) were conducted
    - ✓ In the process of defining a formalized architecture, the concepts and modules indicated in M0.1, and agreed by all partners, were specially taken into consideration
    - ✓ SPD considerations, fundamental embedded systems concepts and applications were pinpointed
    - ✓ The 4 pSHIELD layers were analysed further in terms of theoretical definitions and pSHIELD hardware and software components and functions/services
    - ✓ The model of the conceptual pSHIELD functional architecture was indicated
  - ➢ Results:
    - ✓ Key pSHIELD concepts have been formalized
    - ✓ The link with WP2 activities and outcomes is being processed (Requirements and Metrics)
    - ✓ The link with WP3-5 activities and outcomes is being processed (4 pSHIELD layers)
    - ✓ A reference Architecture is formalized
    - ✓ Architectural Components have been described by partners, according to their technical competences and involvement in the project
    - ✓ Internal D2.3.1 is close to finalization

Description of criticalities met during the period:

- ➢ D2.3.1has strong interdependencies with requirement and metric analysis and technical work conducted in other WPs. Some missing inputs from the latter, as well as partner's focus on composing the 6 mid-term review follow up documents, have been delayed the finalization of D2.3.1

Corrective actions:

- ➢ The corrective directions suggested in the mid-term review are being processed by involved partners and D2.3.1 is expected to be finalized and delivered prior to September's review meeting

Meetings performed during the period:

- ➢ 14th January: phone conference (second in T2.3)
- ➢ 15th June: phone conference (third in T2.3)
- ➢ T2.3 was a point in agenda in numerous plenary phone conferences

Deviations between actual and planned person-months:

- …

Dissemination activities and exploitation perspectives:

- No dissemination activities were conducted during the reference period, but as stated in the Technical Annex, HAI anticipates in pSHIELD activities and findings (architecture, demonstration and prototypes) to enhance its knowledge and competence in embedded systems as parts of security solutions

3.9.3 Integrated Systems Development

ISD withdrawn from the project. It was announced by them during Project Assembly phone conference on 15 February 2011. No report of activities and costs will be delivered.

3.10 Norway

Summary of progress by CWIN and Movation (MAS)

pSHIELD objective stated:
The project's main objective is to conceive and design a preliminary, innovative, modular, composable, expandable and high-dependable architectural framework which allows to achieve the desired SPD level in the context of integrated and interoperating heterogeneous services, applications, systems and devices; and to develop concrete solutions capable of achieving this objective in specific application scenarios with minimum engineering effort.

For the pilot one of the previous four scenarios, but reduced in scope, has been carefully selected in industrial exploitation perspective, in order to cover a minimum significant view of the foreseen industrial needs, the monitoring of a railway.

From the Norwegian point of view, pSHIELD concentrates on the secure interworking between heterogeneous systems. This interworking is achieved by inviting relevant partners such as the Norwegian Rail Administration (JBV) and Telenor Objects as associated partners to pSHIELD.

The work has provided the following aspects towards the objectives:

- innovative, modular, expandable architecture framework – the basis of such an architecture is the interoperable ETSI TS102.690 M2M platform. The aspects of modular and expandable are part of the TS102.690. Innovative aspects are the semantic description for secure interworking. However, this platform needs to be extended in order to satisfy the needs for dependability and security. The foreseen extensions will be identified during the remaining part of pSHIELD
- integrated and interoperating heterogeneous services, applications, systems and devices – Semantic technologies have been identified as tools for interworking and interoperability. The main achievements are the description of components through ontologies, e.g. a sensor ontology describing the SPD sensors. A Semantic MediaWiki has been implemented in our associate partner JBV as well as CWIN in order to allow interoperability between applications and services. We established .rdf export and import for exchange of these service related aspects.

Integration from sensors into this application framework have been achieved through an integration into the Telenor Objects platform, and from there further towards the applications platforms at CWIN and JBV. The path for Integration is established, and the integration of sensor to Telenor Objects platform as well as the application platforms are established. Further work will concentrate on interoperability of security.

- Develop concrete solutions in specific applications scenarios – A liaison between the pSHIELD partners and Telenor Objects, JBV, the Norwegian Computer Society, the Norwegian Mobile Association and Wireless Future has been created. During this liaison we identified promising IoT platforms satisfying the needs of privacy, security and dependability. The Telenor Objects platform Shepherd is on of these pilot platforms, wand will be made available for other pilot applications. Thus pSHIELD opened for a much wider entry into the Nordic and European Market, ensuring an industry-ready design of the framework. The specific application scenario was created together with the Norwegian Rail Administration, and has already now envisaged 4-6 new application scenarios, covering goods tracking, quality-of-transport control, maintenance of rolling equipment and track reporting. Together with the liaison partners new scenarios such as e-Health (Rikshospitalet) and Socialtainment ("mobility in the post-oil age") have been identified. Additonal contacts have been established to ABB, the market leader for IoT based energy supply and the Norwegian Defence Research Establishment (FFI). Workshops are planned for Q3.2011 to establish the potential for pSHIELD results.

Highlight clearly significant and tangible results

During the second reporting period, CWIN and Movation have provided/performed:

- established a sensor platform consisting of nano-, micro- and personal nodes to measure acceleration, temperature, position, and light conditions. The platform is already deployed in the Telenor Innovation Fair, and foreseen for implementation in the locomotive.
- first implementation on the measurement locomotive provided additional challenges for the operation:
  - a fully-autonomous operation. The sensor platform needs to reboot into operation on a "power-on" contact. This caused a major redesign of internal libraries for the sensors and the platform in order to ensure "boot into operation"
  - need for a multi-technology implementation, as the GPS receive information inside the measurement locomotive is very limited. This requirement caused us to consider a multi-technology implementation based on both a mobile phone and the personal node platform.
- Identification of SPD functionalities for the JBV prototype, especially in the security domain including cryptography and identity handling.
- Establish industrial contacts to ABB in order to expand the pSHIELD approach into the industrial energy environment
- Established contacts to FFI to enhance the SPD matrix into an attribute-based access authentication for the Internet of Things.
- Discussed with SIMLINK the use of an encrypted platform, the WlanSIM, as a potential future pSHIELD demonstrator.

- Discussed SPD functionalities with the national hospital (Rikshospitalet in order to receive requirements from the medical and healthcare sector. This sector is more conservative, asking for implemented standards before using new technology.
- Implementation of the semantic MediaWiki platform pSHIELD.unik.no for increased collaboration and better quality control of progress in the project
- established data exchange with the Shepherd platform from TelenorObjects, being an instance of the ETSI TS102.690 M2M platform.

3.10.1 Centre for Wireless Innovation

Beneficiary:	CWIN
Work Package(s)	WP2 - SPD metric, requirements and system design WP3 – SPD node WP5 – SPD middleware and overlay WP6 – Platform integration, validation & demonstration WP7 – Knowledge exchange and industrial validation
Task(s)	Task 2.2 Multi-technology SPD metrics Task 2.3 Multi-technology architectural design Task 3.1 Nano, Micro/Personal node Task 3.2 Power node Task 5.1 SPD driven semantics Task 5.3 Policy-based management Task 6.1 Multi-technology system integration Task 6.4 Multi-technology demonstration Task 7.1 Dissemination Task 7.2 Exploitation
Period:	1. January 2011 - 30. June 2011
Effort planned in this period:	Task 2.2 Multi-technology SPD metrics 1PM Task 2.3 Multi-technology architectural design 0,5 PM Task 3.1 Nano, Micro/Personal node 2PM Task 3.2 Power node 0,5PM Task 5.1 SPD driven semantics 2PM Task 5.3 Policy-based management 1PM Task 6.1 Multi-technology system integration 2PM Task 6.4 Multi-technology demonstration 0,5PM Task 7.1 Dissemination 0PM
Effort actual or spent in this period:	Task 2.2 Multi-technology SPD metrics 1PM Task 2.3 Multi-technology architectural design 0,5 PM Task 3.1 Nano, Micro/Personal node 2PM Task 3.2 Power node 0,5PM Task 5.1 SPD driven semantics 1PM

	Task 5.3 Policy-based management 1PM Task 6.1 Multi-technology system integration 2PM Task 6.4 Multi-technology demonstration 0.5PM Task 7.1 Dissemination 0.5PM
% of work completed at the end of the period (indicative):	Task 2.2 Multi-technology SPD metrics 90% Task 2.3 Multi-technology architectural design 60% Task 3.1 Nano, Micro/Personal node 90% Task 3.2 Power node 75% Task 5.1 SPD driven semantics 90% Task 5.3 Policy-based management 50% Task 6.1 Multi-technology system integration 50% Task 6.4 Multi-technology demonstration 40% Task 7.1 Dissemination 70%

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

- Task 2.2
  - ➢ Examination of basis SPD technologies, to be useable for the prototype
  - ➢ Follow discussions and establish understanding related to prototype
  - ➢ **Results**: dependability and security issues identified for final demonstration
- Task 2.3
  - ➢ Node layer technologies such micro, nano, personal and power node had been identified.
  - ➢ Key pSHIELD applications and SPD functionalities within the applications had been identified and discussed.
  - ➢ **Results**:
    - o Node layer technologies had been described in D2.3.1.
    - o Applications and functionalities had been explained in D2.3.1.
- Task 3.1
  - ➢ Suitable pSHIELD nodes had been explored.
  - ➢ Nodes for pSHIELD prototype has been identified.
  - ➢ Node technologies including software and hardware had been studied, discussed and tested.
  - ➢ **Results**: Based on the exploration of different types of nodes, characteristics of pSHIELD node types such as micro/nano, personal and power node had been defined in D3.1. Identified node technologies has been described in D3.2.
- Task 3.2
  - ➢ identification of potential power nodes
  - ➢ our focus was on personal nodes, thus contributions on power nodes where high-level discussions, no detailed developments on power nodes
  - ➢ **Results:** identification of SPD similarity between power and personal nodes
- Task 5.1
  - ➢ Explored different ontology languages
  - ➢ Different ontology languages had been analysed and evaluated based certain criteria (e.g., expressivity, complexity, reasoning performance etc.)
  - ➢ A semantic media wiki platform has been established for knowledge presentation with export/import functionalities.
- ➢ **Results:**

    - Evaluation of ontology languages had been documented in the draft of D5.1
    - Semantic MediaWiki platform: http://pshield.unik.no

- Task 5.3
  - Explored how to enhance policy-based management with semantics.
  - Evaluation of different policy languages.
  - Evaluation of semantically enhanced-policy management and execution, including attribute-based access.
  - **Results**:
    - identification of research on how attribute-based access can be defined through semantic technologies
    - Extension of semantic attribute-based access for IoT-based sensor access
- Task 6.1
  - Exploration of ways to integrate node layers with the middleware/overlay layers using M2M platform.
  - Test of such integration possibilities.
  - **Results**: Implementation of autonomous platform for use in Measurement Train "Roger"
- Task 6.4:
  - Functionalities of early pSHIELD demonstrator have been identified.
  - Extension towards a multi-technology (phone and personal node) platform performed.
  - **Results**: Early demonstration of node (micro & power node) integration to Telenor Object platform

Description of criticalities met during the period:

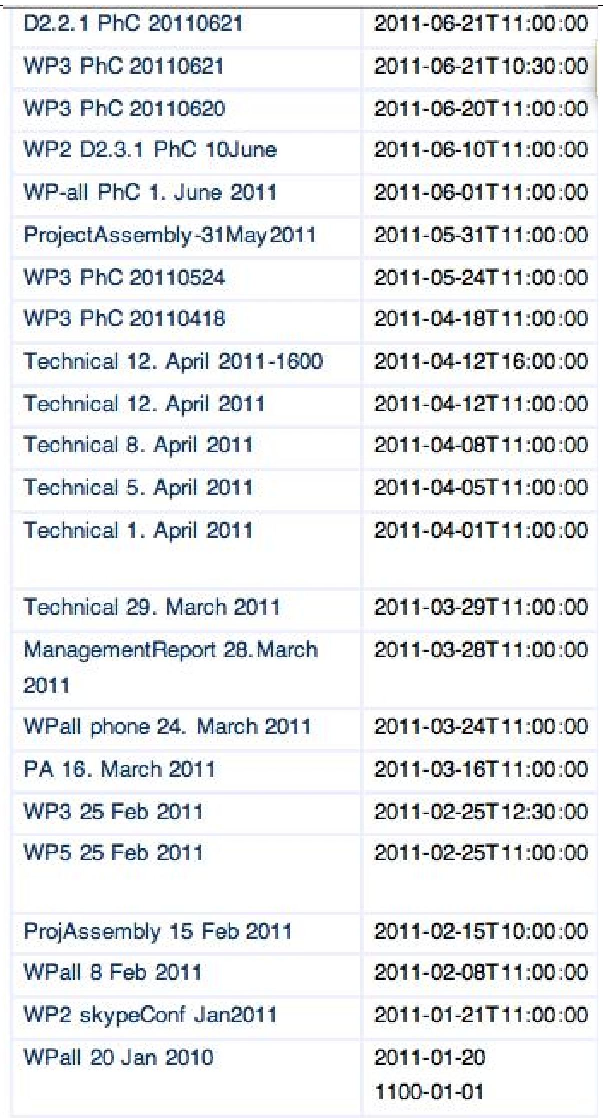
- unclear status of pSHIELD, no finances for follow-on project. This hampered the internal support for pSHIELD, and caused key personnel to leave the project
- restructuring of resources due to financial constraints
- technology: requirement for autonomous platform - the first platform implementation showed that the industrial requirements need an "automatic boot" and a fully-autonomous operation, with no interaction from operators. This requirement caused a reprogramming of some sensor and platform libraries.
- The "electromagnetic-dense" measurement locomotive used for implementation did not provide sufficient GPS reception. In order to establish positioning information, we decided to establish a mobile phone in parallel and use the multiple-location information on the phone. This also opens for dependability requirements, which will be further elaborated in the remaining phase of the project.

Corrective actions:

- Manpower transfer from Mushfiq Chowdhury to Sarfraz Alam and Zahid Iqbal.
- Multi-technology implementation of phone and personal node for demonstration

Meetings performed during the period:

- participation in all WP phone conferences and project meetings as documented on the wiki



D2.2.1 PhC 20110621	2011-06-21T11:00:00
WP3 PhC 20110621	2011-06-21T10:30:00
WP3 PhC 20110620	2011-06-20T11:00:00
WP2 D2.3.1 PhC 10June	2011-06-10T11:00:00
WP-all PhC 1. June 2011	2011-06-01T11:00:00
ProjectAssembly-31May2011	2011-05-31T11:00:00
WP3 PhC 20110524	2011-05-24T11:00:00
WP3 PhC 20110418	2011-04-18T11:00:00
Technical 12. April 2011-1600	2011-04-12T16:00:00
Technical 12. April 2011	2011-04-12T11:00:00
Technical 8. April 2011	2011-04-08T11:00:00
Technical 5. April 2011	2011-04-05T11:00:00
Technical 1. April 2011	2011-04-01T11:00:00
Technical 29. March 2011	2011-03-29T11:00:00
ManagementReport 28. March 2011	2011-03-28T11:00:00
WPall phone 24. March 2011	2011-03-24T11:00:00
PA 16. March 2011	2011-03-16T11:00:00
WP3 25 Feb 2011	2011-02-25T12:30:00
WP5 25 Feb 2011	2011-02-25T11:00:00
ProjAssembly 15 Feb 2011	2011-02-15T10:00:00
WPall 8 Feb 2011	2011-02-08T11:00:00
WP2 skypeConf Jan2011	2011-01-21T11:00:00
WPall 20 Jan 2010	2011-01-20 1100-01-01

Deviations between actual and planned person-months:

- Task 5.1 SPD driven semantics planned 2PM, used 1PM, underspent 1PM. Focus of CWIN was towards integration, SPD functionalities are covered by UNIROMA1 and SelexElsag (SE)
- Task 7.1 Dissemination planned 0PM, used 0,5PM, overspent 0,5 PM. Total budget for dissemination was too small.

Dissemination activities and exploitation perspectives:

- Dissemination had the focus on scientific dissemination, Movation (MAS) was responsible for targeted industrial dissemination. The results of the scientific dissemination were one journal article, one conference publication and an envisaged PhD.
    1. Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, "Interoperability of Security-enabled Internet of Things", to appear in Wireless Personal Communication Special Issue on "Internet of Things and Future Applications", Springer-Netherland, 2011.
    2. Mohammad M. R. Chowdhury, Josef Noll, "Securing Critical Infrastructure: A

Semantically Enhanced Sensor Based Approach", 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic System Technology, WiRELESS ViTAE 2011, Chennai, India, Feb. 28-March 2011.

- Exploitation is not typical for an academic institution, but we discuss with MAS if they want to take over responsibility for the exploitation of the embedded platform. We have already two installations, and have recognized strong interest from other projects and companies.

3.10.2 Movation AS

Beneficiary:	Movation (MAS)
Work Package(s)	WP1 – Management WP3 – SPD node WP5 – SPD middleware and overlay WP6 – Platform integration, validation & demonstration WP7 – Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project Management Task 3.1 Nano, Micro/Personal node Task 5.1 SPD driven semantics Task 6.1 Multi-technology system integration Task 6.4 Multi-technology demonstration Task 7.1 Dissemination Task 7.2 Exploitation
Period:	1. January 2011 - 30. June 2011
Effort planned in this period:	Task 1.1 Project Management 0PM Task 3.1 Nano, Micro/Personal node 1PM Task 5.1 SPD driven semantics 0PM Task 6.4 Multi-technology demonstration 0,5PM Task 7.1 Dissemination 0PM
Effort actual or spent in this period:	Task 1.1 Project Management 0,5PM Task 3.1 Nano, Micro/Personal node 0,5PM Task 5.1 SPD driven semantics 1PM Task 6.4 Multi-technology demonstration 0.5PM Task 7.1 Dissemination 1PM
% of work completed at the end of the period (indicative):	Task 1.1 Project Management 60% Task 3.1 Nano, Micro/Personal node 90% Task 5.1 SPD driven semantics 90% Task 6.4 Multi-technology demonstration 40% Task 7.1 Dissemination 70%

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

- Task 1.1
  - Established the means to take over project leadership, i.e. consistency mechanisms on the semantic MediaWiki
  - Increased the responsibilities of the Norwegian contribution towards an SPD-enabled prototype
  - **Results**:
    - Agreements on how to successful collaborate
- Task 3.1
  - Follow discussions and establish understanding related to prototype
  - Correlate results with industrial needs in the domains of health care, energy automation and transport
  - Supported CWIN in the design and implementation of the prototype
  - **Results**: pSHIELD prototype consisting of nano, micro and personal node established and installed in the Telenor Innovation Fair
- Task 5.1
  - Working towards semantic interoperability, “from sensors to business decisions”
  - Industrial collaboration to populate date from the embedded platform
  - A semantic media wiki platform has been established for knowledge presentation with export/import functionalities.
  - **Results**:
    - Identified tripple store as the core storage for semantic information, evaluation of challenges for sensor integration.
    - Semantic MediaWiki platform: http://pshield.unik.no
- Task 6.4:
  - Supported discussions of pSHIELD prototype, including path towards SPD functionality
  - Support for extension towards a multi-technology (phone and personal node) platform.
  - **Results**: Early demonstration of node (micro & power node) integration to Telenor Object platform

Description of criticalities met during the period:

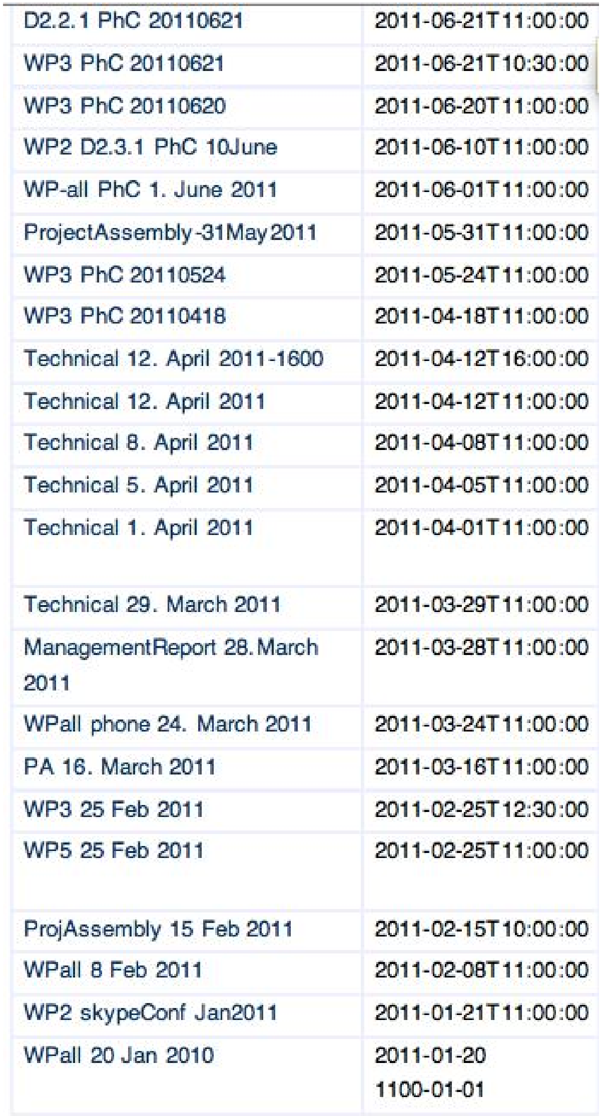
- project management issue caused unnecessary tensions and work
- technology: requirement for autonomous platform - the first platform implementation showed that the industrial requirements need an “automatic boot” and a fully-autonomous operation, with no interaction from operators. This requirement caused a reprogramming of some sensor and platform libraries.
- The “electromagnetic-dense” measurement locomotive used for implementation did not provide sufficient GPS reception. In order to establish positioning information, we decided to establish a mobile phone in parallel and use the multiple-location information on the phone. This also opens for dependability requirements, which will be further elaborated in the remaining phase of the project.

Corrective actions:

- Agreed to take over responsibility as project manager. Contributed to a collaborative project management with a good team consisting of Przemek Osocha, Francesca Matarese, Elisabetta Campaiola and Josef Noll.
- Suggestion for multi-technology implementation of phone and personal node for demonstration

Meetings performed during the period:

- participation in all WP phone conferences and project meetings as documented on the wiki, in addition to the individual communication with project members and the JU



D2.2.1 PhC 20110621	2011-06-21T11:00:00
WP3 PhC 20110621	2011-06-21T10:30:00
WP3 PhC 20110620	2011-06-20T11:00:00
WP2 D2.3.1 PhC 10June	2011-06-10T11:00:00
WP-all PhC 1. June 2011	2011-06-01T11:00:00
ProjectAssembly-31May2011	2011-05-31T11:00:00
WP3 PhC 20110524	2011-05-24T11:00:00
WP3 PhC 20110418	2011-04-18T11:00:00
Technical 12. April 2011-1600	2011-04-12T16:00:00
Technical 12. April 2011	2011-04-12T11:00:00
Technical 8. April 2011	2011-04-08T11:00:00
Technical 5. April 2011	2011-04-05T11:00:00
Technical 1. April 2011	2011-04-01T11:00:00
Technical 29. March 2011	2011-03-29T11:00:00
ManagementReport 28. March 2011	2011-03-28T11:00:00
WPall phone 24. March 2011	2011-03-24T11:00:00
PA 16. March 2011	2011-03-16T11:00:00
WP3 25 Feb 2011	2011-02-25T12:30:00
WP5 25 Feb 2011	2011-02-25T11:00:00
ProjAssembly 15 Feb 2011	2011-02-15T10:00:00
WPall 8 Feb 2011	2011-02-08T11:00:00
WP2 skypeConf Jan2011	2011-01-21T11:00:00
WPall 20 Jan 2010	2011-01-20 1100-01-01

Deviations between actual and planned person-months:

- Task 1.1 Project management planned 0PM, used 0,5PM, overspent 0,5PM. The project members asked the Movation representative to take over the administrative leadership, which requires being much more involved in administrative matters
- Task 3.1 nano, micro, personal nodes planned 1PM, used 0,5PM, underspent 0,5 PM. Focus on getting liaison with national partners and prototypical demonstrations in place, left technology development to the other partners.
- Task 5.1 SPD driven semantics planned 0PM, used 1PM, overspent 1PM. Focus on Semantic interworking, both with respect to representation (wiki) and import/export functionality of embedded platform data (not resolved).
- Task 7.1 Dissemination planned 0PM, used 1PM, overspent 1PM. The prototypical demonstrations foreseen in Norway enhanced the visibility of pSHIELD work, and opened for contacts in defence, health care and energy automation.
- Both the increased effort in prototypical demonstration and the new role as administrative project manager caused the overspending. The current estimate is that the Norwegian partners will have an overspent of about 22%, which is asked to funded through an increased national contribution. If that fails, then CWIN and Movation will increase their internal funding.

Dissemination activities and exploitation perspectives:

- Movation (MAS) was responsible for targeted industrial dissemination.
- (1) ABB in Norway has two groups with research interests related to SHIELD issues. The security group represented by Judith Rossebø and the wireless sensor group represented by Paal Orten. ABB was one of the core developers of the WirelessHART protocol, and expects that an industrial uptake will require SPD functionalities as indicated by pSHIELD.
  Status: First contacts established, resulting in an invitation to the Industrial Embedded System Workshop (19.-20. October 2011) in Trondheim. From there we will discuss further.
- Norwegian Defence Research Establishment (FFI)
  FFI is the prime institution responsible for defence-related research in Norway. The Establishment is the chief adviser on defence-related science and technology to the Ministry of Defence and the Norwegian Armed Forces' military organization.
  Status: Meeting planned in Q3.2011
- 28. June 2011, Meeting with Simlink, having developed a WLAN SIM
  - security options with OTA (over the air application install) and controlling of devices
  - interesting technology for micro- and personal-nodes
  - several sensor applications in the market
- 9. May 2011, An example of the pSHIELD personal node platform (embedded Linux) was provided to ESIS and Telenor Objects, who used the platform within the electrical motorcycle of ESIS. This motorbike is part of the Telenor Innovation Fair at Fornebu, Norway.
- 5. April 2011, Presentation of "Security, Privacy and Dependability" of embedded systems to the National Hospital "Rikshospitalet". The goal of this meeting is to elaborate the applicability of pSHIELD integrated sensors for eHealth purposes, together with Telenor Objects.
  Results: health sector needs standardised solution before the roll-out. Too early for pSHIELD.
- Movation is considering the exploitation of the embedded platform. We have already two installations, and have recognized strong interest from other projects and companies. As hardware support is outside of the core operation of Movation, a potential solution will be in the collaboration with one of our Inner Circle Partners or an industrial partner.

3.11 Slovenia

3.11.1 THYIA Tehonlogije (Coordinator)

Beneficiary[26]:	**THYIA**
Work Package(s)	WP1[27] – Project management (total 2PM for WP2 management) WP2 – SPD metric, requirements and system design (total 11 PM) WP3 – SPD node (total 21 PM) WP4 – SPD Network (total 8 PM) WP5 – SPD Middleware and Overlay (total 11 PM) WP6 – Platform integration, validation & demonstration (total 25 PM) WP7 – Knowledge exchange and industrial validation (total 6PM)
Task(s)	Task 1.1 Project management Task 2.1 Multi-technology requirements & specification Task 2.3 Multi-technology SPD metrics Task 2.3 Multi-technology architectural design Task 3.1 Nano, micro/personal node Task 3.3 Dependable self-x and cryptographic technologies Task 4.1 Smart SPD driven transmission Task 4.2 Trusted and dependable Connectivity Task 5.1 SPD driven Semantics Task 5.2 Core SPD services Task 5.4 Overlay monitoring and reacting system by security agents Task 7.1 Dissemination
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 Project management – 1.5 PM Task 2.1 Multi-technology requirements & specification – 3 PM Task 2.2 Multi-technology SPD metrics – 3 PM Task 2.3 Multi-technology architectural design – 4 PM Task 3.1 Nano, micro/personal node -5 PM Task 3.3 Dependable self-x and cryptographic technologies- 2 PM Task 4.1 Smart SPD driven transmission - 0.25 PM Task 4.2 Trusted and dependable Connectivity - 0.25 PM Task 5.1 SPD driven Semantics - 0.3 PM Task 5.2 Core SPD services 0.5 PM Task 5.4 Overlay monitoring and reacting system by security

[26] This report is per Beneficiary, and it provides as many as WPs in which it is involved each Beneficiary (see as PPR - Project Periodic Report, section 1.2.7.)
[27] x is 1, 2, 3, 4, 5, 6, and 7

	agents – 0.5 PM Task 7.1 Dissemination 0.2 PM
Effort actual or spent in this period:	Task 1.1 Project management – 0 PM 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 Task 3.1 Nano, micro/personal node -0 PM Task 3.3 Dependable self-x and cryptographic technologies-0 PM Task 4.1 Smart SPD driven transmission - 0 PM Task 4.2 Trusted and dependable Connectivity - 0 PM Task 5.1 SPD driven Semantics - 0 PM Task 5.2 Core SPD services 0 PM Task 5.4 Overlay monitoring and reacting system by security agents – 0 PM Task 7.1 Dissemination 0 PM
% of work completed at the end of the period (indicative):	Task 1.1 Project management – 0% Task 2.1 Multi-technology requirements & specification –0% Task 2.2 Multi-technology SPD metrics – 0% Task 2.3 Multi-technology architectural design – 0% Task 3.1 Nano, micro/personal node - 0% Task 3.3 Dependable self-x and cryptographic technologies- 0% Task 4.1 Smart SPD driven transmission – 0% Task 4.2 Trusted and dependable Connectivity - 0% Task 5.1 SPD driven Semantics - 0% Task 5.2 Core SPD services 0% Task 5.4 Overlay monitoring and reacting system by security agents – 0% Task 7.1 Dissemination 0%

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

- **Task 1.1 Project management**
  - On the request from SESM, THYIA took the role “Project Coordinator” starting from 8th of December 2010 when signed the GA with the Artemis JU.
  - THYIA spends some additional effort for the administrative project coordination. The management effort was spent for WP2.
  - THYIA was substituted by MAS officially on the 5th of August 2011.
  - Contributions to D1.1.1, D1.1.2 and D1.1.3 documents
  - Results:
    - A voluntary work for the administrative coordination engaged additional human and other resources that are not covered with the national agreement.
    - Repository BSCW server development and administration
    - An extra work was dedicated for development and finalisation of D1.1.1, D1.1.2 and D1.1.3 documents as support to SESM.
- **Task 2.1 Multi-technology requirements & specification**
  - Intensive contributions in D2.1.1

- Studies, analysis and R&D activities for the application scenario, pSHIELD system, node, network, middleware and overly requirements and specifications are performed.
- Additionally contributes with two internal deliverables
- Results:
  - 90% completed D2.1.1.
  - A pre-development phase for selecting the pSHIELD SPD components for the Demonstrator
  - A pre-development phase for designing the application scenario (simulation, HW and SW models and components)

- **<u>Task 2.2 Multi-technology SPD metrics</u>**
  - Intensive contributions in D2.2.1
  - Studies, analysis and R&D activities for pSHIELD system, node, network, middleware and overly metrics requirements and specifications are performed.
  - Results:
    - Almost in a final draft version D2.2.1 that will be corrected in accordance with additional work performed for Formalised Conceptual Models (now as deliverable M0.1) and Aggregation Metrics (now as deliverable M0.2).
    - Selection of the conceptual models for the SPD metrics related to the WSNs, Enhanced-SPD nano, mikro/personal node.
    - Initial work for the simulation
    - Selection of the nano-micro architecture (HW and SW), Security and Dependability Metrics
- **<u>Task 2.3 Multi-technology architectural design</u>**
  - Contributions in D2.3.1 plus two internal deliverables for overly and cross-layer architecture
  - Studies, analysis and R&D activities for pSHIELD nano, micro/personal node architecture based of the D2.1.1 requirements and specifications are performed.
  - Results:
    - A final first draft version D2.3.1 that will be corrected in accordance with additional work performed for deliverables M0.1 and M0.2
    - Selection of the pSHIELD reference architecture for the Demonstrator
    - Selection of the Enhanced SPD nano, micro/personal node that will be used for the Demonstrator
    - Initial architectural design of the pSHIELD Demonstrable Network.
    - Studies on the TiniOS, Contiki and Hydra sensor node solutions and their possible up-grade to SPD Nodes.
    - Study on the pSHIELD Gateway (GW) solution
- **<u>Task 3.1 Nano, micro/personal node</u>**
  - Contributions in D3.1
  - Studies, analysis and R&D activities for detailed specifications (HW and SW partition) for pSHIELD nano, micro/personal node architecture based of the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications.
  - Results:
    - A final first version D3.1 is developed.
    - Embedded System security base on the whole design pyramid is investigated (protocol, algorithm, architecture, micro-architecture and circuit level)
    - Potential architecture for SPD core module that include TPM and MTM features
    - Secure firmware, secure boot and bootstrapping with key management is investigated

- An architectural solution of nano node analysed for 3D integration technology is considered as first choice that can be also modelled by conceptual models.
- An architectural solution for micro/personal node is analysed as a possible upgrade of Contiki and Hydra OS solutions.
- SPD conceptual models are proposed for sensor node based on the IEEE 802.11, IEEE 802.15.4 standards

<u>Task 3.3 Dependable self-x and cryptographic technologies</u>

- Contributions in D3.4
- Studies, analysis and R&D activities for detailed specifications regarding cryptography technologies based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - A first draft version D3.4 is developed.
  - Self-x technologies are studied in details, and possible solutions are identified.
  - Elliptic Curve Cryptography techniques (fast algorithms, TinyECC) are investigated for WSNs as possible solutions.
  - Automatic access control, denial-of-services, self-configuration and self-recovery as mechanisms in charge of preventing non authorised/malicious people to access the physical resources of the node are also investigated, and a potential model for the Demonstrator is identified.

<u>Task 4.1 Smart SPD driven transmission</u>

- Studies, analysis and R&D activities for detailed specifications regarding SPD smart driven transmission based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - Cognitive Radio and SDR are considered as candidate technologies.
  - Security technologies like IPsec for the network layer and possible modification (light version) for small sensor nodes are considered and compared with other possible SoC solutions.

<u>Task 4.2 Trusted and dependable Connectivity</u>

- Studies, analysis and R&D activities for detailed specifications regarding dependable connectivity based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - Different architectural solutions are considered for network management.

<u>Task 5.1 SPD driven Semantics</u>

- Studies, analysis and R&D activities for detailed specifications regarding semantic ontology based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - OWL technologies, an internal reports
  - Potential solutions are identified
  - New SW modules for middleware are identified

<u>Task 5.2 Core SPD services</u>

- Studies, analysis and R&D activities for detailed specifications regarding core SPD service based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - Lange based support for service oriented architecture – future direction
  - New SW modules for middleware are identified

<u>Task 5.4 Overlay monitoring and reacting system by security agents</u>

- Studies, analysis and R&D activities for detailed specifications regarding security agents based on the D2.1.1, D2.2.1, and D2.3.1 requirements and specifications are performed.
- Results:
  - AOA architectures
  - Developing secure agent system using delegation based trust management
  - New SW modules for middleware are identified

Task 7.1 Dissemination

- Dissemination versus national authority, external communications with industry and academy (notional and international). Support to CWIN dissemination activities.

A summary progress towards objectives.

The fulfilment of project's task and objectives is almost 100%. Details are provided below.

- A voluntary work for the administrative coordination engaged additional human and other resources that are not covered with the national agreement
- Responsibility for the repository BSCW server development and administration
- An extra work dedicate for development and finalisation of D1.1.1, D1.1.2 and D1.1.3 documents as support to SESM
- 90% completed D2.1.1
- Selection of the pSHIELD SPD components for the Demonstrator
- Initial conceptual models for the application scenario (simulation, HW and SW models and components)
- Almost in a final draft version D2.2.1 that will be corrected in accordance with additional work performed for Formalised Conceptual Models (now as deliverable M0.1) and Aggregation Metrics (now as deliverable M0.2)
- Selection of the conceptual models for the SPD metrics related to the WSNs, Enhanced-SPD nano, mikro/personal node (now included in deliverable M0.1)
- Selection of the nano-micro architecture (HW and SW), Security and Dependability Metrics (now included in deliverable M0.1)
- A final first draft version D2.3.1
- Selection of the pSHIELD reference architecture for the Demonstrator (now included in deliverable M0.1)
- Selection of Enhanced SPD nano, micro/personal node that will be used for the Demonstrator (now included in deliverable M0.1)
- Initial architectural design of the pSHIELD Demonstrable Network (now included in deliverable M0.1)
- Study on the TiniOS, Contiki and Hydra sensor node solutions and their possible up-grade to SPD Nodes (now included in deliverable M0.1)
- Study on the pSHIELD Gateway (GW) solution (now included in deliverable M0.1)
- A final first version D3.1 is developed
- Embedded System security base on the whole design pyramid is investigated (protocol, algorithm, architecture, micro-architecture and circuit level) – ongoing work
- Potential architecture for SPD core module that include TPM and MTM futures – ongoing work
- Secure firmware and bootstrapping with key management is investigated – ongoing work
- An architectural solution of nano node analysed for 3D integration technology is considered as

first choice that can be also modelled by conceptual models (now included in deliverable M0.1)

- An architectural solution for micro/personal node is analysed as a possible upgrade of Contiki and Hydra OS solutions (now included in deliverable M0.1)
- SPD conceptual models are proposed for sensor node based on the IEEE 802.11, IEEE 802.15.4 standards (now included in deliverable M0.1)
- A first draft version D3.4 is developed
- Self-x technologies are studied in details, and possible solutions are identified -ongoing work
- Elliptic Curve Cryptography techniques (fast algorithms, TinyECC) are investigated for WSNs as possible solutions – ongoing work
- Automatic access control, denial-of-services, self-configuration and self-recovery as mechanisms in charge of preventing non authorised/malicious people to access the physical resources of the node are also investigated, and a potential model for the Demonstrator is identified – ongoing work
- Cognitive Radio and SDR are considered as candidate technologies – ongoing work
- Security technologies like IPsec for the network layer and possible modification (light version) for small sensor nodes are considered and compared with other possible SoS solutions – ongoing work
- Different architectural solutions are considered for network management – ongoing work
- OWL technologies, an internal reports
- Lange based support for service oriented architecture – future direction
- AOA architectures – ongoing work
- Developing secure agent system using delegation based trust management – ongoing work

Clearly significant and tangible results

- Administrative coordination of the project and PM role
- Responsibility for repository BSCW server development and administration
- D1.1.1, D1.1.2 and D1.1.3 deliverables
- D2.1.1 deliverable
- D2.2.1 deliverable
- D2.3.1 deliverable
- D3.1 first draft
- D3.4 first draft
- Selection of the conceptual models for the SPD metrics related to the WSNs, Enhanced-SPD nano, mikro/personal node (now included in deliverable M0.1)
- Selection of the nano-micro architecture (HW and SW), Security and Dependability Metrics (now included in deliverable M0.1)
- Selection of the pSHIELD reference architecture for the Demonstrator (now included in deliverable M0.1)
- Selection of the Enhanced SPD nano, micro/personal node that will be used for the Demonstrator (now included in deliverable M0.1)
- Initial architectural design of the pSHIELD Demonstrable Network (now included in deliverable M0.1)
- Study on the TiniOS, Contiki and Hydra sensor node solutions and their possible up-grade to SPD Nodes (now included in deliverable M0.1)
- Study on the pSHIELD Gateway (GW) solution (now included in deliverable M0.1)

- An architectural solution of nano node analysed for 3D integration technology is considered as first choice that can be also modelled by conceptual models (now included in deliverable M0.1)
- An architectural solution for micro/personal node is analysed as a possible upgrade of Contiki and Hydra OS solutions (now included in deliverable M0.1)
- SPD conceptual models are proposed for sensor node based on the IEEE 802.11, IEEE 802.15.4 standards (now included in deliverable M0.1)

3.12 Portugal

3.12.1. Critical Software

Beneficiary:	Critical Software – CS
Work Package(s)	**WP1 - Project Management**
Task(s)	Task 1.1 Project Management Task 1.2 Liaisons
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 1.1 – 0.5 PM Task 1.2 – 0.4 PM
Effort actual or spent in this period:	Task 1.1 – 0.5 PM Task 1.2 – 0,4 PM
% of work completed at the end of the period (indicative):	Task 1.1 – Actual = 75 % (Planned: 75%) Task 1.2 – Actual = 60 % (Planned: 60%)

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

- Task 1.1 – Project Management
  - After the review meeting held in March 2011 in Brussels there were 6 major deliverables that were required to be produced within a short period of time. One of these, M06 "Management Report", was to produce the overall periodic report and a large amount of effort was spent working with THYIA to ensure the document produced was of suitable quality. From other projects that Critical Software has been involved with we have experience in producing these reports and could offer some suggestions on what was needed to ensure the pSHIELD periodic Report was written to the required standard.
  - Another outcome of the above meeting was an extension to the project of 7 months taking the finish date up to the end of 2011. Once this was confirmed to the project consortium Critical Software assessed the new dates for each of the Work Packages and the related deliverables. Also the extension to the project did not allow for any further effort to be claimed so the planned effort of the project that had not been used had to be spread over the longer period of time. This was done ensuring that Critical Software would deliver on all its required inputs to the project deliverables.
  - Within this period there still was no signed national Grant Agreement from FCT (*Fundação para a Ciência e a Tecnologia*). This has been received by us on 22nd July 2011. During the period of this report however Critical Software regularly spent resources chasing FCT to see the status of this and pushing to get the situation resolved.
  - During all of the Management and planning meetings (and there have been a large number of these) Critical Software has ensured there is always a representative of CSW present during these. This has been done to ensure that whatever decisions are made we have an input into the decision making process as opposed to having no voice in the project.

- Task 1.2 - Liaisons
  - From analysing other FP7 projects Critical Software has looked at the industrial partners involved with these with a view to understanding how the pSHIELD technology could be utilised within different business scenarios.

Beneficiary:	Critical Software – CS
Work Package(s)	**WP2 - SPD Metric, requirements and system design**
Task(s)	Task 2.1 Multi-technology requirements & specification Task 2.2 Multi-technology SPD metrics Task 2.3 Multi-technology architectural design
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 2.1 – 0,2 PM Task 2.2 – 0,4 PM Task 2.3 – 0,4 PM
Effort actual or spent in this period:	Task 2.1 – 0,2 PM Task 2.2 – 0,4 PM Task 2.3 – 0,4 PM

% of work completed at the end of the period (indicative):	Task 2.1 – Actual = 100 % (Planned: 100%) Task 2.2 – Actual = 90 % (Planned: 90%) Task 2.3 – Actual = 90 % (Planned: 90%)

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

- Task 2.1; Task 2.2; Task 2.3
  - Participation in WP2 meetings (phone conferences organised by WP leader and Task leaders).
  - Review and contribution to deliverables:
    - D2.1.1 "System Requirements and Specification" (e.g. contribution to methodology for pSHIELD System Requirements Specification);
    - D2.2.1 "Preliminary SPD Metrics Specification" (e.g. contribution to SPD metrics composition – "medieval castle" approach);
    - D2.3.1 "Preliminary System Architecture Design" (e.g. contribution to middleware definitions).

Additional information:

- WP2 focuses on the identification of the overall pSHIELD system requirements and specifications, its design and the definition of the SPD metrics. The main objective of CSW's participation in this WP is to ensure that we participate in the discussions and within the document elaboration that will form the basis of the pSHIELD work, namely the work to be performed within WP3, WP4, WP5 and WP6.
- In the WP Kick-Off Meeting, it was decided that CSW's main task will be related with the discussion and review of the three deliverables that are to be produced. Nevertheless, CSW also provides contribution to the deliverables in areas of its expertise.
- The remaining work within WP2 will mainly address the activities related with final review and proof-reading of the deliverables before being issued to release.

Beneficiary:	Critical Software - CS
Work Package(s)	**WP3 - SPD Node**
Task(s)	Task 3.1 Nano, micro/personal node Task 3.3 Dependable self-x and cryptographic technologies
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 3.1 – 0,5 PM Task 3.3 – 3,0 PM
Effort actual or spent in this period:	Task 3.1 – 0,2 PM Task 3.3 – 3,0 PM
% of work completed at the end of the period (indicative):	Task 3.1 – Actual = 10 % (Planned: 25%) Task 3.3 – Actual = 97 % (Planned: 97%)

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

- Task 3.1
  - Participation in Task meetings (phone conferences organised by WP leader and Task leader)
  - Instigated by task leader, CSW participation in this task focus the review of its outcome, namely the task deliverables and their possible interactions with Task 3.3

- Task 3.3
  - Participation in WP3 meetings (phone conferences organised by WP leader).
  - After the research studies and evaluations performed in the first period, in this second period the main activities in this task concerned:
    - Studies of SotA cryptography libraries available for resource constraint devices, according to outcome of first period research studies and pSHIELD's application scenario;
    - Complementary study to test the respective algorithms implementation on the hardware of a possible micro (TelosB mote) and power (Linux based computer) node;
    - Selection and description of cryptographic libraries.
  - Results: The results of Task 3.3 activities are formalised within Deliverable 3.4 "SPD self-x and cryptographic technologies", available at pSHIELD BSCW Server.

Additional information:

- The remaining work within Task 3.3 is expected to exhibit, by means of a physical setup, a recommended cryptographic scheme deployed on a WSN platform including key exchange, authentication and secure communication, thus tightly related with the CSW work on Task 4.2.

Beneficiary:	Critical Software - CS
Work Package(s)	**WP4 - SPD Network**
Task(s)	Task 4.2 Trusted and dependable Connectivity
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 4.2 – 3,0 PM
Effort actual or spent in this period:	Task 4.2 – 2,0 PM
% of work completed at the end of the period (indicative):	Task 4.2 – Actual = 78 % (Planned: 86%)

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

- Task 4.2
  - ➢ The activities performed in this task are being performed in parallel with the work on Task 3.3. The main activity undertaken was the research relating to the state-of-the-art technology within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme.
  - ➢ After the research studies and evaluations performed in the first period, in this second period the main activities in this task concerned preliminary studies and discussions regarding the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices (pSHIELD application scenario).
  - ➢ Results: The results of Task 4.2 activities are formalised in Deliverable 4.2 “SPD network technologies prototypes report”, available at the pSHIELD BSCW Server.

Additional information:

- ➢ The remaining work within Task 4.2 is expected to exhibit, by means of a physical setup, a recommended cryptographic scheme deployed on a WSN platform including key exchange, authentication and secure communication, thus tightly related with CSW work on Task 3.3.

Beneficiary:	Critical Software - CS
Work Package(s)	**WP5 - SPD Middleware & Overlay**
Task(s)	Task 5.2 Core SPD services Task 5.3 Policy-based management Task 5.4 Overlay monitoring and reacting system by security agents
Period:	1st January 2011 – 30th June 2011
Effort planned in this period (Details from original TA):	Task 5.2 – 2,4 PM Task 5.3 – 0,4 PM Task 5.4 – 1,2 PM
Planned effort as a result of consortium change proposal (see ‘Additional Information’):	Task 5.2 – 4,5 PM Task 5.3 – 5,5 PM Task 5.4 – 0,0 PM
Effort actual or spent in this period:	Task 5.2 – 2,0 PM Task 5.3 – 5,5 PM Task 5.4 – 0,0 PM
% of work completed at the end of the period (indicative):	Task 5.2 – Actual = 35 % (Planned: 55%) Task 5.3 – Actual = 100 % (Planned: 100%) Task 5.4 – Actual = 00 % (Planned: 00%)

Description of the activities carried out during the period to reach specific objectives within the task/WP: • Task 5.2 ➢ Participation in WP5 meetings (phone conferences organised by WP leader). ➢ Analysis of the OSGi Knopflerfish open source platform as technological implementation of pSHIELD middleware architecture. ➢ Analysis of possible integration of CSW work performed within WP3/WP4 with the middleware implementation performed in this task. • Task 5.3 ➢ Participation in WP5 meetings (phone conferences organised by WP leader). ➢ Completion of the research started in first period on the state-of-the-art on the paradigm of policy-based management (PBM), namely regarding PBM architectures, policy specification languages and affiliated protocols, and an elaboration on the mapping to pSHIELD. ➢ Results: The table of contents for the results of Task 5.3 activities has been formalised in Deliverable 5.2 “SPD middleware and overlay functionalities prototype”. • Task 5.4 ➢ This task was not addressed within the CSW contribution (see section “Additional Information”).
Additional information: ➢ Instigated by CSW, our participation in WP5 was re-evaluated. This issue was discussed in the PA meeting held in Norway and CSW agreed to put more effort in T5.3 in order to provide a research study concerning PBM, moving this effort from T5.4 and continuing to have a presence in T5.2. ➢ The indicative % of the completed work for Task 5.2 and Task 5.3 presented in this table is taking into account effort reallocation. ➢ The remaining work in Task 5.2 involves the continuation of services’ specification and contribution to pSHIELD demonstrator according to the task objectives.

Beneficiary:	Critical Software – CS
Work Package(s)	**WP6 - Platform integration, validation & demonstration**
Task(s)	Task 6.1 Multi-Technology System Integration Task 6.2 Multi-Technology Validation & Verification Task 6.3 Lifecycle SPD Support Task 6.4 Multi-Technology demonstration
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 6.1 – 3,0 PM Task 6.2 – 0,5 PM Task 6.3 – 0,5 PM Task 6.4 – 0,5 PM
Effort actual or spent in this period:	Task 6.1 – 0,5 PM Task 6.2 – 0,0 PM Task 6.3 – 0,0 PM Task 6.4 – 0,0 PM

% of work completed at the end of the period (indicative):	Task 6.1 – Actual = 08 % (Planned: 50%) Task 6.2 – Actual = 00 % (Planned: 50%) Task 6.3 – Actual = 00 % (Planned: 50%) Task 6.4 – Actual = 00 % (Planned: 50%)

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

- Task 6.1
  - ➢ Discussion, identification and analysis of integration of CSW work within the pSHIELD application scenario.

- Task 6.2; Task 6.3; Task 6.4
  - ➢ These tasks did not formally start before the end of the reporting period.

Additional information:

- ➢ Due to project overall delay, the formal work in WP6 tasks is yet to be started. Nevertheless, internal discussions were held in order to define integration of CSW work in pSHIELD application scenario.

Beneficiary:	Critical Software – CS
Work Package(s)	**WP7 - Knowledge exchange and industrial validation**
Task(s)	Task 7.1 Dissemination Task 7.2 Exploitation
Period:	1st January 2011 – 30th June 2011
Effort planned in this period:	Task 7.1 – 0,2 PM Task 7.2 – 0,9 PM
Effort actual or spent in this period:	Task 7.1 – 0,2 PM Task 7.2 – 0,9 PM
% of work completed at the end of the period (indicative):	Task 7.1 – Actual = 90 % (Planned: 85%) Task 7.2 – Actual = 45 % (Planned: 45%)

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

- Task 7.1
  - ➢ The Critical Software pSHIELD team followed up the seminar held internally and has launched this information on the company website to spread the details to the wider community. In doing this it also invited comments and questions about the tasks and planned useage of this information.
- Task 7.2
  - ➢ For exploitation the details gathered from presenting the project to the wider community by using the Critical Software website to disseminate the details (described within T7.1) have been added to the details of the information regarding industrial partners that are working within present ongoing FP7 project (Task 1.2 – Liaisons). This has allowed Critical to identify who the target audience is for this technology and to allow Critical to focus its Exploitation efforts.
  - ➢ For Exploitation Critical has needed to understand exactly who the target market is and now has been able to define exactly who this would be and focus its effort on delivering what is required for the market.

A summary progress towards objectives.

The work performed in **WP1** has mainly focused on project management tasks. The main amount of effort was required for working with the consortium to produce the overall Periodic Report (M06). Utilising Critical Software's experience from other FP7 projects we were able to help the consortium in the production of this deliverable.

Also, as a result of the granted 7 month extension, there was a large amount of replanning undertaken to ensure Critical Software delivered on its agreed inputs within each specific work package and did this without negatively impacting its budget (the extension was granted to the project without any increase in effort).

Besides the management activities address by the work in WP1, during the three weeks period after mid-term review, CSW participated in several technical meetings and contributed to the production of the technical documents M0.1 ("Formalized conceptual models of the key pSHIELD concepts"), M0.2 ("Proposal for the aggregation of SPD metrics during composition") and M0.5 ("The pSHIELD focus areas, key innovations and project outputs").

In this second period of the project, Critical Software continued to contribute to **WP2** deliverables according to the planned activities, namely participating in WP meetings and contributing to deliverables' development and review.

In accordance with CSW's contribution shown within the Technical Annex, CSW's main contribution to pSHIELD is within the areas of "*Cryptography for low cost nodes*" and "*Dependable authentic key distribution mechanisms*". These activities have been planned according to three main phases: **Research**, **Selection** and **Integration**. According to the SPD features and technologies description that were presented within the Technical Annex (Table 2.2 – page 25), these two areas (mentioned above) fit into **WP3** and **WP4**, respectively. Nevertheless, since they are interrelated, the work is being performed in parallel.

Within this second period, the main activities have involved studies of SotA cryptography libraries available for resource constraint devices, according to outcome of first period research studies and pSHIELD's application scenario, a complementary study to test the respective algorithms implementation on the hardware of a possible micro (TelosB mote) and power (Linux based computer) node, and the selection and description of cryptographic libraries to be used in the third phase of CSW activities.

The main activities addressed within **WP5** included a state-of-the-art research study on the paradigm of policy-based management (PBM), namely regarding PBM architectures, policy specification languages and affiliated protocols, and an elaboration on the mapping of these to pSHIELD.

At the end of the "research" phase of the WP3 and WP4 activities, within the scope of **WP7**, the pSHIELD team reviewed the information gathered regarding the similar FP7 projects, looked at the industrial partners involved and assessed how the "Exploitation" could be undertaken.

For the next period, Critical Software will continue to contribute to the work packages where it is present so that the project goals can be successfully attained.

The main activities will be focused on WP3, WP4, WP5 and WP6, where our work is expected to exhibit a recommended cryptographic scheme deployed on a WSN platform, according to the pSHIELD application scenario.

After the initial WP meetings and a thorough analysis of each WP objectives, at consortium level and in the interests of the consortium and Critical Software, CSW requested to reallocate the planned PM on different tasks.

This reallocation was needed to resolve the need to extra effort within the software development and integration activities in Task 3.3 and also to perform activities within Task 5.3 that had not been initially planned but would be needed to support the future work on policy-based management. Overall it involved changes in both WP3 and WP5 and these changes had no negative effect on the development of the WP's deliverables, only positive benefits.

These changes are being managed at the WP level by the WP leaders and by the Technical Manager. With this approach, it will possible to ensure that the CSW objectives for the next period can be successfully achieved.

4 Deliverables and milestones tables

4.1 Deliverables (excluding the periodic and final reports)

TABLE 1. DELIVERABLES

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I with 7 months extension (proj month)	Delivered Yes/No	Actual / Forecast delivery date	Comments
D1.1.1	Collaborative tools and document repository	1	THYIA	O	PP	9	Yes	9	
D7.1.1	Web Site	7	SESM	O	PU	9	Yes	9	
D1.1.2	Quality Control Guidelines	1	SESM/MAS	R	PP	10	Yes	12	The document was delivered at Month 10, but non accepted. Re-delivered at Month 12
D2.1.1	System Requirements and Specifications	2	ASTS	R	PU	10	Yes	15	The document was delivered at Month 10, but non accepted. Re-delivered at Month 15
D2.2.1	Preliminary SPD Metrics Specifications	2	ESI/TECNALIA	R	PP	13	Yes	13	
D2.3.1	Preliminary System Architecture Design	2	HAI	R	PP	13	Yes	13	
D4.1	SPD network technologies prototype	4	SCOM	O, R	PP	13	Yes	13	

4.2 Milestones

TABLE 2. MILESTONES							
Milestone no.	**Milestone name**	**Work package no**	**Lead beneficiary**	**Delivery date from Annex I with 7 months extension (proj month)**	**Achieved Yes/No**	**Actual / Forecast achievement date**	**Comments**
M1	Project collaborative Working environment	WP1, WP7	THYIA, SESM	9	Yes	9	
M2	System requirements and specification	WP2	ASTS	10	Yes	15	The document was delivered at Month 10, but non accepted. Re-delivered at Month 15
M3	Preliminary SPD metrics and system architecture design and network prototype	WP2, WP4	ESI/TECNALIA, HAI, SCOM	13	Yes	13	

5 Project management

5.1 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 planed, 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. In frame of consortium management tasks the role of project coordinator who is a contact point with JU was maintained.

5.2 Encountered problems

Project Coordinator change

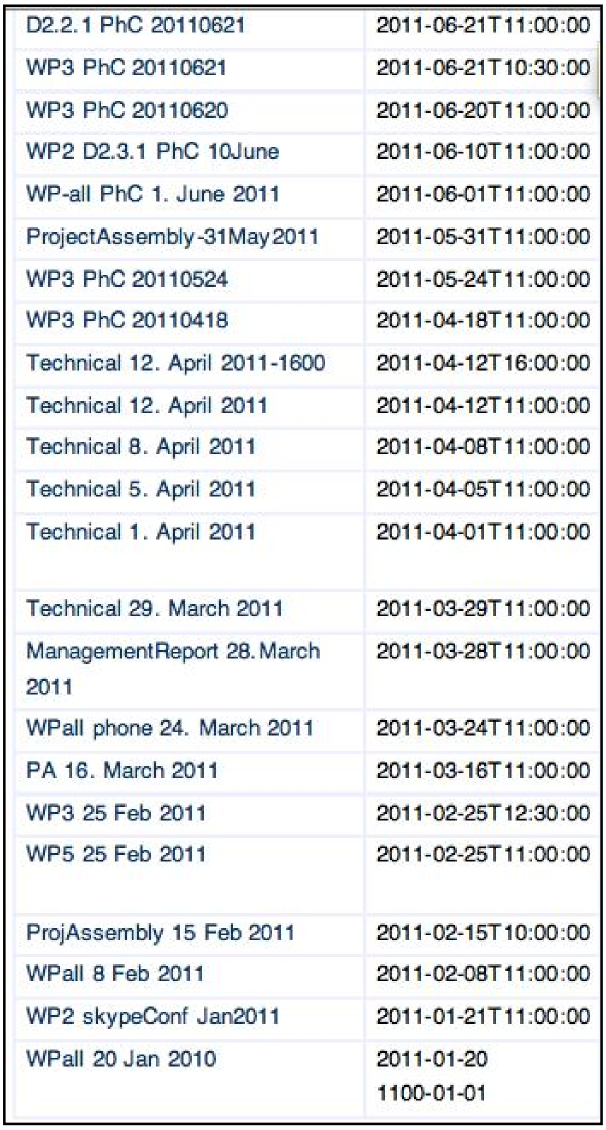
New project coordination has been decided in May 2011. MAS would take the administrative part of the coordination including correspondence to internal agreement mentioned in the Annex I to the JU Artemis Grant Agreement, while SESM would continue taking care of the technical part of the coordination. Official acceptance of PC change has been communicated by Project Officer on 5 August 2011.

5.3 Changes in the consortium

Greek partner ISD is withdrawn from the project. It was announced by them during Project Assembly phone conference on 15 February 2011.

5.4 Project meetings

Minutes of Meetings as well as corresponding documents are stored at the project official repository BSCW Server (http://bscw.juartemis-pshield.eu) and at Wiki Collaborative Tool (http://pshield.unik.no):



D2.2.1 PhC 20110621	2011-06-21T11:00:00
WP3 PhC 20110621	2011-06-21T10:30:00
WP3 PhC 20110620	2011-06-20T11:00:00
WP2 D2.3.1 PhC 10June	2011-06-10T11:00:00
WP-all PhC 1. June 2011	2011-06-01T11:00:00
ProjectAssembly-31May2011	2011-05-31T11:00:00
WP3 PhC 20110524	2011-05-24T11:00:00
WP3 PhC 20110418	2011-04-18T11:00:00
Technical 12. April 2011-1600	2011-04-12T16:00:00
Technical 12. April 2011	2011-04-12T11:00:00
Technical 8. April 2011	2011-04-08T11:00:00
Technical 5. April 2011	2011-04-05T11:00:00
Technical 1. April 2011	2011-04-01T11:00:00
Technical 29. March 2011	2011-03-29T11:00:00
ManagementReport 28. March 2011	2011-03-28T11:00:00
WPall phone 24. March 2011	2011-03-24T11:00:00
PA 16. March 2011	2011-03-16T11:00:00
WP3 25 Feb 2011	2011-02-25T12:30:00
WP5 25 Feb 2011	2011-02-25T11:00:00
ProjAssembly 15 Feb 2011	2011-02-15T10:00:00
WPall 8 Feb 2011	2011-02-08T11:00:00
WP2 skypeConf Jan2011	2011-01-21T11:00:00
WPall 20 Jan 2010	2011-01-20 1100-01-01

Table 1 – Project meetings

5.5 Project planning and status

The project is delayed. A proposal of seven months of extension has been sent to the Project Officer on 29.03.2011 and accepted.

5.6 Impact of deviations

The impact of this deviation from the original plan is not marginal. With this deviation the consortium get extra initial time to deeply investigate the technological issues of this project and to select appropriate methodology for modelling SPD composability of ESNs.

Moreover, the impact of this deviation introduced an extra reporting period in September 2011.

5.7 Changes to the legal status

Spanish partner ESI changed its official name to TECNALIA. SELEX Communications and ELSAG DATAMAT joined and changed their official name to SELEX ELSAG.

5.8 Project website

- pSHIELD project website is available at address:
  http://www.pshield.eu
  It contains general project information, public deliverables, and is used for information, news and promotion of the project. The service is provided by SESM.

- Document Repository is available at address:
  http://bscw.juartemis-pshield.eu
  The access to repository is limited only to authorised persons. The service is provided by THYIA.

- Collaborative Tool is available at address:
  http://pshield.unik.no
  Semantic Media Wiki service is used by consortium for collaboration and day-to-day work. It allows on meetings and phone conferences planning and wiki style discussion on technical problems. The service is provided by CWIN.

5.9 Dissemination and exploitation activities

pSHIELD dissemination and exploitation activities are reported in §1 of this report.

5.10 Co-ordination activities

During the analysed period necessary co-ordination actions were taken. In particular a physical meeting and many phone conferences listed above were organised. Also dissemination and exploitation tasks listed above were done. Contact and exchange of information between partners was provided on daily basis by means of email, phone calls and mail.

6 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 § 3 and related beneficiaries forms.

Table 3 – Person-Month Status Table

Table 3. Person-Month Status Table																			
Contract N. 100204																			
Acronym: pSHIELD																			
Period: 01/01/2011-30/06/2011																			
		Total	SESM	ASTS	ED	ETH	SCOM	TRS	UNIGE	UNIROMA1	AS	TECNALIA	MGEP	ATHENA	HAI	CWIN	MAS	THYIA	CS
Work package 1:	Actual WP total	**19,88**	10,00	1,00	2,40	1,50	1,50	0,25		1,20	0,50		0,13				0,50	0,00	0,90
Management	Planned WP total	**27,78**	15,00	1,00	3,00	2,00	1,50	0,25		2,00	0,50		0,13				0,00	1,50	0,90
Work package 2:	Actual WP total	**39,10**	2,00	9,00	8,00	12,00	0,30					2,30		0,00	3,00	1,50		0,00	1,00
SPD Metrics, requirements and system design	Planned WP total	**54,10**	3,00	10,00	8,00	12,00	0,30					2,30		3,00	3,00	1,50		10,00	1,00
Work package 3:	Actual WP total	**57,70**	10,00			33,00					8,50			0,00		2,50	0,50	0,00	3,20
SPD Node	Planned WP total	**80,00**	15,00			42,00					7,00			2,00		2,50	1,00	7,00	3,50
Work package 4:	Actual WP total	**22,60**					10,50		7,00			0,10	3,00	0,00				0,00	2,00
SPD Network	Planned WP total	**18,10**					9,00		3,00			0,10	2,00	0,50				0,50	3,00
Work package 5:	Actual WP total	**51,70**			24,10			5,50		11,60						2,00	1,00	0,00	7,50
SPD Middleware & overlay	Planned WP total	**68,30**			26,50			5,50		22,00						3,00	0,00	1,30	10,00
Work package 6:	Actual WP total	**31,75**	0,00	20,75	5,00	2,00	0,50									2,50	0,50		0,50
Platform integration, validation & demonstration	Planned WP total	**61,00**	2,00	39,00	8,00	4,00	0,50									2,50	0,50		4,50
Work package 7:	Actual WP total	**7,20**	1,00	2,00	1,00							0,20	0,40			0,50	1,00	0,00	1,10
Support activities	Planned WP total	**6,75**	1,00	2,00	2,00							0,20	0,25			0,00	0,00	0,20	1,10
	Actual total	**229,93**	**23,00**	**32,75**	**40,50**	**48,50**	**12,80**	**5,75**	**7,00**	**12,80**	**9,00**	**2,60**	**3,53**	**0,00**	**3,00**	**9,00**	**3,50**	**0,00**	**16,20**

Tables 3.1 – Personnel, Subcontracting And Other Major Direct Cost Items

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SESM FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 2, 3, 7	Personnel costs		107.892,70€		107.892,70€	Internal staff
3	Subcontracting		4.003,63€		4.003,63€	Consultancy
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs		4.161,31€		4.161,31€	Travel costs
TOTAL DIRECT COSTS[28]			116.057,64€		116.057,64€	
TOTAL INDIRECT COSTS			53.946,35€		53.946,35€	Overhead for personnel costs (rate 50%)

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ASTS FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 2, 6, 7	Personnel costs		140,905.48	37,980.37	178,885.85	Salaries of 7 engineers and 5 senior engineers.
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS29			140,905.48	37,980.37	178,885.85	
TOTAL INDIRECT COSTS			70,452.74	18,990.18	89,442.92	*Overhead rate 50% of personnel costs*

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

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

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ELSAGDATAMAT FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,5,6,7	Personnel costs		€ 92.406		€ 92.406	15,99 PM for 3 senior researchers and 2 analysts
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS[30]			€ 92.406		€ 92.406	
TOTAL INDIRECT COSTS			€ 46.203		€ 46.203	*Overhead rate 50% of personnel costs*

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ETH FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 2, 3	Personnel costs	0	90000 €	20000 €	110000 €	Salary of engineers involved in research, design and development activities. Salary of personnel involved in management activities.
	Subcontracting	0	0	0	0	
	Remaining direct costs	0	0	0	0	
TOTAL DIRECT COSTS[31]		0	90000 €	20000 €	110000 €	
TOTAL INDIRECT COSTS		0	45000 €	10000 €	55000 €	Overhead for personnel costs (rate 50%)

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

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

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SCOM FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
2, 4	Personnel costs		71680€		71680€	
	Subcontracting		51000€		51000€	Development of embedded experimental platform.
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS[32]			122680 €		122680 €	
TOTAL INDIRECT COSTS			35840 €		35840 €	*overhead rate 50% of personnel costs*

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TRS FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 5	Personnel costs		*3.905,26 €*	*4.728,67 €*	*8.633,93 €*	*Salaries of 2 senior systems engineer and one director for a total of six months*
	Subcontracting					
5	Consumables		*1.000,00 €*	*1.000,00 €*	*2.000,00 €*	*Programming & simulation license OS SW*
	Major cost item 'Y' ………..					
5	Remaining direct costs					
TOTAL DIRECT COSTS[33]			*4.905,26 €*	*5.728,67 €*	*10.633,93 €*	
TOTAL INDIRECT COSTS			*1.952,63 €*	*2.364,34 €*	*4.316,97 €*	*Overhead rate 50% of personnel costs*

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

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

Table 3.1 Personnel, subcontracting and other major Direct cost items for Beneficiary UNIGE for the period 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
4	Personnel costs		34000.00 €		34000.00 €	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: 2 PM Full Professor 3 PM Assistant Professor 3 PM PhD
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS[34]			34000.00 €		34000.00 €	
TOTAL INDIRECT COSTS			13260.00 €		13260.00 €	overhead rate 39% of personnel costs

Table 3.1 Personnel, subcontracting and other major Direct cost items for Beneficiary UNIROMA1 for the period 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,5	Personnel costs		€ 93.475,00		€ 93.475,00	12,8 PM for 7 professors and 7 researcher
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs (Adjustment to previous period)		€ 3.784,00		€ 3.784,00	Some labour rates have been revised
TOTAL DIRECT COSTS[35]			€ 97.259,00		€ 97.259,00	
TOTAL INDIRECT COSTS			€ 48.629,50		€48.629,50	overhead rate 50% of personnel costs

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

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

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY AS FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 3	Personnel costs		36.565,79 €		36.565,79 €	Salaries for project manager and project engineer
	Subcontracting		0			
	Major cost item 'X'		0			
	Major cost item 'Y' ………..		0			
	Remaining direct costs		0			
TOTAL DIRECT COSTS[36]			36.565,79 €		36.565,79 €	
TOTAL INDIRECT COSTS			7.313,16 €		7.313,16 €	*overhead rate 20% of personnel costs*

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TECNALIA FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP2, WP4, WP7	Personnel costs		16.386,30 €		16.386,30 €	Salaries for 2,6 p/m
	Subcontracting					
	Major cost item 'Travel'					
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS[37]			16.386,30 €		16.386,30 €	
TOTAL INDIRECT COSTS			3.277,26 €		3.277,26 €	*overhead rate 20% of personnel costs*

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

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

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY MGEP FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
WP1, WP4, WP7	Personnel costs		18073.6€		18073.6€	Salary researchers
	Subcontracting					
	MEMSIC Wireless Sensor Network. Professional kit wirth Mote Runner		2348€		2348€	
	Major cost item 'Y' ………..					
	Remaining direct costs					
TOTAL DIRECT COSTS[38]			20421,6€		20421,6€	
TOTAL INDIRECT COSTS			3614.72€		3614.72€	20% of personnel costs

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY HAI FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
2	Personnel costs		18.900 €		18.900 €	Salaries (3PMs)
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ………..					
	Remaining direct costs		37,95 €		37, 95 €	Hosting WP2 partial meeting
TOTAL DIRECT COSTS[39]			18.937,95 €		18.937,95 €	
TOTAL INDIRECT COSTS			994,14 €		994,14 €	5,26% of personnel costs

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

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

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY CWIN FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
2,3, 5, 6,7	Personnel costs		82.848 €		82.848 €	Salary
	Subcontracting					
	Remaining direct costs		4.531 €		4.531 €	Equipment costs
TOTAL DIRECT COSTS			87.379 €		87.379 €	
TOTAL INDIRECT COSTS						

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY MAS FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,3,5,6,7	Personnel costs		€ 26.214		€ 26.214	Salary for researchers
	Subcontracting					
	Other direct costs					
	Remaining direct costs					
TOTAL DIRECT COSTS			€ 26.214		€ 26.214	
TOTAL INDIRECT COSTS						

TABLE 3.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY CS FOR THE PERIOD 01/01/2011 – 30/06/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3,4,5, 7	Personnel costs		€ 42.394,08		€ 42.394,08	This has corresponded to the full resources used within the scope of the pSHIELD project during this reporting period.
	Subcontracting					
1,2	Travel costs		€ 2.492,63		€ 2.492,63	These costs have been incurred during CSW attendance at all the physical meetings held during the period and any costs incurred during Project Management and dissemination activities.
	Remaining direct costs					
TOTAL DIRECT COSTS[40]			€ 44.886,71		€ 44.886,71	
TOTAL INDIRECT COSTS			€ 8.478,82		€ 8.478,82	20% of personnel costs

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

7 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.

7.1 Certificates

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