PROJECT PERIODIC REPORT

eement 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 01.07.2011 to 31.12.2011**

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

Dr. Josef Noll (MOVATION)

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: 08/02/2012

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

Due date of deliverable: 29th February 2012
Actual submission date: 8th February 2012

Start date of project: 1st June 2010 Duration: 19 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	08/02/2012	
All partners contribute			
Reviewed by			
Name	**Company**		
Antonio Di Marzo	SESM	23/02/2012	
Approved by			
Name	**Company**		
Josef Noll	MOVATION		

Modification History		
Issue	**Date (DD/MM//YY)**	**Description**
01	10/02/2012	Minor changes at page 70
02	23/02/2012	A new section “Justification of cost deviations” has been added

Contents

Figures

Tables

Acronyms

AC	Alternating Current
AES	Advanced Encryption Standard
A-FSK	Audio Frequency Shift Keying
API	Application Programming Interface
CR	Cognitive Radio
DC	Direct Current
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ESs	Embedded Systems
ESD	Embedded System device
ESNs	Embedded System Networks
FPGA	Field Programmable Gate Array
FPSL	Free Space Path Loss
GPS	Global Positioning System
GUI	Graphical User Interface
HW	Hardware
ICT	Information Communication Technology
ID	Identifier
IDS	Intrusion Detection System
KETs	Key Enabling Technologies
MAC	Media Access Control
MHz	Mega Hertz
M2M	Machine to Machine
NMP	Nano /Micro /Personal
OSGI	Open Service Gateway Initiative
OWL	Web Onthology Language
PA	Project Assembly
PhC	Phone Conference
PPR	Project Periodic Report
R&D	Research & Development
RSA	Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman (cryptographic algorithm)
SCADA	Supervisory Control And Data Acquisition
SDR	Software Defined Radio
SINAD	SIgnal-to-Noise And Distortion ratio
SotA	State of the Art
SPD	Security Privacy Dependability
SW	Software
TA	Technical Annex
TMC	Technical Management Committee
TPM	Trusted Platform Module
UML	Unified Modelling Language
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuits
XML	eXtensible Markup Language

WP	Work Package
WSN	Wireless Sensor Network

1 Publishable summary

1.1 Summary

pSHIELD was a pilot project co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on applying and prototyping security, privacy, and dependability (SPD) features within the context of Embedded Systems. The pilot project prepared initial investigations to be enhanced with R&D activities through the main research project nSHIELD. pSHIELD investigated and validated 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 developed **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 approached 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 was documented through in total 19 public deliverables. Technology prototypes were established, including FPGA-based power nodes and cognitive radios for embedded systems. Middleware applications showed the composability of SPD for wireless sensor networks. Real-life pilots such as rail monitoring were established on the Italian and Norwegian railway network.

Through these prototypes pSHIELD demonstrated composable security, and provided a first view on the SHIELD architectural framework. Though market applicability is still some 3-5 years ahead, 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 pilot had the main focus on the development of technologies for embedded sensors and the middleware to provide interoperability and composability, the system aspects will be more clearly addressed through the SHIELD project.

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 are 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. The pilot demonstrated innovative concepts, established a modular, composable, and dependable architectural framework.

Through the introduction of a SPD **metrics** the overall SPD level is improved in any specific application domain, with minimum engineering effort.

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, the project members estimate an overall 30% cost reduction for a full SHIELD oriented design methodology.

The SHIELD consortium comprises 4 manufacturers and system integrators (ASTS, SE, ETH, HAI,), 4 universities (MGEP, UNIGE, UNIROMA1, CWIN), 6 SMEs (THYIA, TRS, Tecnalia, AS, CS, MAS) and 2 Industrial R&D organizations (SESM, ATHENA) from 6 European countries. The high involvement of specialized SMEs, skilled universities and research centres created an expert research team and made SHIELD "a worthwhile project, with taxpayer's money well spent."

The pSHIELD project has been a proof of concept for innovative research in the Embedded Systems and SPD domains. In particular it focused and piloted the following key concepts:**Demonstrate composability**: The main novelty is the enabling of the composability of SPD functionalities at different layers and among different technologies. The mechanism behind the composability was based on (i) semantic technologies, focusing on the heterogeneous integration and reasoning functionality, and (ii) middleware technology, focusing on the implementation in real environments..

1. **New technologies:** A sub-set of the SHIELD technologies, such as "cognitive communication" and "SPD-based power node" are the very first significant examples of SPD features for Embedded Systems.
2. **Modularity and expandability:** The SHIELD framework, in order to perform composability, makes use of (i) the semantic description of components and (ii) proper adapters and proxies that make a generic device, a SHIELD-enabled device. By doing so, the expandability is assured by design (for a new component, it is sufficient to provide a semantic description and a proper adapter, to become part of SHIELD) and the modularity, as expressed in the Technical Annex, is preserved by foreseeing three different classes of (independent) adapters for the three different layers.
3. **Innovative, modular, composable, expandable and high-dependable architectural framework:** the pilot project includes, in its majour achievements, the design of the SHIELD architectural framework in a formal (UML) language, with a clear identification of the SHIELD adapters for modular, expandable and high dependable composability. This is the first instance of such innovative architecture in the context of embedded systems.
4. **Metrics:** metrics are the other biggest novelty in the SHIELD project, since it doesn't exist an integrated way to measure the level of Security, Privacy and Dependability resulting from the composition of atomic functionalities. They have been investigated in the pSHIELD project and a first version, based on a recoginzed standard as Common Criteria, has been used to validate the first basic functionalities of the framework.
5. **Validate the SHIELD integrated system in one application scenario:** the pilot project validated key SPD features by means of a set of integrated prototypal demonstrator, mainly

addressing SPD issues in the specific railways application scenario (freight trains transporting hazardous material).

1.2 Main results achieved

The pilot project has demonstrated that, by adequately composing devices and innovative (atomic) functionalities (like dependable power supply or cyphering), it is possible to create a vertical framework that address security, privacy and dependability (SPD) issues in a specific scenario. In particular different SPD functionalities have been demonstrated through the following pilot prototypes.

FPGA Power node prototype (SPD): with this prototypal demonstrator, made by real hardware and software technologies, the following SPD functionalities have been achieved: SPD metrics, Self recovery from hardware transient faults (through fault injection), Auto reconfiguration, Data encryption, Provision of security and privacy services, Hardware data encryption/decryption

Cognitive Radio prototype (SPD): this prototypal demonstrator, composed by a real cognitive radio platform coupled with a realistic emulator, the following SPD functionalities have been achieved: Threats tolerant transmission

Middleware prototype for composability (SPD): this prototypal demonstrator has integrated a working middleware, with a working reasoning engine for SHIELD metrics elaboration, into real embedded devices performing cyphering tasks. The results has been the achievement of the following functionalities: SPD Audit, Cryptographic Support, Identification and Authentication, Protection of the SPD functionalities, Security Management

Heterogeneous Platform prototype (SPD): this real life prototypal demonstrator, integrated in a real environment with the support of the Norwegian railways Wagon, allowed the consortium to implement the following SPD functionalities: Auto start up on power failure, Auto reconfigurable on software failure, Auto synchronization on software failure, End-to-end secure communication, Mal-user detection, Access control for accessing sensor data

Rail car monitoring system (SPD): last, but not least, this prototypal demonstrator, developed with the support of the Italian Railways authority, has been based on the integration of real hardware into a rail car and the proper configuration of these technologies to perform the following SPD functionalities: Intrusion awareness, fault-tolerance, data redundancy and diversity

All the above mentioned functionalities, relevant on an SPD perspective in the railways application scenario, have been obtained by the composition or the integration of the SHIELD technologies developed in the scope of the project.

The work was 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.

All deliverables expected for WP2 were completed.

Clearly significant and tangible results are:

- The application scenario requirements
- The requirements of the overall SHIELD system for each SPD technology, for each layer
- High level, architectural, interface and performance requirements
- Refinements of the all requirements and specifications made on the feedback from WP3, WP4, WP5 and WP6 prototypes developments
- SPD composition algebra and decomposition of the SPD attributes is proposed
- Two complementary methods "Castel" and "Security Assurance" represent basic techniques for development of SPD metrics composition for the prototypes and the scenario selected and demonstrated
- Innovative SPD system solutions for the future standards for the interoperation of nodes and systems
- Clear guidelines for the prototype development in WP3, WP4, WP5 and WP6 (providing support to the validation phase)
- A coherent, composable and modular architecture for a flexible distribution of SPD information and functionalities between different ESs while supporting security and dependability characteristics
- The resulting architecture is reconfigurable offline, meaning that mechanisms have to be provided to the designer for enabling/disabling nodes in order to tailor the overall system to his needs
- Intra-layer and inter-layer interfaces have been defined in the system architecture to ensure the correct communication among the different SPD modules.

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.

All deliverables expected for WP3 were completed.

Clearly significant and tangible results are:

- Based on developed conceptual pSHIELD SPD Node Layer model the Power Node Prototype was designed and built
- Development of SW/HW framework based on Xilinx development board
- Improvement of pSHIELD Node Adapter blocks: pSHIELD Interface and SPD Node Status
- Improvement of pSHIELD Node Adapter block: Security and Privacy based on hardware data encryption/decryption
- Improvement of pSHIELD Node Adapter block: Dependability based on reconfigurable application bit-stream
- Improvement and tests of application block: A-FSK Demodulator code
- In the frame of demonstrator preparations, the data acquisition FPGA board was developed to provide the main FPGA Power Node Prototype with encrypted and A-FSK modulated data from the field
- 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
- SotA solutions in the field of secondary power supply source to guarantee the correct system operation
- Design of two different protection circuits for a power supply (DC). One of them includes a solution to plug/unplug different sub-systems and a current sensor to monitor power consumption
- Manufacture of both protections boards. Several tests have been carried out in order to ensure that these protections can avoid damages into the system. The protection board which allows to control and monitor power consumption has been tested in an embedded wireless platform
- Development of iPhone complementary solution
- The micro/nano node types have been integrated into the Telenor platform where privacy and dependability have been demonstrated. Security (man in the middle attack) has been targeted on the micro node (Sun Spot)
- Design of two different protection circuits for a power supply (AC) following the normative EN/60950-1
- Design of an autonomy power supply system based on fuel cells, solar panels and turbines to feed continuously a system up to 500W and ensure its autonomy during ten days if the energy harvesting system fails
- Manufacture of two different protection boards based on thermal fuse varistors or varistors and a gas discharge. Several tests have been carried out in order to ensure that these protections can avoid damages into the system
- Real-world adaptations of "trusted boot" and "fail-safe" operations have been added to the power node
- Integration of sensor platform and interworking with the Shepherd platform
- Integration of AES Rijndael algorithm and evaluation of some code optimisations in an embedded wireless platform.

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.

All deliverables expected for WP4 were completed.

Clearly significant and tangible results are:

- New technologies enabling smart SPD driven transmissions have been identified. In particular, some strategies supporting the cognitive radio (CR) paradigm have 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
- pSHIELD simulator development: the scenario consists in a number of entities (agents) carrying a mobile device which is able to transmit and receive data at 3 different frequencies (namely 900, 1800 and 1900 MHz) to a centralised control centre
    - The agents move randomly throughout a radio-disturbed environment, where randomly placed jammers emit a disturbing signal
    - The jammers can be either fixed or moving and their emitted signal follows the Rayleigh distribution with fixed parameters. Fixed jammers positions and characteristics are stored in an XML file, which is loaded in the setup stage together with the map of the ground
    - The mobile devices periodically send a single radio data to the control center, where a running cognitive node receives and elaborates it. Also, a periodical polling is performed by the agents to question the node, which answers back
    - A slightly different scenario can be also set by introducing a moving jammer: an agent carrying a jamming device can be introduced in the scene. Such an intruder-agent differs from the others as he obviously disturbs communications to the node. Also, he communicates a false GPS survey to the node
    - The radio data reception represents, from the node point of view, the sensing logical block of the cognitive cycle. The agents' mobile terminals are the sensors which monitor the environment sending a radio survey (radio sensors) and a positioning piece of information (GPS sensor)
    - The node then analyzes all the data received from each agent, both singularly and collectively. For each agent, the signal-to-noise and distortion ratio (SINAD) of the received data packet is computed. Also, the relative positions of the agents are compared, on the basis of the datum sent by an agent himself and of the fused data sent by the agents in the sensing range. By means of a voting algorithm, rankings are assigned to the IDs of each agent. The intruder's position and ID are worked out as soon as enough information is gathered, based on such rankings

    - In the decision stage, the SINAD datum is compared to an acceptable (fixed to 10 dB) threshold. If the communication with an agent turns out to be too disturbed, a suitable strategy ST is chosen to schedule a change in frequency transmission
    - The action block provides a change in the state of the system. As already explained, this module implements the active interaction of the system towards the surrounding environment or towards itself: the action of changing frequency is selected based on the strategy ST chosen during the previous step. Such an action is executed on the system itself by means of suitable actuators, namely the agents. Actually, as already pointed out, through a periodical polling, the agents themselves ask the node for information: however this does not change the heart of the matter
    - The detection of the intruder does not trigger a decision and a subsequent action in the cognitive cycle. The information relative to the false agent is simply communicated to an interface. Such an interface could simply be in a control center, or could display data on the mobile devices, thus leaving the decision step under human control. Alternatively, a strategy could be implemented to be learned by the cognitive node in a future perspective
- 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.
- Study of the resource footprint (energy consumption among them) and its impact on performance on some commercially available 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.

All deliverables expected for WP5 were completed.

Clearly significant and tangible results are:

- The formal pSHIELD Semantic Model, realized in OWL language
- The methodology to derive the pSHIELD meta-model
- Inferential engine for composition compliant with the Common Criteria approach
- The implementation, in an open source environment (OSGI), of a working middleware providing the core pSHIELD services
- The interaction of the pSHIELD middleware with external nodes with proper libraries
- The definition of the Security Agent software module implementing the Common Criteria composition
- Analysis of the Policy Based solutions candidates for the pSHIELD implementation
- Simulation assessment on the performance of a policy-based-approach
- Mathematical formulation of the context-aware SPD composition based on the Hybrid Automata theory, supported by Matlab simulations

- Realisation of the integrated demonstrator for WP5 technologies which has been used also as platform for validation in WP6.

The WP5 activities have lead to the design of a coherent and almost complete architecture of pSHIELD Middleware, as well as the preliminary implementation of some of its components (and the validation of the others by means of simulation tools). By doing so, all the involved concepts and objectives have been supported by tangible outputs.

Another significant result is that these outputs perfectly fit the Metrics and requirements defined in WP2 and provide the adequate degree of flexibility to interface with the modules developed (or designed) by WP3 and WP4.

Last, but not least, the obtained results have no constraints with respect to the implementation in real environment, since solutions are i) scalable, ii) technology independent, iii) modular.

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

1. Development of SPD-related software and hardware components;
2. Validation of implemented solution through an iterative and incremental process;
3. Demonstration of the proposed architecture with pilot demonstrators.

All deliverables expected for WP6 were completed.

During the reference period, from the above listed objectives, the first has been met to a satisfactory extent, since several partners have been developing demonstration prototypes. The last two points are subsequent steps, following the registration and planning of separate demo components.

The activities of WP6 in the reference period, without being completed, validate the expectations of tangible results, hopefully reached upon the completion of Demonstration procedure. These activities had the following, clearly significant and tangible results:

- Determination of the content of the pSHIELD Demonstration Platform, presented in Oslo meeting
- Description of a variform and quantitatively efficient group of prototypical demonstrators
- Decision upon the use case environment in the form of freight trains transporting hazardous material
- Demonstration of the usability and transmission of data produced by sensors, in the service of specific use case scenarios as critical infrastructure protection
- Exploration of the platform's synthetic capability and composability, through possible synergies and fusion/cooperation of components.

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

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

All deliverables expected for WP7 were completed.

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 §1.3 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 public 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.

Clearly significant and tangible results for dissemination are:

- A dedicated internal dissemination session has been arranged to improve knowledge sharing, cooperation and synergy
- Seven scientific articles published in high quality conferences in this period
- A PhD thesis was successfully discussed in December 2011. Part of the research carried out during this work is strongly related to pSHIELD concepts. Several others are in the pipeline
- 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 company, the Norwegian Defence Research Establishment (FFI), and the Italian Ferrovie dello Stato.
- pSHIELD consortium was present at **ARTEMIS and ITEA Co-Summit** in Helsinki, Finland on 25-26 October 2011. Latest results of the project through a live prototype were presented.

Industrial exploitation of pSHIELD will focus on the following areas:

- 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.

Exploitation plan has been completed. It represents consortium participants' plans according to the exploitation of project results. It should be highlighted that further development of pSHIELD ideas is expected in new project nSHIELD, so some exploitation results may be achieved as a result of pSHIELD work continuation in frame of nSHIELD project.

1.2.1. Measures on how pSHIELD has reached the scope

The evaluation summarised in the table below represents a self-evaluation of the project, related to the project internal quality measures. The evaluation shows that **pSHIELD has received good results.** Four areas are identified as areas for improvement, while the scope has been sufficiently outlined in a majority of 11 areas.

Aspect of scope	Achieved (-,o,+)	Comment
41A) Has the project delivered a suitable architecture in the early phase of the project?	o	The architecture was outlined only after the first review
41B) Have suitable APIs been defined to ensure interworking?	o	The selected semantic approach for interworking allows handling of heterogeneous components
42A) Have the performed R&D approaches received the result?	+	Technology developments are well under-way
42B) Are the results well in line with the state-of-the-art in research?	+	yes
42C) 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
43A) Is a map of the business ecosystem established?	o	The map has not been explicitly drawn, but key players have been identified
43B) 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
43C) Have initial contacts with playmakers and with a similar projects been established?	+, o	Initial contact with key players is established to the degree that can be expected for a pilot project. Contacts to other projects needs still to be improved
44A) Are key players identified?	+	Yes, ranging from both security domain, energy automation and communication
44B) Is (initial) contact established?	+	yes
44C) Is the scientific dissemination being taken towards both conferences and journals?	+	Yes, papers have been submitted to both conferences and journals
44D) Is the feedback from the scientific dissemination documented?	o	Though feedback was given it was not explicitly documented
44E) Did internal dissemination take place, and did it include hand on experience?	+	Yes, internal dissemination is part of the physical meetings
44F) Does the project have a solid base of basic information through Web pages and public documents?	+	Though being a pilot project, a total of 19 public deliverables have been produced documenting the achievements of the p
44G) Does the project supports collaborative approaches?	+	The project has established a well-functioning collaborative platform, and is using phone conferences to a good extent

Table 1 – Measures on how pSHIELD has reached the scope

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 threats 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 new SPD metrics* which allow fast, standard validations and certification as well as *methods and mechanism to easily design and keep SPD level compliance for 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 were 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.

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 environment. Within the area of hardware development, the project developed a power nodes supporting SPD functionality, and cognitive communication for addressing the SPD challenges related to the physical layer. A semantic overlay allows us to compose the required security level according to the application requirements.

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 as a promising starting point ETSI TS102.690, the "Functional architecture for an M2M platform". 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:

- 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 "off-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. Having successfully developed the sensors system fulfilling the demand of "autonomous operation", the sensor data were successfully integrated into Telenor's M2M Shepherd platform. While privacy (sensor data and access) and dependability (interworking of sensor systems) was demonstrated in Q3.2011, the remaining time was used to extend toward security, especially "replay". A demonstration of this functionality is moved towards nSHIELD
- Installation of a pSHIELD Sensor Network was performed with the Italian Railway provider, with a successful installation in Q3.2011
- Further industrial actors are identified, namely ABB and the Norwegian Defence Research Establishment (FFI). Workshops were performed to discuss and to establish the potential for pSHIELD results
- Communication with ABB, resulting in an invitation to the Industrial Embedded System Workshop (19.-20. October 2011) in Trondheim. Main focus is on the "measurable security" for embedded systems. The main feedback from this collaboration is that industrial actors focus on their own security solutions, and that a commonly identified security measure across heterogeneous platforms is seen as a future option.
- FFI would like to collaborate, and expects to establish a strategic collaboration in this area
- SIMlink analyses how the technology can be used to support home appliances in a secure way, e.g. heat control systems (in collaboration with Danfoss)

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. The second period showed an increase of the scientific dissemination with in total eight papers, out of which one paper was accepted as a Journal Paper. During the third period of reporting, other **seven papers** were published or accepted for publication:

- Mariana Esposito, Inaki Eguia, Francesco Flammini, Alfio Pappalardo and Erkuden Rios, "Formalizing SPD metrics for Embedded Systems Multilayer approach" Second

Eastern European and Mediterranean Software Process Improvement Conference (EuroMed SPI II), Zamudio, Spain, October 6-7, 2011.

- Josef Noll, "Security, Privacy and Dependability in the Internet of Things (IoT)", WWRF#27, invited paper to WG7, 18.-20. October 2011
- Josef Noll, Zahid Iqbal and Mohammad M.R. Chowdhury, "Integrating context- and content-aware mobile services into the cloud", CWI/CTIF seminar on Mobile Cloud Computing and wireless applications, 24.-25. October 2011, Aalborg University in Copenhagen
- 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.
- S. S. Alam, L. Marcenaro and C. Regazzoni, "Opportunistic Spectrum Sensing and Transmissions", Cognitive Radio and Interference Management: Technology and Strategy, IGI-Global, 2012.
- Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crowdroid: behavior-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM. ISBN 978-1-4503-1000-0.

In total six PhD students have dedicated their research work to pSHIELD. The following PhD thesis has been finished in December 2011:

- Sarfraz Alam, "Secure interworking of sensor systems in heterogeneous business environments", PhD thesis.

1.3.4 Contribution to workshops and exhibitions

In this last period of the project, pSHIELD has been presented at the following event:

- ARTEMIS and ITEA Co-Summit in Helsinki, Finland on 25-26. October 2011. Latest results of the project were presented through a live prototype.

A complete overview over all dissemination events is available at the public Web page http://www.pshield.eu and our Wiki http://pshield.unik.no/

---------- END of PUBLIC part ----------

2 Project objectives for the period

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 **D2.1.2, D2.2.2** and **D2.3.2**.

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 the objectives have been reported in **D3.1, D3.2, D3.3** and **D3.4.**

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 the objectives have been reported in **D4.1** and **D4.2**.

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 the objectives have been reported in **D5.1, D5.2, D5.3** and **D5.4**.

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

1. Development of SPD-related software and hardware components;
2. Validation of implemented solution;
3. Demonstration of the proposed architecture with pilot demonstrators.

The results of the objectives have been reported in **D6.1, D6.2, D6.3** and **D6.4.**

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

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

The results of the objectives have been reported in **D7.1.2** and **D7.2.1**.

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), SE (ex ED) (8PMs), ESI (2PMs), ETH (12PMs), HAI (9PMs), SE (ex 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), SE (ex 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), SE (ex SCOM) (2.3, reviewer), THYIA (T2.1, T2.2, T2.3, involved almost in all targeted objectives).
Overall summary for WP2:

- Targeted objective for D2.1.2 are reached up to 100%.
  - As major objective in this task:
    - ✓ 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
- Targeted objective for D2.2.2 are reached up to 100%.
  - As major objective in this task:
    - ✓ The definition of proper SPD metrics to assess the achieved SPD level of each layer (node, network, middleware and overlay), as well as of the overall system
- Targeted objectives for D2.3.2 are reached up to 100%.
  - As major objective in this task:
    - ✓ The definition of SHIELD system architecture. Identification of the SPD layers functionalities, their intra and inter layer interfaces and relationships

3.1.2 Significant and tangible results

Clearly significant and tangible results are:

- Tangible results for D2.1.2
  - As major achievements in this task:
    - ✓ The application scenario requirements
    - ✓ The requirements of the overall SHIELD system for each SPD technology, for each layer
    - ✓ High level, architectural, interface and performance requirements
    - ✓ Refinements of the all requirements and specifications are made on the feedback from WP3, WP4, WP5 and WP6 prototypes developments
- Tangible results for D2.2.2
  - As major achievements in this task:
    - ✓ SPD composition algebra and decomposition of the SPD attributes is proposed

- ✓ Two complementary methods “Castel” and “Security Assurance” represent basic techniques for development of SPD metrics composition for the prototypes and the scenario selected and demonstrated
- ✓ Innovative SPD system solutions for the future standards for the interoperation of nodes and systems
- ✓ Clear guidelines for the prototype development in WP3, WP4, WP5 and WP6 (providing support to the validation phase)

- Tangible results for D2.3.2
  - As major achievements in this task:
    - ✓ A coherent, composable and modular architecture for a flexible distribution of SPD information and functionalities between different ESs while supporting security and dependability characteristics
    - ✓ The resulting architecture has to be reconfigurable, offline, meaning that mechanisms should be provided to the designer for enabling/disabling nodes in order to tailor the overall system to his needs. Furthermore, fault diagnosis and fault recovery have to be addressed both in hardware and software layers
    - ✓ Intra-layer and inter-layer interfaces should be defined in the system architecture to ensure the correct communication among the different SPD modules.

Related project taken in considerations are: **CESAR** (pSHIELD participants: ASTS, CS, SE (ex ED), HAI, and ATHENA), **EMMON** (pSHIELD participants: CS and SESM), **IMSK** (pSHIELD participants: SE (ex 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

3.2.1 Progress towards objectives

Reporting period from the 01.07.2011 to the 31.12.2011.

Work Package 3 according to initial Technical Annex starts from month 1 and lasts until month 11 of the project. 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 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 on Technical Annex, requirements and specifications defined as WP2 output, and maintaining exchange of information with other WPs. The leader of WP3 is SESM based on the PA decision taken in October 2010.

3.2.2 Significant and tangible results

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

AS works:

- 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
- Search for real solutions available on market that could be considered as nano and micro nodes to estimate the power consumption of this kind of systems
- Search for energy storage systems and power harvesting methods available on market to study the most suitable technology to feed nano and micro nodes
- Design of two different protection circuits for a power supply (DC). One of them includes a solution to plug/unplug different sub-systems and a current sensor to monitor power consumption
- Manufacture of both protections boards. Several tests have been carried out in order to ensure that these protections can avoid damages into the system. The protection board which allows to control and monitor power consumption has been tested in an embedded wireless platform

CS works:

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

CWIN works:

- Development of iPhone complementary solution
- Modification of pSHIELD nodes towards security

- Node technologies refinements of software, as a result of life tests
- Results: The micro/nano node types have been integrated into the Telenor platform, privacy and dependability has been demonstrated. Security (man in the middle attack) has been targeted on the micro node (Sun Spot)

Task 3.2 Power node (Task Leader: ETH)

ETH works:

- The activities carried out in this task have been focused on the design of the Power Node, a mobile and rugged high performance embedded node with SPD intrinsic functionalities and on the related demonstrator
- The activities performed in the last semester are:
  - Integration of the Power Node board demonstrator
  - Development of the final version of the Power Node rugged enclosure
  - Power node thermal studies evaluation, test and feedback
- These activities are based on deliverable D2.1.2 Requirements and Specification and on deliverable D2.3.2 Architecture.
- The results obtained are:
  - the test of the second release of the Power Node prototype has been complete.
  - Further activities related to bugs corrections and hw/sw improvements for the second/final version have been performed
  - The thermal studies and rugged enclosure design have been completed
  - The second prototype of Power Node cold-plate based cooling system has been completed
  - The development activities for the demonstrator have been completed and the prototype (without the cooling system) has been presented at the 2nd review in Oslo, September 2011
- The description of the demonstrator and the results obtained during the test and evaluation are presented mainly in D3.1 and D3.3, and also in D6.1, D6.3 and D6.4.

SESM works:

- Works based on outputs of WP2, in particular: D2.1.2 requirements and specification and D2.3.2 architecture
- Based on developed conceptual pSHIELD SPD Node Layer model the Power Node Prototype was designed and build
- Development of SW/HW framework based on Xilinx development board
- The pSHIELD Node Layer blocks in VHDL and C language code, as described in D2.3.2 pSHIELD Architecture
- Improvement of pSHIELD Node Adapter blocks: pSHIELD Interface and SPD Node Status
- Improvement of pSHIELD Node Adapter block: Security and Privacy based on hardware data encryption/decryption
- Improvement of pSHIELD Node Adapter block: Dependability based on reconfigurable application bit-stream
- Improvement and tests of application block: A-FSK Demodulator code

- In the frame of demonstrator preparations, the data acquisition FPGA board was developed to provide the main FPGA Power Node Prototype with encrypted and A-FSK modulated data from the field
- The FPGA Power Node Demonstrator was in between presented at the project 2nd review in Oslo, September 2011
- Results of works on Power Node Prototype are presented in D3.1 and D3.3, but also some results of works were contributed to WP6 deliverables D6.1, D6.3 and D6.4.

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 two different protection circuits for a power supply (AC) following the normative EN/60950-1
- Search for real solutions available on market that could be considered as power nodes to estimate the power consumption of this kind of systems
- Design of an autonomous power supply system based on fuel cells, solar panels and turbines to feed continuously a system up to 500W and ensure its autonomy during ten days if the energy harvesting system fails
- Manufacture of two different protection boards based on thermal fuse varistors or varistors and a gas discharge. Several tests have been carried out in order to ensure that these protections can avoid damages into the system

CWIN works:

- Real-world adaptations of "trusted boot" and "fail-safe" operations have been added to the power node
- Integration of sensor platform and interworking with the Shepherd platform
- Results: Development, integration and successful demonstration

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

AS works:

- Due to AES Rijndael is the cipher algorithm 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 efficiency of the system
- Integration of AES Rijndael algorithm and evaluation of some code optimisations in an embedded wireless platform

CS works:

- Participation in WP3 meetings (phone conferences organised by WP leader)
- In this last period, the proposed work for WP3 was completed with the conclusion of the complementary studies to test the cryptographic algorithms implementation on the

hardware of a micro node (TelosB mote)

- The output of this task was used as input to the work performed in WP6 that exhibited, by means of a physical setup, a cryptographic scheme deployed on a WSN platform, allowing to demonstrate pSHIELD's composability functionality

Status of the deliverables:

All the WP3 deliverables were finalized and submitted. Some delays with reference to initial deadlines had place. Deliverables are available at pSHIELD Wiki deliverables page, while public ones are available at the projects website.

- D3.1 SPD node technologies prototypes (internal M15) – deliverable was finalized according to the schedule, and provided at the pSHIELD 2nd review in September 2011. To maintain the highest quality of project output, some improvements were introduced to the document later on, after actual deadline
- D3.2 SPD nano, micro/personal node technologies prototype report (public M16) – the document was finalized, and actual submission date is the end of January 2012
- D3.3 SPD power node technologies prototype report (public M17) – deliverable was finalized according to the schedule, but some improvements were introduced after actual deadline
- D3.4 SPD self-x and cryptographic technologies prototype report (public M16) – deliverable was finalized according to the schedule, some improvements were introduced after actual deadline

3.3 WP4 SPD Network

3.3.1. Progress towards objectives

New technologies enabling smart SPD driven transmissions have been identified. In particular, some strategies supporting the cognitive radio (CR) paradigm 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.

3.3.2. Significant and tangible results

WP4 SPD Network (Leader: SE (ex 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.

Main efforts in this period have been devoted in the development of a pSHIELD simulator, whose preliminary release was presented at the September review in Oslo.

The scenario consists in a number of entities (agents) carrying a mobile device which is able to transmit and receive data at 3 different frequencies (namely 900, 1800 and 1900 MHz) to a centralized control centre. The agents move randomly throughout a radio-disturbed environment, where randomly placed jammers emit a disturbing signal.

The jammers can be either fixed or moving and their emitted signal follows the Rayleigh distribution with fixed parameters. Fixed jammers positions and characteristics are stored in an XML file, which is loaded in the setup stage together with the map of the ground.

The mobile devices periodically send a single radio data to the control centre, where a running cognitive node receives and elaborates it. Also, a periodical polling is performed by the agents to question the node, which answers back.

A radio data sent by an agent contains the following piece of information:
Position of the agent (x,y) on the mapped ground: this is generated by a trajectories simulator. It simulates a GPS sensor on the mobile device. If a video monitoring of the ground area is available, positioning data coming from a tracker can be possibly fused to GPS data to obtain a better position estimation.

1. Frequency of transmission: this can be chosen among the three available frequencies at the beginning of the simulation
2. Power of the transmitted signal: fixed
3. Power of the signal received from the node: this depends on the distance and it is calculated through FSPL. Also, it can be disturbed by jammers
4. Possibly detected jammers' estimated power: each jammer has a typical radius (coded in the XML configuration file) of influence, inside which the agent can measure its power
5. ID of possible neighbors agents (within a fixed sensing radius).

A slightly different scenario can be also set by introducing a moving jammer: an agent carrying a jamming device can be introduced in the scene. Such an intruder-agent differs from the others as he obviously disturbs communications to the node. Also, he communicates a false GPS survey to the node.

Task	**Partner**	**Progress**	**Indicators**
4.1	SE (ex SCOM)	Study of the SPD network technologies prototypes (contribute to D4.2 Technologies Prototypes Report)	Deliverable 4.2
4.1	UNIGE	Study of the SPD network technologies prototypes (contribute to D4.2 Technologies Prototypes Report)	Deliverable 4.2
4.1	SE (ex SCOM)	Implementation of the demo using the technology prototype	Demo
4.2	UNIGE	Implementation of the demo using the technology prototype	Demo

The radio data reception represents, from the node point of view, the sensing logical block of the cognitive cycle. The agents' mobile terminals are the sensors which monitor the environment sending a radio survey (radio sensors) and a positioning piece of information (GPS sensor).

The node then analyzes all the data received from each agent, both singularly and collectively. For each agent, the signal-to-noise and distortion ratio (SINAD) of the received data packet is computed. Also, the relative positions the agents are compared, on the basis of the datum sent by an agent himself and of the fused data sent by the agents in the sensing range. By means of a voting algorithm, rankings are assigned to the IDs of each agent. The intruder's position and ID are worked out as soon as enough information is gathered, based on such rankings.

In the decision stage, the SINAD datum is compared to an acceptable (fixed to 10 dB) threshold. If the communication with an agent turns out to be too disturbed, a suitable strategy ST is chosen to schedule a change in frequency transmission.

The action block provides a change in the state of the system. As already explained, this module implements the active interaction of the system towards the surrounding environment or towards itself: the action of changing frequency is selected based on the strategy ST chosen during the previous step. Such an action is executed on the system itself by means of suitable actuators, namely the agents. Actually, as already pointed out, through a periodical polling, the agents themselves ask the node for information: however this does not change the heart of the matter.

The detection of the intruder does not trigger a decision and a subsequent action in the cognitive cycle. The information relative to the false agent is simply communicated to an interface. Such an interface could simply be in a control center, or could display data on the mobile devices, thus leaving the decision step under human control. Alternatively, a strategy could be implemented to be learned by the cognitive node in a future perspective.

Task	Partner	Progress	Indicators
4.2	MGEP	Completion of the 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	Completion of the study of 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	Completion of the study of anomaly detection systems.	Publication
4.2	UNIGE	Completion of the studies on 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 to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly.	Publication
4.2	CS	Completion of 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.	Deliverable 4.2
4.2	CS	Completion of the preliminary studies and discussions regarding the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices	Deliverable 4.2

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 behavior could be considered as an evidence of an intrusion. **Hybrid IDS, where the system is based on 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, modeling normal behavior 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 neighbors. The protection of the nodes is also necessary so it is high recommended to implement a local agent for the nodes able to analyze 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 assess 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, CS'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.

The results of Task 4.2 activities are formalised in Deliverable 4.2 "SPD network technologies prototypes report".

3.4 WP5 SPD Middleware & Overlay

3.4.1. Progress towards objectives

WP5 (SELEXELSAG (SE) 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 (SE Leader), and Task 5.4 Overlay monitoring and reacting system by security agents (SE 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)

In this last period the final objectives of pSHIELD project, with respect to WP5, have been completely met. The main objectives were:

1. Define a semantic to describe the pSHIELD system, to adequately manage metrics and to enable the composability mechanism
2. Define the core services, at Middleware layer, to realize the composability of SPD functionalities
3. Study and define proper mechanisms to drive the composability, by means of:
   a. Policies
   b. Control algorithms
4. Put all these objectives together to provide a proof of concept of the Composability of SPD functionalities.

All these objectives have been met with significant results that encourage the prosecution of the research in the nSHIELD project towards more challenging objectives (i.e. real implementation, use-case extension, standardization).

Overall summary for WP5:

- Targeted objectives for D5.1 are reached up to 100%
- Targeted objectives for D5.2 are reached up to 100%
- Targeted objectives for D5.3 are reached up to 100%
- Targeted objectives for D5.4 are reached up to 100%

3.4.2. Significant and tangible results

The measurable outcomes for each objective are:

Measurable outcome for objective 1

- The formal pSHIELD Semantic Model, realized in OWL language
- The methodology to derive the pSHIELD meta-model
- Inferential engine for composition compliant with the Common Criteria approach

Measurable outcome for objective 2

- The implementation, in an open source environment (OSGI), of a working middleware providing the core pSHIELD services
- The interaction of the pSHIELD middleware with external nodes with proper libraries
- The definition of the Security Agent software module implementing the Common Criteria composition

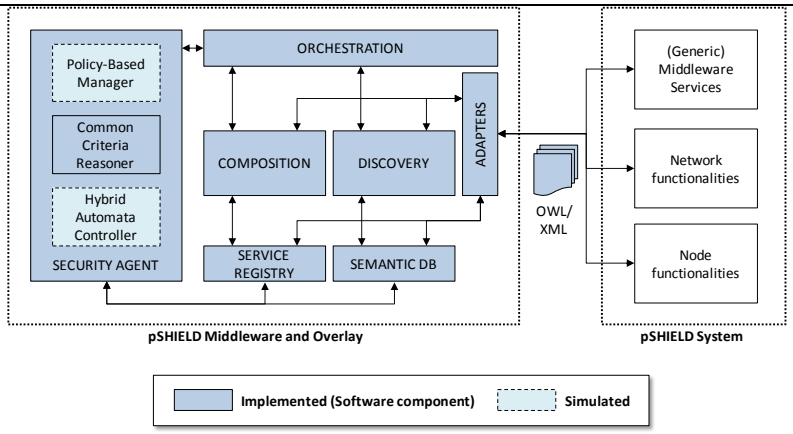
Measurable outcome for objective 3

- Analysis of the Policy Based solutions candidates for the pSHIELD implementation.
- Simulation assessment on the performance of a policy-based-approach
- Mathematical formulation of the context-aware SPD composition based on the Hybrid Automata theory, supported by Matlab simulations.

Measurable outcome for objective 4

- Realization of the integrated demonstrator for WP5 technologies which has been used also as platform for validation in WP6.

As reported in Deliverables D5.x, the WP5 activities have lead to the design of a coherent and almost complete architecture of pSHIELD Middleware, as well as the preliminary implementation of some of its components (and the validation of the others by means of simulation tools). By doing so, all the involved concept and objectives have been supported by tangible outputs. This is summarized in the following figure



Another significant result is that these outputs perfectly fit the Metrics and requirements defined in WP2 and provide the adequate degree of flexibility to interface with the modules developed (or designed) by WP3 and WP4.

Last, but not least, the obtained results have no constraints with respect to the implementation in real environment, since solutions are i) scalable, ii) technology independent, iii) modular.

The Middleware developed in WP5 will be the basis of the ARTEMIS-JU project nSHIELD. Its functionalities will be refined and enriched and possibly transferred into real devices to constitute preliminary prototypes in an exploitation perspective.
Since most of the partners of pSHIELD are involved in nSHIELD too, the information flow is immediate and very effective.

The major exploitation perspective for technologies developed in WP5 is to push for the standardization of the SPD Middleware to obtain a platform that can be used in different context to offer security services (or at least the possibility to compose security services).

Moreover the adoption of the standard Common Criteria should be enforced to increase the validity of the platform and other Security standard should be taken into account too to extend its applicability.

3.5 WP6 Platform integration, validation & demonstration

3.5.1. Progress towards objectives

WP6 aims at:

- Developing SPD-related software and hardware components
- Validating the implemented solution
- Demonstrating the proposed architecture with pilot demonstrators

The distribution of the work done is shared between four Tasks, the outcomes of which are reflected in respective Deliverables.

3.5.2. Significant and tangible results

The status of these four Tasks by the end of the period of reference is as follows:

- **Task 6.1 - Multi-Technology System Developments**, coordinated by HAI, attempts to concentrate all the discrete prototypes developed by partners in the framework of technical development work packages. In this way, pSHIELD demonstration environment is close to be determined, synthesized from the components registered here (D6.1) and the respective equipment, as well as the selected application scenario. Specifically, these prototypes include so far (for the reference period and per presenting partner): Platform for Heterogeneous WSNs + Application Scenario (ASTS), FPGA Power Node (SESM), Cognitive Radio Node (UNIGE), Security integration across heterogeneous platforms (CWIN), Nano-Micro Personal Node Prototype (THYIA) and Middleware prototype for the demonstration of composability (CS). Details for the work of each partner that is not listed right below can be found in the respective document.

- **Task 6.2 - Multi-Technology Validation & Verification**, coordinated by SE was finalized at the end of reference period. It contains the efforts of validation and verification of the SPD features and concepts, integrated on an identified platform for pSHIELD scenario. These efforts correspond to the work of SE, UNIROMA1, TRS, CS and ASTS, shared between the development of pSHIELD Scenario Platform, the Validation and Verification processes (especially for concepts of Middleware and its sub-topics of Overlay, Ontologies and Secure Communication among heterogeneous WSNs) and the description of Tests. Details for the work of each partner that is not listed right below can be found in the respective document.

- **Task 6.3 - Multi-technology Pilot Demonstration** is the task dedicated to the validation of the proposed architecture in the selected industrial application scenario: monitoring of freight trains transporting hazardous material. Also, closing to its end in the reference period, the respective deliverable presents the demonstration capabilities, in the environment of corresponding scenarios and use cases, for a series of demonstrator prototypes. The latter concern the FPGA Power Node Prototype, the Cognitive Radio Node Prototype, the Middleware Prototypes, as well as prototypical implementations of Security integration across heterogeneous platforms and specific Layers. The work has been conducted mainly

by ASTS (task leader), SESM and UNIROMA1. Details for the work of each partner that is not listed right below can be found in the respective document.

- **Task 6.4 - Real world requirements for SPD-based systems**, coordinated by ASTS is the task targeted to guarantee the proposed architecture components to be future-proof, and to support the real-world requirements for industrial operations. The corresponding deliverable involves the aforementioned demonstration prototypes, examined from the view of their interconnection with industrial priorities. The consortium wishes to exploit the knowledge produced by the implementation of prototypes to the direction of discovering the degree of readiness of industrial sectors to adopt a pSHIELD product. The deliverable is completed and the main contributions have been provided by ASTS, SESM, UNIROMA1 and SE with the assistance of CWIN and HAI. Details for the work of each partner that is not listed right below can be found in the respective document.

The activities of WP6 in the reference period, without being completed, validate the expectations of tangible results, hopefully reached upon the completion of Demonstration procedure. These activities had the following outcomes:

- Determination of the content of the pSHIELD Demonstration Platform, presented in Oslo meeting
- Description of a variform and quantitatively efficient group of prototypical demonstrators
- Decision upon the use case environment in the form of freight trains transporting hazardous material
- Demonstration of the usability and transmission of data produced by sensors, in the service of specific use case scenarios as critical infrastructure protection
- Exploration of the platform's synthetic capability and composability, through possible synergies and fusion/cooperation of components

With the pSHIELD project partners of the consortium will have the opportunity to participate in the design of an innovative communication platform, conveying information from sensors to centralized infrastructures, for the management of critical operations or situations. The technological framework refers to Embedded Systems and their utilization in an environment with adequately increased SPD levels during operation. A basic notion and desirable feature of pSHIELD regards the possibilities to abstract components from the platform and create pSHIELD subsystems, depending on the needs of specific applications.

This composability is what partners, especially the industrial ones, wish to, firstly, consolidate and later exploit in the form of a SHIELD prototype. pSHIELD product can be incorporated in individual company business plans or form the basis for a common consortium exploitation plan, that will include implementation of applications in specific business areas.

HAI, for example, will investigate the possibility of embodying pSHIELD exploitation perspectives in its current evolving business plan. Prominent application areas in this plan are Infrastructure

Security and Border Surveillance, having a lot in common with Urban railways protection and Voice/Facial recognition (two of the selected SHIELD application topics). The development of high reliable *security* systems applicable in various aspects of social life, are in the front line of priorities. Cameras and sensors can be used to detect hazardous and illegal actions (e.g. border crossings). The devices usually have to be deployed at remote in between distances and far from the operation centre, on mountainous or harsh terrains, etc. If they are able to be organized, through their heterogeneity, with great composability, enhanced overall situational control and awareness for authorities could be possible.

Another application in the same domain concerns the prevention of natural disasters and their impact in public *safety*. Cameras and thermal sensors are used for the notification of abnormal conditions and derivation of alarms. The critical operations of fire fighting, involves the communication of a number of authorities, from fire and forest inspection departments to local communities, ministries, police and governmental crisis operation centres. Their effective organization, vital in these situations of high emergency, could be assisted with a composable SPD network platform, allowing each part to have access to the kind of information of its specific interest.

pSHIELD is expected to contribute significantly in the implementation of these business plans, since its values and concepts (security, privacy and dependability in the context of embedded systems) are of great importance in this area. Furthermore, the results of demonstration will depict platform capabilities, limits and commercial potentialities, while simultaneously they will guide us to the future research field and improvements.

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 were 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.

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 project developed a power nodes supporting SPD functionality, and cognitive communication for addressing the SPD challenges related to the physical layer. An semantic overlay allows us to compose the required security level according to the application requirements.

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:

- 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. Having successfully developed the sensors system fulfilling the demand of “autonomous operation”, the sensor data were successfully integrated into Telenor’s M2M Shepherd platform. While privacy (sensor data and access) and dependability (interworking of sensor systems) was demonstrated in Q3.2011, the remaining time was used to extend toward security, especially “replay”. A demonstration of this functionality is moved towards nSHIELD.
- Installation of a pSHIELD Sensor Network was performed with the Italian Railway provider, with a successful installation in Q3.2011
- Further industrial actors are identified, namely ABB and the Norwegian Defence Research Establishment (FFI). Workshops were performed to discuss to establish the potential for pSHIELD results.
- Communication with ABB, resulting in an invitation to the Industrial Embedded System Workshop (19.-20. October 2011) in Trondheim. Main focus is on the "measurable security" for embedded systems The main feedback from this collaboration is that industrial actors focus on their own security solutions, and that a commonly identified

security measure across heterogeneous platforms is seen as a future option.

- FFI would like to collaborate, and expects to establish a strategic project in this area.
- SIMlink analyses how the technology can be used to support home appliances in a secure way, e.g. heat control systems (in collaboration with Danfoss)

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. The second period showed an increase of the scientific dissemination with in total eight papers, out of which one paper was accepted as a Journal Paper. During the third period of reporting, other **seven papers** were published or accepted for publication:

- Mariana Esposito, Inaki Eguia, Francesco Flammini, Alfio Pappalardo and Erkuden Rios, "Formalizing SPD metrics for Embedded Systems Multilayer approach" Second Eastern European and Mediterranean Software Process Improvement Conference (EuroMed SPI II), Zamudio, Spain, October 6-7, 2011.
- Josef Noll, "Security, Privacy and Dependability in the Internet of Things (IoT)", WWRF#27, invited paper to WG7, 18.-20. October 2011
- Josef Noll, Zahid Iqbal and Mohammad M.R. Chowdhury, "Integrating context- and content-aware mobile services into the cloud", CWI/CTIF seminar on Mobile Cloud Computing and wireless applications, 24.-25. October 2011, Aalborg University in Copenhagen
- 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.
- S. S. Alam, L. Marcenaro and C. Regazzoni, “Opportunistic Spectrum Sensing and Transmissions”, Cognitive Radio and Interference Management: Technology and Strategy, IGI-Global, 2012.
- Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crowdroid: behavior-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM ’11, pages 15–26, New York, NY, USA, October 2011. ACM. ISBN 978-1-4503-1000-0.

In total six PhD students have dedicated their research work to pSHIELD. The following PhD thesis has been finished in December 2011:

- Sarfraz Alam, "Secure interworking of sensor systems in heterogeneous business environments", PhD thesis.

Contribution to workshops and exhibitions

pSHIELD has been presented at the following event:

- ARTEMIS and ITEA Co-Summit in Helsinki, Finland on 25-26 October 2011. Latest results of the project were presented through a live prototype.

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.

Exploitation plan has been completed. It represents consortium participants' plans according to the exploitation of project results. It should be highlighted that further development of pSHIELD ideas is expected in new project nSHIELD, so some exploitation results may be achieved as a result of pSHIELD work continuation in frame of nSHIELD project.

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

Beneficiary:	SESM
Work Package(s)	WP1 – 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 6.1 Multi Technology System Developments Task 6.2 Multi-Technology Validation & Verification Task 6.3 Multi-technology Pilot Demonstration Task 6.4 Real world requirements for SPD-based systems Task 7.1 Dissemination
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 Project management – 11PM Task 1.2 Liaisons – 5PM Task 2.1 Multi-technology requirements & specification – 0PM Task 2.3 Multi-technology architectural design – 0PM Task 3.2 Power node – 10PM Task 6.2 Multi-Technology Validation & Verification – 5PM Task 6.3 Multi-technology Pilot Demonstration – 4PM Task 7.1 Dissemination – 4PM
Effort actual or spent in this period:	Task 1.1 Project management – 11PM Task 1.2 Liaisons – 5PM Task 2.1 Multi-technology requirements & specification – 0PM Task 2.3 Multi-technology architectural design – 0PM Task 3.2 Power node – 10PM Task 6.2 Multi-Technology Validation & Verification – 5PM Task 6.3 Multi-technology Pilot Demonstration – 4PM Task 7.1 Dissemination – 4PM
% of work completed at the end of the period (indicative):	Task 1.1 Project management – 100% Task 1.2 Liaisons – 100% Task 2.1 Multi-technology requirements & specification – 100% Task 2.3 Multi-technology architectural design – 100% Task 3.2 Power node – 100% Task 6.1 Multi Technology System Developments – 100%

	Task 6.2 Multi-Technology Validation & Verification – 100% Task 6.3 Multi-technology Pilot Demonstration – 100% Task 6.4 Real world requirements for SPD-based systems – 100% 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 during the period.
  - Role of WP3 Leader.
- Task 1.2 Liaisons
  - Continuous studies on projects concerning topics related to pSHIELD.
  - Contacting partners to exchange information on their liaisons.
- Task 2.1 Multi-technology requirements & specification
  - Based on analysis of TA (Annex I) described goals and relevance to Sub-Programme 6 Priority, Industry Priorities and Artemis Targets well designed set of node requirements were described in deliverable D2.1.1 chapter 8 "Node Requirements and Specifications".
  - In discussed period continuous studies on requirements were conducted leading to refinement of requirements in next revision of D2.1.1, that is deliverable D2.1.2 "System Requirements and Specifications – Next Realize".
- Task 2.3 Multi-technology architectural design
  - Based on studies of SotA technologies available on market the generic pSHIELD node architecture were developed following previously prepared D2.1.2 node requirements and specifications.
  - Generic conceptual model of a pSHIELD node were developed 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).
  - In discussed period developed pSHIELD Node Architecture model was refined and presented in deliverable D2.3.2.
- Task 3.2 Power node
  - Continuous works on development of pSHIELD SPD Power Node Prototype hardware and software demonstrating selected pSHIELD node capabilities described by node architecture in D2.3.2.
  - Result:
    - Updated works based "next revisions" of D2.3.2 requirements and specification and D2.3.2 architecture deliverables.
    - Updated works based on endorsed M0.1 and M0.2 documents.
    - Design of Power Node Prototype based on developed conceptual pSHIELD SPD Node
    - Layer model: continuous development of SW/HW framework based on Xilinx development board.
    - Improved implementation of pSHIELD Node Layer blocks in VHDL and C language code.
    - Improved implementation of pSHIELD Node Adapter blocks: pSHIELD Interface and SPD Node Status.
    - Improved implementation of pSHIELD Node Adapter block: Security and Privacy based on hardware data encryption/decryption.
    - Improved implementation of pSHIELD Node Adapter block: Dependability based reconfigurable application bit-stream.
    - Development and implementation of application: FSK Demodulator code.

- Design and development of FSK Modulator hardware and software based on Altera FPGA development board.

- Task 6.1 Multi Technology System Developments
  - Works on development of FPGA Power Node prototype compliant with pSHIELD architecture.
  - The test environment following pSHIELD proposed railway use case was prepared.
  - Specification of pSHIELD Network layer and Middleware layer communication was prepared.
  - Description of the prototype with test environment and pSHIELD interfaces was contributed to deliverable D6.1 "Platform Development Report" to chapter "FPGA Power Node Prototype".
- Task 6.2 Multi-Technology Validation & Verification
  - Works with WP5 partners on development of common data interface for exchange of information with middleware layer.
  - The works are presented in deliverables D6.1 and D6.3.
- Task 6.3 Multi-technology Pilot Demonstration
  - Works on preparation of demonstration of pSHIELD Power Node capabilities.
  - Demonstration of SPD Power Node statuses and metrics, composition capabilities and communication interface.
  - Preparation of several use case scenarios: Node discovery and legacy component integration; Metrics and high performance presentation; Self-reconfiguration; Dependability presentation; Security verification.
  - Description of activities was contributed to deliverable D6.3 "Multi-technology Pilot Demonstrator" to chapter "FPGA Power Node Demonstrator".
- Task 6.4 Real world requirements for SPD-based systems
  - Works on real-life requirements from industrial implementations.
  - Analysis of industry-readiness for pSHIELD-based solutions.
- Task 7.1 Dissemination
  - Exchange of informative materials on the project subject.
  - Preparation and presentation of pSHIELD project at Marie Curie Researchers Symposium, SCIENCE – Passion, Mission, Responsibilities", Polish Presidency of the EU Council, Poster presentation, Warsaw, Poland, 25-27 September 2011.
  - Preparation and presentation of pSHIELD project at ARTEMIS/ITEA2 Co-Summit 2011 Exhibition (with MAS). Poster presentation. pSHIELD project stand, demonstration of SPD prototypes. Helsinki, Finland, 24-26 October 2011.
  - Results: Presentation of project at exhibition, making it recognized by governments and industry representatives.

A summary progress towards objectives.

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

- SESM acts as Technical Project Coordinator (TPC). 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. Meantime the role of Administrative Project Coordinator was moved from THYIA to MAS, anyway SESM acted all the time as TPC.
- 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 SESM took necessary steps to realise project aims. The Nodes requirements were initially defined based on analysis of Annex I (TA) and relevance to Sub-Programme 6 Priority, Industry Priorities and Artemis Targets. They were contributed to deliverable D2.1.1 chapter 8 "Node Requirements and Specifications". In reported period, based on gathered experience, the Node requirements were analyzed and updated in next release of deliverable, that is in D2.1.2.

Based on requirements the pSHIELD SPD Node Architecture was developed and described in D2.3.1, and then updated in D2.3.2 according to last development results. 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.

Based on developed SPD Node architecture the Power Node Prototype was proposed and developed. Implementation of theoretical architecture in real hardware and software allows on verification and validation of proposed pSHIELD concepts. The FPGA Power Node Prototype was introduced in deliverable D3.1 and described in details in deliverable D3.3 "SPD power node technologies prototype report".

Clearly significant and tangible results

- Development of extensive set of Node requirements that exactly follow goals of Annex I. Results updated in deliverable D2.1.2 chapter "Node Requirements and Specifications".
- 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. Contribution updated in D2.3.2 (Node section).
- The first version of pSHIELD Power Node prototype was developed and presented during Consortium Meeting in Rome 12-13.07.2011, and then at the pSHIELD Project 2nd Review in Oslo, 29.09.2011.

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 ARTEMIS/ITEA2 Co-Summit 2011 Exhibition. pSHIELD project stand, demonstration of SPD prototypes. Helsinki, Finland, 24-26 October 2011.

Corrective actions

- 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 role of Administrative Project Coordinator was moved by consortium to Movation AS.
- The Consortium Meeting in Rome 12-13.07.2011 was organized to answer the main project question: how to proceed to succeed pSHIELD.
- The Pre-Meeting in Oslo 28.09.2011 before 2nd Review was organized to allow consortium to discuss next steps in project.

3.7.2. Ansaldo ASTS

Beneficiary:	ASTS
Work Package(s)	WP1 - Project Management WP2 - Scenarios, user requirements and architecture design WP6 - Platform Integration, validation & demonstration WP7 - Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project management Task 1.2 Liaisons Task 2.1 Multi-technology requirements & specification Task 2.2 Multi-technology SPD metrics Task 6.1 Multi-Technology System Developments Task 6.2 Multi-Technology Validation & Verification Task 6.3 Multi-technology Pilot Demonstration Task 6.4 Real world requirements for SPD-based systems Task 7.1 Dissemination Task 7.2 Exploitation
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 Project management: 1 Task 1.2 Liaisons: 1 Task 2.1 Multi-technology requirements & specification: 0,85 Task 2.2 Multi-technology SPD metrics: 1 Task 6.1 Multi-Technology System Developments: 2 Task 6.2 Multi-Technology Validation & Verification: 3,90 Task 6.3 Multi-Technology Pilot Demonstration: 8,75 Task 6.4 Real world requirements for SPD-based systems: 3,29 Task 7.1 Dissemination: 0,75 Task 7.2 Exploitation: 3
Effort actual or spent in this period:	Task 1.1 Project management: 1 Task 1.2 Liaisons: 1 Task 2.1 Multi-technology requirements & specification: 0,85 Task 2.2 Multi-technology SPD metrics: 1 Task 6.1 Multi-Technology System Developments: 2 Task 6.2 Multi-Technology Validation & Verification: 3,90 Task 6.3 Multi-Technology Pilot Demonstration: 8,75 Task 6.4 Real world requirements for SPD-based systems: 3,29 Task 7.1 Dissemination: 0,75 Task 7.2 Exploitation: 3
% of work completed at the end of the period (indicative):	Task 1.1 Project management: 100% Task 1.2 Liaisons: 100% Task 2.1 Multi-technology requirements & specification: 100% Task 2.2 Multi-technology SPD metrics: 100% Task 6.1 Multi-Technology System Developments: 100% Task 6.2 Multi-Technology Validation & Verification: 100% Task 6.3 Multi-Technology Pilot Demonstration: 100% Task 6.4 Real world requirements for SPD-based systems: 100% Task 7.1 Dissemination: 100% Task 7.2 Exploitation: 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) aimed at managing the project.
- Task 1.2
  - Sharing activities with the Technical Management Committee (TMC) and the other partners to promote and improve the project results, in order to ensure a fruitful exchange of knowledge.
- Task 2.1
  - Revision and checking of D2.1.1 document on the basis of the results obtained during the platform integration, validation and demonstration (WP6) according to the railway application scenario.
- Task 2.2
  - Revision and checking of D2.2.1 document, according to the results obtained in the other deliverables;
  - Results: support the identification of metrics required for the SPD measurements, also according to the proposed scenario considered in Task 6.3;
- Task 6.1
  - Analysis on the components of the architecture of the testbed, in order to address the SPD concerns;
  - Drafting of the sections in charge of ASTS.
- Task 6.2
  - Analysis on the integration of different components included in the prototype and tested in the pilot demonstration;
  - Drafting of the sections in charge of ASTS.
- Task 6.3
  - Coordination activities with the other 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;
  - Demonstration of the overall monitoring system, including heterogeneous smart sensors installed in a freight car. The tests have been performed with both stopped and moving car.
- Task 6.4
  - Coordination activities with the other partners to collects the inputs required to define the industrial impact and future-proof of the pilot demonstrator;
  - Identification of the industry-related developments of SPD functionalities, based on industrial experiences.
- 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 several scientific publications;
- Task 7.2
  - Promote among its exploitation of the results achieved, starting with programs dedicated to assessing the impact of the project on your business
  - Activation of programs dedicated to assessing the impact of results explored in the project (regarding SPD requirements and metrics, monitoring platforms and related issues) to encourage their exploitation in the transportation solutions proposed by the company for the freight trains monitoring.

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 have been postponed. In particular the final check of the consistence of the outputs provided in the WP2 has been completed after reaching the final status on WP6. Similarly, the further planned effort in the WP1, WP6 and WP7 has been spent later.
Dissemination activities and exploitation perspectives: ➢ Further dissemination activities regarding the results of project are already planned. The research issues will be further promoted through the participation in conferences and workshops on the topics of the project.

3.7.3. Selex Elsag (ex Elsag Datamat)

Beneficiary:	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 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 July 2011 – 31st December 2011
Effort planned for the period:	**WP1 – 0,6 PM** Task 1.1 – 0,6 PM **WP2 – 0 PM** Task 2.1 – 0,0 PM Task 2.2 – 0,0 PM Task 2.3 – 0,0 PM **WP5 – 12,9 PM** Task 5.1 – 2,5 PM Task 5.2 – 2,5 PM Task 5.3 – 4,4 PM Task 5.4 – 3,5 PM **WP6 – 8 PM** Task 6.2 – 8,0 PM

	WP7 – 1 PM Task 7.2 – 1,0 PM
Effort actual or spent in this period:	**WP1 – 0,6 PM** Task 1.1 – 0,6 PM **WP2 – 0 PM** Task 2.1 – 0,0 PM Task 2.2 – 0,0 PM Task 2.3 – 0,0 PM **WP5 – 12,9 PM** Task 5.1 – 2,5 PM Task 5.2 – 2,5 PM Task 5.3 – 4,4 PM Task 5.4 – 3,5 PM **WP6 – 8 PM** Task 6.2 – 8,0 PM **WP7 – 1 PM** Task 7.2 – 1,0 PM
% of work completed at the end of the period (indicative):	**WP1 – 100,0%** Task 1.1 – 100,0% **WP2 – 100,0%** Task 2.1 – 100,0% Task 2.2 – 100,0% Task 2.3 – 100,0% **WP5 – 100,0%** Task 5.1 – 100,0% Task 5.2 – 100,0% Task 5.3 – 100,0% Task 5.4 – 100,0% **WP6 – 100,0%** Task 6.2 – 100,0% **WP7 – 100,0%** Task 7.2 – 100.0%
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/organization to/of physical meetings and phone conferences; ➢ Preparation of answers to open issues from first review meeting; ➢ Preparation of mid-term and final review meeting. Objectives: manage the project • Task 6.2 ➢ Tests tailoring and test-bed definition for validation and verification of SPD functionalities and concepts	

integrated on a identified platform

- Validation and verification of SPD functionalities composition through the semantic composition representing the medial castle composition method

Objectives: validate SPD functionalities composition on an identified platform

- WP5

In this last period the final objectives of pSHIELD project, with respect to WP5, have been completely met. The main objectives were:

1. Define a semantic to describe the pSHIELD system, to adequately manage metrics and to enable the composability mechanism.
2. Define the core services, at Middleware layer, to realize the composability of SPD functionalities.
3. Study and define proper mechanisms to drive the composability, by means of:
    i. Policies
    ii. Control algorithms
4. Put all these objectives together to provide a proof of concept of the Composability of SPD functionalities.

All these objectives have been met with significant results that encourage the prosecution of the research in the nSHIELD project towards more challenging objectives (i.e. real implementation, use-case extension, standardization).

1. Targeted objectives for D5.1 are reached up to 100%
2. Targeted objectives for D5.2 are reached up to 100%
3. Targeted objectives for D5.3 are reached up to 100%
4. Targeted objectives for D5.4 are reached up to 100%

Significant and tangible results

- The formal pSHIELD Semantic Model, realized in OWL language
- The methodology to derive the pSHIELD meta-model
- Inferential engine for composition compliant with the Common Criteria approach
- The implementation, in an open source environment (OSGI), of a working middleware providing the core pSHIELD services.
- The interaction of the pSHIELD middleware with external nodes with proper libraries
- The definition of the Security Agent software module implementing the Common Criteria composition
- Analysis of the Policy Based solutions candidates for the pSHIELD implementation.
- Simulation assessment on the performance of a policy-based-approach
- Mathematical formulation of the context-aware SPD composition based on the Hybrid Automata theory, supported by Matlab simulations.
- Realization of the integrated demonstrator for WP5 technologies which has been used also as platform for validation in WP6.

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:

- 12th – 13th July, University of Rome "La Sapienza": plenary consortium meeting, ALL
- 21st July – WP5 partners technical meeting, Rome
- 26th July - WP5 partners technical meeting, phone call
- 2nd September, SESM: Technical Phone Call, ALL
- 7th September - WP5 partners technical meeting, Rome
- 15th September, SESM: Technical Phone Call, ALL
- 21st September, SESM: Technical Phone Call, ALL
- 28th September, MAS, consortium meeting for mid-term review preparation – ALL
- 29 th-30th September, MAS; mid-term review meeting - ALL
- 6th October, SESM: Technical Phone Call, ALL
- 20th October- WP5 partners technical meeting, phone call
- 3rd November- WP5 partners technical meeting, phone call
- 24th November, SESM: Technical Phone Call, ALL
- 24th November- WP5 partners technical meeting, phone call
- 14th December, SESM: Technical Phone Call, ALL

3.7.4. Eurotech

Beneficiary:	ETH
Work Package(s)	WP1 - Project management WP3 - SPD node WP6 - Platform integration, validation & demonstration
Task(s)	Task 1.1 Project management Task 3.2 Power node Task 6.4 Real world requirements for SPD-based systems
Period:	1 July 2011 – 31 December 2011
Effort planned in this period:	Task 1.1 Project management: 0,5MM Task 3.2 Power node: 9MM Task 6.4 Real world requirements for SPD-based systems: 2MM
Effort actual or spent in this period:	Task 1.1 Project management: 0,5MM Task 3.2 Power node: 9MM Task 6.4 Real world requirements for SPD-based systems: 2MM
% of work completed at the end of the period (indicative):	Task 1.1 Project management: 100% Task 3.2 Power node: 100% Task 6.4 Real world requirements for SPD-based systems: 100%

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 management, final reporting activities, final review meeting preparation.
- Task 3.2

- The activities carried out in this task have been focused on the design of the Power Node, a mobile and rugged high performance embedded node with SPD intrinsic functionalities and on the related demonstrator.
- Integration of the Power Node board demonstrator.
- Development of the final version of the Power Node rugged enclosure.
- Power node thermal studies evaluation, test and feedback.
- Results: the test of the second release of the Power Node prototype has been completed. Further activities related to bugs corrections and hw/sw improvements for the second/final version have been performed. Thermal studies and rugged enclosure design completed. Second prototype of Power Node cold-plate based cooling system. The development activities for the demonstrator have been completed.

- Task 6.4
  - Final demonstrator development and integration (in collaboration with SESM).

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 SPD layer will rely. This 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 been completed and has been integrated in the final pilot. The design and development of the cooling system and of the rugged enclosure has been completed and the second version of the prototype of the cold-plate based liquid cooling system has been integrated in the final prototype.

Highlight clearly significant and tangible results

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

- test of the second release of the Power Node prototype completed.
- Final bugs correction and improvements for the second/final version identified.
- Second release of the Power Node prototype integrated in the final demonstrator.
- Second prototype of the cold-plate based cooling system completed and integrated in the demonstrator.

Deviations from Annex I and their impact on other tasks

Workpackage 3 activities have been completed as planned after the extension of the project.

Use of resources

Resources have been used according to the activities plan defined after the project extension.

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 Elsag (ex Selex Communications)

Beneficiary:	SELEX ELSAG (ex SELEX COMMUNICATIONS)
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 Developments Task 7.2 Exploitation
Period:	1st July 2011 – 31st December 2012
Effort planned in this period:	Task 1.1/2 Project Management/Liaisons - 0.5MM Task 2.3 Multi Technology Architectural Design – 0.0MM Task 4.1 Smart SPD driven transmission – 2.5MM Task 6.1 Multi Technology System Developments – 0.5MM Task 7.2 Exploitation – 1.0MM
Effort actual or spent in this period:	Task 1.1/2 Project Management/Liaisons – 0.5MM Task 2.3 Multi Technology Architectural Design – 0.0MM Task 4.1 Smart SPD driven transmission – 4.0MM Task 6.1 Multi Technology System Developments – 0.5MM Task 7.2 Exploitation – 1.0MM
% of work completed at the end of the period (indicative):	Task 1.1/2 Project Management/Liaisons – 100% Task 2.3 Multi Technology Architectural Design – 100% Task 4.1 Smart SPD driven transmission – 113% Task 6.1 Multi Technology System Developments – 100.0% Task 7.2 Exploitation – 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP: • Task 2.3 ➢ Completion of the study of the metrics for the SPD classification related to the architectural design • Task 4.1	

- Completion of the study and motivation of the main features needed for making the pSHIELD SPD-Based Radio System working
- Completion of the identification and continuation of the study on the reconfigurable radio components with waveform parameters (frequency, bandwidth, …) allowing SPD transmissions
- Completion of the identification and continuation of the study on spectrum sensing features for Cognitive Radio analysis and the available/used resources
- Completion of the study of some 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 July: WP2.3 meeting
- 28th July: WP4.1 meeting
- 28th- 30th September: review meeting
- 26th October: phone conference
- 17th, 24th November: phone conference
- 14th December: phone conference

Deviations between actual and planned person-months:

- 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.

Dissemination activities and exploitation perspectives:

- In order to disseminate the results achieved during project-related activities, the Company has participated to international conferences and forums where part of the work performed in pSHIELD has been discussed.
- The dissemination was supported also by Finmeccanica MindSh@re Technological Communities, through documents exchange and workshops.
- pSHIELD related publications:
    - L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C. S. Regazzoni, Sk. S. Alam and C. Armani (SE), "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, 2011

3.7.6. Tecnologie delle Reti e dei Sistemi

Beneficiary:	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 July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 - Project Management – 0,25 PM Task 5.1 - SPD driven Semantics – 2 PM
Effort actual or spent in this period:	Task 1.1 - Project Management – 0,25 PM Task 5.1 - SPD driven Semantics – 2 PM
% of work completed at the end of the period (indicative):	Task 1.1 - Project Management – 100% Task 5.1 - SPD driven Semantics – 100%

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

- Task 1.1
  - Controlling project scheduling, achievements and costs
  - Coordination of technical activities inside the task

  Results: updated schedules and reporting of progress and resource expenditure

- Task 5.1
  - Implementation of semantic patterns of SPD composition, based on declarative rules
  - Development of the semantic reasoner for SPD composition

A summary progress towards objectives

The activities carried out in this last time-frame are based on the outcomes from the previous period, mostly concerning the fulfilment of the run-time components that shall supply SPD composition in accordance with the models formalized in the ontology.

The concept of connectors, previously devised in order to provide an analytical specification for the composition of SPD status values (based on Common Criteria), and the concepts of dynamic composition, based on the knowledge of the semantic constraints among components at design-time and run-time, have been implemented by means of rules in the JENA framework. The operators MIN, OR, MEAN, etc. have been coded through built-in and custom primitives, and model assertions and constraints have been coded, in a declarative fashion, in a set of rules; finally, an automatic reasoner has been developed so that, when fed by

rules and system model, it is able to devise new compositions, based on the knowledge of modules that at the moment are active in the system, in order to guarantee the prearranged overall SPD level.

The pSHIELD demonstration scenario platform has been modelled according to the framework, and suitable instances of the ontology and rules have been developed for validation purposes; the test has proved that the semantic reasoner is able to devise all the compositions that, among the valid ones, succeed in obtaining a prearranged target for the overall SPD level.

The outcomes are documented in deliverables D5.3 (pSHIELD semantic models report) and D6.2 (Platform validation and verification)

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

Description of criticalities met during the period:

- No meaningful criticalities were met during the period

Meetings performed during the period:

- 12nd - 13rd July - Consortium meeting, Rome
- 21st July – WP5 partners technical meeting, Rome
- 26th July - WP5 partners technical meeting, phone call
- 7th September - WP5 partners technical meeting, Rome
- 20th October- WP5 partners technical meeting, phone call
- 3rd November- WP5 partners technical meeting, phone call
- 24th November- WP5 partners technical meeting, phone call

Deviations between actual and planned person-months:

No deviation is reported: according to the new project schedule, the extension of the project has been taken into account during the allocation of residual resources, and we have managed to fit the remaining budget to the new duration of 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.
- Application and further development of such technologies are planned in a number of oncoming research projects in TRS. A major exploitation is expected in the CHIMERA Project (Cognitive, tHInking and adaptive fraMEwork for pRoduction optimizAtion), submitted to FP7 ICT part of Call Factories of the Future, that shall leverage semantic technologies to build an effective platform for predictable, manageable and verifiable manufacturing processes.

3.7.7. Università degli Studi di Genova

Beneficiary:	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 Jul 2011 – 31th Dec 2011
Effort planned in this period:	Task 4.1 Smart SPD driven transmission – PM 0.5 (Effectively needed 0.5) Task 4.2 Trusted and dependable Connectivity – PM 0.5 (Effectively needed 0.5)
Effort actual or spent in this period:	Task 4.1 Smart SPD driven transmission – PM 0.5 Task 4.2 Trusted and dependable Connectivity – PM 0.5
% of work completed at the end of the period (indicative):	Task4.1 Smart SPD driven transmission - 100% Task 4.2 Trusted and dependable Connectivity – 100%

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

Main efforts in this period have been devoted in the development of a pSHIELD simulator that was presented at the September review in Oslo.

The scenario consist in a number of entities (agents) carrying a mobile device which is able to transmit and receive data at 3 different frequencies (namely 900, 1800 and 1900 MHz) to a centralized control centre. The agents move randomly throughout a radio-disturbed environment, where randomly placed jammers emit a disturbing signal. The jammers can be either fixed or moving and their emitted signal follows the Rayleigh distribution with fixed parameters. Fixed jammers positions and characteristics are stored in an XML file, which is loaded in the setup stage together with the map of the ground.

The mobile devices periodically send a single radio data to the control centre, where a running cognitive node receives and elaborates it. Also, a periodical polling is performed by the agents to question the node, which answers back.

A radio data sent by an agent contains the following pieces of information:

1. Position of the agent (x,y) on the mapped ground: this is generated by a trajectories simulator. It simulates a GPS sensor on the mobile device. If a video monitoring of the ground area is available, positioning data coming from a tracker can be possibly fused to GPS data to obtain a better position estimation.
2. Frequency of transmission: this can be chosen among the three available frequencies at the beginning of the simulation.
3. Power of the transmitted signal: fixed.
4. Power of the signal received from the node: this depends on the distance and it is calculated through FSPL. Also, it can be disturbed by jammers.
5. Possibly detected jammers' estimated power: each jammer has a typical radius (coded in the XML configuration file) of influence, inside which the agent can measure its power.

6. ID of possible neighbour agents (within a fixed sensing radius).

A slightly different scenario can be also set by introducing a moving jammer: an agent carrying a jamming device can be introduced in the scene. Such an intruder-agent differs from the others as he obviously disturbs communications to the node. Also, he communicates a false GPS survey to the node.

The radio data reception represents, from the node point of view, the sensing logical block of the cognitive cycle. The agents' mobile terminals are the sensors which monitor the environment sending a radio survey (radio sensors) and a positioning piece of information (GPS sensor).

The node then analyzes all the data received from each agent, both singularly and collectively. For each agent, the signal-to-noise and distortion ratio (SINAD) of the received data packet is computed. Also, the relative positions the agents are compared, on the basis of the datum sent by an agent himself and of the fused data sent by the agents in the sensing range. By means of a voting algorithm, rankings are assigned to the IDs of each agent. The intruder's position and ID are worked out as soon as enough information is gathered, based on such rankings.

In the decision stage, the SINAD datum is compared to an acceptable (fixed to 10 dB) threshold. If the communication with an agent turns out to be too disturbed, a suitable strategy ST is chosen to schedule a change in frequency transmission.

The action block provides a change in the state of the system. As already explained, this module implements the active interaction of the system towards the surrounding environment or towards itself: the action of changing frequency is selected based on the strategy ST chosen during the previous step. Such an action is executed on the system itself by means of suitable actuators, namely the agents. Actually, as already pointed out, through a periodical polling, the agents themselves ask the node for information: however this does not change the heart of the matter.

The detection of the intruder does not trigger a decision and a subsequent action in the cognitive cycle. The information relative to the false agent is simply communicated to an interface. Such an interface could simply be in a control centre, or could display data on the mobile devices, thus leaving the decision step under human control. Alternatively, a strategy could be implemented to be learned by the cognitive node in a future perspective.

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:

- 28-30 September: review meeting in Kjeller/Oslo
- 24th November: phone call
- 14th December: 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 1 PM in this period. 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: o 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 o 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, 2011 o S. S. Alam, L. Marcenaro and C. Regazzoni, "Opportunistic Spectrum Sensing and Transmissions", Cognitive Radio and Interference Management: Technology and Strategy, IGI-Global, 2012.

3.7.8. Università degli Studi di Roma "La Sapienza"

Beneficiary:	UNIROMA1
Work Package(s)	WP1 - Project management
Task(s)	Task 1.1 - Project management
Period:	1st July 2011 – 31st December 2011
Effort planned for the whole project:	**WP1 – 2,0 PM** Task 1.1 – 2 PM
Effort actual or spent in this period:	**WP1 – 0,4 PM** Task 1.1 – 0,4 PM
% of work completed at the end of the period (indicative):	**WP1 – 95%** Task 1.1 – 95%
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. ➢ Organization of the consortium meeting in UNIROMA1 premises ➢ Support the review meetings. Objectives: manage the project	
Meetings performed during the period: ➢ 12th – 13th July, University of Rome "La Sapienza": plenary consortium meeting, ALL	

- 2nd September, SESM: Technical Phone Call, ALL
- 15th September, SESM: Technical Phone Call, ALL
- 21st September, SESM: Technical Phone Call, ALL
- 29th September, MAS, consortium meeting for mid-term review preparation – ALL
- 39th September, MAS; mid-term review meeting - ALL
- 6th October, SESM: Technical Phone Call, ALL
- 24th November, SESM: Technical Phone Call, ALL
- 14th December, SESM: Technical Phone Call, ALL

Beneficiary:	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 July 2011 – 31st December 2011
Effort planned for the whole project:	**WP5 – 22,0 PM** Task 5.1 – 5,0 PM Task 5.2 – 9,0 PM Task 5.4 – 8,0 PM
Effort actual or spent in this period:	**WP5 – PM 4,0** Task 5.1 – 0,5 PM Task 5.2 – 2,0 PM Task 5.4 – 1,5 PM
% of work completed at the end of the period (indicative):	**WP5 – 120%** Task 5.1 – 114% Task 5.2 – 128% Task 5.4 – 114%

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

- **T5.1 - SPD driven Semantics**
  - Finalization of the pSHIELD Ontology with the enabling of composability fully compliant with the WP2.
  - Enrichment of technological analysis on the basis of the results achieved during the project.
  - Some additional work has been performed in the scope of WP6 to contribute and review the D6.x deliverables with respect to the sections that are directly impacted by the semantic.
  - Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Objectives: provide semantic models to enable the pSHIELD seamless approach
Tangible Results: release of pSHIELD Semantic models prototype (OWL file), release of deliverables D5.1 (final version) and D5.3 (final version).

- **T5.2 - Core SPD services**
  - Finalization of the high level design of the pSHIELD Middleware Architecture.
  - Finalization and refinement of the implementation of the pSHIELD Middleware core services into the OSGI Knoplerfish platform taking into account the inputs coming from the application scenario.
  - Enrichment of technological analysis on the basis of the results achieved during the project.
  - Finalization of internal deliverable D5.2 on pSHIELD Middleware technologies
  - Finalization of deliverable D5.4 of pSHIELD SPD Middleware

- Some additional work has been performed in the scope of WP6 to contribute and review the D6.x deliverables with respect to the sections that are directly impacted by the middleware.
- Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Objectives: define the basic services at middleware layer in the multilayered approach; provide the Overlay with the (secure) discovery functionality
Tangible Results: release of the OSGI prototype tailored on the application scenario, release of deliverables D5.2 (final version) and D5.4 (final version).

- **T5.4 - Overlay monitoring and reacting system by security agents**
  - Finalization of the Hybrid Automata that represent the pSHIELD node and network.
  - Harmonization of Common Criteria approach and Hybrid Automata approach by formalizing the concept of "context aware composition".
  - Application of Model Predictive Control to the context aware composition, with the formalization of a typical MPC problem tailored on pSHIELD needs.
  - Assessment of the "Security Agent" concept, in conjunction with Task 5.2
  - Some additional work has been performed in the scope of WP6 to contribute and review the D6.x deliverables with respect to the sections that are directly impacted by the control algorithms.
  - Extensive advanced research, carried out since the project start, for developing methodologies suitable for supporting the above-mentioned work.

Objectives: design and develop the Overlay; design the closed-loop control algorithms to enable the Composability functionality
Tangible Results: release of Matlab-Simulink models and simulations as proof of concept of HA approach, release of deliverables D5.2 (final version) and D5.4 (final version).

Description of criticalities met during the period:

Deliverable 5.3 and 5.4 have been delivered with some delays due to the preparation of the second review meeting and to the support provided to WP6.

Corrective actions:

No negative impact on the project, so no corrective actions are needed. Documents have been finally delivered.

Meetings performed during the period:

- 12th – 13th July, University of Rome "La Sapienza": plenary consortium meeting, ALL
- 2nd September, SESM: Technical Phone Call, ALL
- 15th September, SESM: Technical Phone Call, ALL
- 21st September, SESM: Technical Phone Call, ALL
- 29th September, MAS, consortium meeting for mid-term review preparation – ALL
- 39th September, MAS; mid-term review meeting - ALL
- 6th October, SESM: Technical Phone Call, ALL
- 24th November, SESM: Technical Phone Call, ALL
- 14th December, SESM: Technical 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 framework to model and control complex interconnected systems by means of Hybrid Automata theory", July 2011.
- Giorgia Anzidei, "Design and implementation of an architecture for the composition of security services in heterogeneous embedded systems.

3.8 Spain

3.8.1 Acorde Seguridad

Beneficiary:	AS
Work Package(s)	WP1 - Project Management
Task(s)	Task 1.1 Project management
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 Project management 0 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	
Meetings performed during the period: ➢ MidTerm Review (Oslo, 28-30 September 2011)	

Beneficiary:	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 July 2011 – 31st December 2011
Effort planned in this period:	Task 3.1 Nano, Micro/Personal node 2 PM Task 3.2 Power Node 2 PM Task 3.3 Dependable self-x and cryptographic technologies 2 PM

Effort actual or spent in this period:	Task 3.1 Nano, Micro/Personal node 3 PM Task 3.2 Power Node 3.5 PM Task 3.3 Dependable self-x and cryptographic technologies 2 PM
% of work completed at the end of the period (indicative):	Task 3.1 Nano, Micro/Personal node 100 Task 3.2 Power Node 100% Task 3.3 Dependable self-x and cryptographic technologies 100%

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

- Task 3.1
  - Design of two different protection circuits (DC source): two power supplies where one of them includes a solution to connect and disconnect up to 5 sub-systems and it is able to monitor power consumption.
  - Manufacture of both protection boards: several tests have been carried out to ensure that it is possible to avoid damages into the system with both designs.
- Task 3.2
  - Design of an autonomy power supply system based on fuel cells, solar panels and turbines to feed continuously a system up to 500W and ensure its autonomy during ten days if the energy harvesting system fails.
  - Design of two different protection boards (AC source): one of them integrates a solution based on fuse varistors and the other one is implemented with varistors and a gas discharge. Several tests have been carried out in order to ensure that these protections can avoid damages into the system.
- Task 3.3
  - Integration of AES Rijndael algorithm and evaluation of some code optimisations in an embedded wireless platform.

Meetings performed during the period:

- PhC: 18th July
- PhC: 2nd September
- PhC: 9th September
- PhC: 6th October
- PhC: 13th October
- PhC: 24th November
- PhC: 14th December
- PhC: 15th December

Deviations between actual and planned person-months:

- The design, engineering and manufacturing of the developed modules has required more effort than initially planned, due to the nature of the associated works and the different trials performed. Nevertheless, the total budget has not been modified.

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:	Tecnalia
Work Package(s)	WP1 - Project Management WP2 - SPD Scenarios, user requirements and architecture design WP4 – SPD Network WP5- SPD middleware & Overlay WP6 – Platform Integration , validation and demonstration
Task(s)	Task 1.1 Project management Task 2.2 Multi-Technology specification and Metrics Task 4.2 Trusted and dependable connectivity Task 5.3 Policy-Based Management Task 6.3 Multi-technology Pilot Demonstration Task 7.1 Dissemination
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 Project management. PM – 0,1 Task 2.2 Multi-Technology specification and Metrics PM – 1 Task 4.2 Trusted and dependable Connectivity - PM: 0,1 Task 7.1 Dissemination – PM: 0,13
Effort actual or spent in this period:	Task 1.1 Project management. PM – 0,1 Task 2.2 Multi-Technology specification and Metrics PM – 1 Task 4.2 Trusted and dependable Connectivity - PM: 0,1 Task 7.1 Dissemination – PM: 0,13
% of work completed at the end of the period (indicative):	Task 1.1 Project management. 100% Task 2.2 Multi-Technology specification and Metrics 100% Task 4.2 Trusted and dependable Connectivity – 100% 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: Reporting of progress and resource expenditure, production of deliverables.
- Task 2.2
  - Refinement for SPD multilayer approach
  - Consolidate quantitative Measurement of Metrics
- Task 4.2
  - Validation of the trusted mechanisms with respect to metrics
- Task 7.1
  - Presentation of metric paper in Euromed conference

Description of criticalities met during the period:

- No severe criticalities were found. The most important point was to conclude with the integration of metrics in the demonstrator

Corrective actions:

- A project extension could be enough to finalize the work, because there was enough time to conclude

with the integration of different pilots
Meetings performed during the period: ➢ pSHIELD technical meeting in Rome: 12-13 of July ➢ 2nd September: phone conference ➢ 28th of September: pSHIELD Review ➢ 9th of November: phone call ➢ 24th of November: phone call ➢ 15th of December: phone call
Deviations between actual and planned person-months: ➢ No deviations
Dissemination activities and exploitation perspectives: ➢ Paper presented in Euromed Conference in Bilbao in October ➢ Trusted metrics module presentation in ESICenter congress

3.8.3 Mondragon Goi Eskola Politecnikoa

Beneficiary:	MGEP – Mondragon Goi Eskola Politeknikoa
Work Package(s)	WP1 - 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 7.1 Dissemination
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 1.1 Project management – PM: 0.12 Task 4.2 Trusted and dependable Connectivity – PM 1 Task 7.1 Dissemination - PM: 0.1
Effort actual or spent in this period:	Task 1.1 Project management – PM:0.12 Task 4.2 Trusted and dependable Connectivity – PM 1 Task 7.1 Dissemination - PM: 0.1
% of work completed at the end of the period (indicative):	Task 1.1 Project management – 100% Task 4.2 Trusted and dependable Connectivity – 100% 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: Reporting of progress and resource expenditure, production of deliverables.
- Task 4.2
  - ➢ Finish the study of the different IDS approaches (misuse vs anomaly detection, and architecture) taking into account the requirements of sensor networks.

- Finish the study of anomaly detection systems.
- Writing of the deliverable 4.2 SPD Network Technologies Prototype Report as part of the work to be done within Task 4.2 Trusted and dependable Connectivity.

- Task 7.1
  - One paper was 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 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 assess 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.

These activities have already been described in the previous review report and this final period has mainly been dedicated to finishing these studies and writing the deliverable 4.2 as mentioned before. One paper was also presented in SPSM '11 workshop in New York on October 2011.
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 writing the deliverable 4.2 SPD Network Technologies Prototype Report as part of the work to be done within Task 4.2 Trusted and dependable Connectivity. The final version of this deliverable can be was uploaded to the project Wiki on November 11th. This included a study of the different IDS approaches and architectures to propose the most suitable for WSN carried out by MGEP.
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.
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 during this period: o Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crowdroid: behaviour-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM. ISBN 978-1-4503-1000-0.

3.9 Greece

3.9.1 ATHENA

Beneficiary:	ATHENA
Work Package(s)	WP6: Platform integration, validation & demonstration WP7: Knowledge exchange and industrial validation
Task(s)	Task 6.1: Multi Technology System Developments Task 6.2 Multi-Technology Validation & Verification Task 6.3 Multi-technology Pilot Demonstration Task 6.4 Real world requirements for SPD-based systems Task 7.1 - Dissemination
Period:	1/7/2011 – 31/12/2011
Effort planned in this period:	Task 6.1: Multi Technology System Developments - 2 PM Task 6.3 Multi-technology Pilot Demonstration - 1 PM Task 6.4 Real world requirements for SPD-based systems - 1PM Task 7.1 – Dissemination – 0,5 PM

Effort actual or spent in this period:	Task 6.1: Multi Technology System Developments – 1,5 PM Task 6.3 Multi-technology Pilot Demonstration – 1 PM Task 6.4 Real world requirements for SPD-based systems – 1PM Task 7.1 – Dissemination – 0,5 PM
% of work completed at the end of the period (indicative):	Task 6.1: Multi Technology System Developments – 75% Task 6.3 Multi-technology Pilot Demonstration – 100% Task 6.4 Real world requirements for SPD-based systems – 100% Task 7.1 - Dissemination – 100%

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

- Task 6.1
  - Presented the synergies and integration of the controlled randomness (CRP) protocol for cryptographic key exchange with the SPD node prototypes that were developed in WP3.
- Task 6.3 & Task 6.4
  - Presented the feasibility of the CRP protocol on resource limited devices as well as the prototype implementation results.
- Task 7.1:
  - V. Voyiatzis , K. Stefanidis and D. N. Serpanos: "Increasing Lifetime of Crypto Keys on Smartphone Platforms with the Controlled Randomness Protocol", In Proceedings of 6th Workshop on Embedded Systems Security WESS 2011, October 2011
  - K. Stefanidis, A. V. Voyiatzis and D. N. Serpanos: "Performance of the Controlled Randomness Protocol on .NET Compact Framework Embedded Systems", In Proceedings of 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, France, February 2011

3.9.2 Hellenic Aerospace Industry

Beneficiary:	HAI
Work Package(s)	WP2 - SPD Metrics, Requirements and System Design
Task(s)	Task 2.3 - Multi-Technology Architectural Design
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 2.3 - Multi-Technology Architectural Design, 1 PM
Effort actual or spent in this period:	Task 2.3 - Multi-Technology Architectural Design, 1 PM
% of work completed at the end of the period (indicative):	Task 2.3 - Multi-Technology Architectural Design, 100%

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

- Task 2.3

- The objective of completing the multi-technology Architecture description included the following activities:
  - ✓ Registration of the most important SPD requirements with impact in the definition of architecture
  - ✓ Description of several types of interfaces, including: internal (interconnecting the 4 pSHIELD layers), external (e.g. user interfaces), node/sensor interfaces and interfaces between pSHIELD components (pS-SPD-ESD, Security Agents etc.)
  - ✓ The newly introduced concept of pSHIELD Overlay was analyzed further
  - ✓ D2.3 was finalized in the form of its second version, D2.3.2
- Results:
  - ✓ Important, for the definition of architectural framework pSHIELD, concepts were clarified
  - ✓ The link with WP2 activities and outcomes was strengthened (Requirements and Metrics)
  - ✓ The interaction with WP3-5 activities and outcomes increased(4 pSHIELD layers)
  - ✓ Partners continued developing architectural components
  - ✓ pSHIELD System Architecture was finalized

Description of criticalities met during the period:

- D2.3, dedicated to the description of the system architecture, is a deliverable synthesizing multifaceted work, having strong interdependencies with requirement and metric analysis, as well as technical work conducted in other WPs. The recorded delay in the finalization of the deliverable followed the general divergence in the execution of the project time plan

Corrective actions:

- pSHIELD System Architecture, as all basic concepts of the project, will be tested during the activities of WP6, where pSHIELD platform will be integrated, validated and demonstrated

Meetings performed during the period:

- Apart from a dedicated phone conference on July, D2.3 and System Architecture were main points in the agenda of almost every general project phone conference conducted in this period

Deviations between actual and planned person-months:

- No significant deviations were recorded for HAI. Given the project process, it was necessary for HAI to put a small amount of extra effort (compared to the originally planned) for the finalization of Task 2.3

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, such as architecture, demonstration and prototypes, to enhance its knowledge and competence in embedded systems as parts of security solutions

Beneficiary:	HAI
Work Package(s)	WP6 - Platform integration, validation & demonstration

Task(s)	Task 6.1 - Multi-Technology System Developments
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 6.1 - Multi-Technology System Developments, 20 PM
Effort actual or spent in this period:	Task 6.1 - Multi-Technology System Developments, 5 PM
% of work completed at the end of the period (indicative):	Task 6.1 - Multi-Technology System Developments, 25% PM[2]

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

- Task 6.1
  - The objective of presenting the platform development procedure includes the following activities:
    - ✓ Presentation of the discrete components and prototypes developed in WP3-5
    - ✓ Preliminary formation of the pSHIELD testbed platform
    - ✓ Exploration of possible inter-component synergies and integration to subsystems
  - Results:
    - ✓ Representation of pSHIELD 4 layers structure and basic concepts by demonstration prototypes

Description of criticalities met during the period:

- D6.1, dedicated to the registration of the prototypes that constitute the overall pSHIELD Demonstration Platform, has been affected by the delays recorded in the development of demonstrators by different partners in different WPs and technological areas. Additionally, it should be stated that the consortium is focusing efforts to conclude the project, working in parallel in all four tasks of critical WP6

Corrective actions:

- D6.1 will be completed on time for the project's final review, in order to form, along with the other 3 WP6 deliverables, a conceptual framework of the pSHIELD Demonstrator

Meetings performed during the period:

- Work in D6.1 was organized and discussed during phone conferences dedicated to WP6 or to each time current pSHIELD activities. The basis for the demonstration platform and its components was set in the review meeting of Oslo (September 2011), where the different prototype demonstrators started to be clarified

Deviations between actual and planned person-months:

- A part of the planned person months was consumed

Dissemination activities and exploitation perspectives:

- No dissemination activities were conducted during the reference period, but as stated in the Technical Annex, HAI expects to be benefited a great deal from the participation in pSHIELD demonstration activities and findings (architecture, demonstration and prototypes).

3.9.3 Integrated Systems Development

ISD withdrew 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 one 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. Additional contacts have been established to ABB, the market leader for IoT based energy supply and the Norwegian Defence Research Establishment (FFI). Workshops performed in Q3-Q4.2011have identified the Eco-system for nSHIELD, and common activities towards the Industry, the Research Council of Norway, and the EU to see the value of the Nordic model for an integrated approach using embedded systems for the Future Internet.

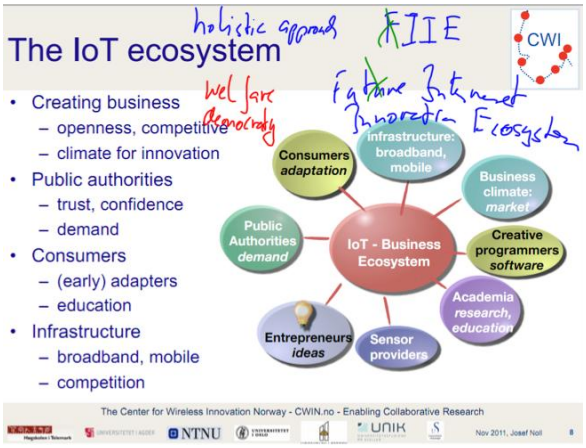


Figure 1 -The Nordic perspective on the IoT

Highlight clearly significant and tangible results

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

- Demonstrated the prototypical 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 the measurement locomotive "Roger" of the Norwegian Rail Administration.
- The exploited real-life experiences when 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.
    - An initial technology study was performed, concluding that an encryption of the physical link between the power node and the micro-sensors should be feasible, but requires in-depth changes of the SunSPOT application environment.
    - A counter-measure for an attack, consisting of a replacement of the Sun Spot sensor, was taken into consideration by implementing an "identify control" of the sensor. The sensor ID is part of the communication with the Telenor Shepherd platform.
    - Telenor adopted their Shepherd platform according to the requirements of pSHIELD for the identity handling of sensors.
- Discussions with ABB in order to expand the pSHIELD approach into the industrial energy environment. Main focus is to gain a common understanding of the security metrics as suggested in pSHIELD.
- Discussions with FFI (Research Institute of the Norwegian Defense) to enhance the SPD matrix into an attribute-based access authentication for the Internet of Things. The results of the discussion were taken as input for a strategic research project in FFI.
- Ongoing collaboration with SIMLINK the use of an encrypted platform, the WlanSIM, as a potential future pSHIELD demonstrator. Current work tends towards a technology demonstrator for home energy control in collaboration with Danfoss.
- 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.

Regarding the ecosystem for a successful Future Internet, several activities were performed.

- CWI Norway was invited speaker in an Internet of Things workshop at Aalborg University. The main outcome was a task force towards the Future Internet Week (May 2012) in Aalborg.
- The task force for the "Nordic perspective on the IoT" gathered support from the national research council and industry. Experts from DK and NO joined in January 2012 (http://wiki.unik.no/index.php/CWI/FutureInternet-Jan2012) to discuss the way ahead, including prototypical demonstrations for the Future Internet Week. The pSHIELD based security, privacy and dependability principles are of fundamental importance for the success of the Future Internet.

3.10.1 Centre for Wireless Innovation

Beneficiary:	CWIN
Work Package(s)	WP3 – SPD node WP6 – Platform integration, validation & demonstration WP7 – Knowledge exchange and industrial validation
Task(s)	Task 3.1 Nano, Micro/Personal node Task 3.2 Power node Task 6.1 Multi Technology System Developments Task 6.4 Real world requirements for SPD-based systems Task 7.1 Dissemination
Period: Effort planned in this period:	01.07.2011 – 31.12.2011 Task 3.1 Nano, Micro/Personal node 0PM Task 3.2 Power node 0PM Task 6.1 Multi Technology System Developments 2PM Task 6.4 Real world requirements for SPD-based systems 3PM Task 7.1 Dissemination 1PM
Effort actual or spent in this period:	Task 3.1 Nano, Micro/Personal node 1.5PM Task 3.2 Power node 1PM Task 6.1 Multi Technology System Developments 2PM Task 6.4 Real world requirements for SPD-based systems 1.5PM Task 7.1 Dissemination 0.5PM
% of work completed at the end of the period (indicative):	Task 3.1 Nano, Micro/Personal node 100% Task 3.2 Power node 100% Task 6.1 Multi Technology System Developments 100% Task 6.4 Real world requirements for SPD-based systems 100% Task 7.1 Dissemination 100%
Description of the activities carried out during the period to reach specific objectives within the task/WP: • Task 3.1 ➢ Development of iPhone complementary solution ➢ Modification of pSHIELD nodes towards security. ➢ Node technologies refinements of software, as a result of life tests Results: The micro/nano node types have been integrated into the Telenor platform, privacy and	

dependability has been demonstrated. Security (man in the middle attack) has been targeted on the micro node (Sun Spot)

- Task 3.2
  - Real-world adaptations of "trusted boot" and "fail-safe" operations have been added to the power node
  - Integration of sensor platform and interworking with the Shepherd platform

Results: Development, integration and successful demonstration

- Task 6.1
  - Prototypical implementation of ways to integrate node layers with the middleware/overlay layers using M2M platform.
  - Dependability add-on feature through combined use of two platforms
  - Integration on the measurement vehicle Roger, evaluation and work on real-life refinements

Results: Implementation of autonomous platform for use in Measurement Train "Roger". Successful demonstration of privacy (data control), and dependability (boot sequences, sensor connectivity). Evaluation of results, focussing on security application (identity handling, man in the middle attack) for the Sensor communication with the power node

- Task 6.4:
  - pSHIELD prototypical demonstrator have been demonstrated
  - Real-life experience has been gathered.
  - Support for Norwegian Rail Administration towards location identification.
  - Multi-technology (phone and personal node) platform integration and demonstration.

Results: Prototypical demonstration of node (micro & power node) integration to Telenor Object platform

- Task 7.1:
  - Dissemination through journal articles
  - Support of Movation for Dissemination activities

Description of criticalities met during the period:

- Key personnel leaving the project, causing re-organisation of the contributions. Thus focus was on technology development rather than deliverable contribution.
- 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.
- The experience with the lack of precise GPS information was also taken further with the Norwegian Rail Administration, who asked for support with respect to "wrong locations" of their GPS-based event measures.

Corrective actions:

- Manpower transfer from Sarfraz Alam and Zahid Iqbal. Second change of key personnel.
- 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
- phone conferences

Previous **Results 1– 20** Next (**20** | 50 | 100 | 250 | 500)

	Date
PSHIELD PhC 20120125	2012-01-25T11:30:00
PhC WP6 - Task 6.4	2012-01-09T14:30:00
PhC WP3-15Dec2011	2011-12-15T11:30:00
PSHIELD PhC 20111214	2011-12-14T11:30:00
PSHIELD PhC 20111124	2011-11-24T11:30:00
PhC WP6 - Tasks 6.3 and 6.4	2011-11-22T11:00:00
TA-update-WPall	2011-10-13T11:30:00
WP3 phone conf	2011-10-12T11:00:00
PSHIELD PhC 20111006	2011-10-06T11:00:00
PSHIELD PhC 20110921	2011-09-21T14:30:00
PSHIELD PhC 20110915	2011-09-15T11:00:00
WP3 PhC 20110909	2011-09-09T11:30:00
PSHIELD PhC 20110902	2011-09-02T11:30:00
D2.3.1 PhC 20110728	2011-07-28T11:00:00
OpenIssue PhC 20110718	2011-07-18T11:00:00
TMC PhC 20110711	2011-07-11T11:00:00
PA PhC 20110706	2011-07-06T11:00:00
PhC 20110701	2011-07-01T10:00:00

- meetings

Review-September2011	29 September 2011	Kjeller/Oslo	Project Review
PreReview-September2011	28 September 2011	Kjeller, Norway	Project pre meeting, incl. video/travel info
Agenda-September2011	29 August 2011	Kjeller	Review Meeting, Detailed Agenda
PA Rome 20110712-13	12 July 2011	University of Rome "La Sapienza"	pSHIELD-PA

Deviations between actual and planned person-months:

The focus of CWIN and Movation were towards integration, prototypical demonstration and dissemination/exploitation. Thus manpower was shifted from other tasks towards WP6 (integration & prototypical demonstration) and WP7 (dissemination).

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.
  - 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.
- 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 WP6 – Platform integration, validation & demonstration WP7 – Knowledge exchange and industrial validation
Task(s)	Task 1.1 Project Management Task 6.4 Real world requirements for SPD-based systems Task 7.1 Dissemination
Period:	01.07.2011 – 31.12.2011
Effort planned in this period:	Task 1.1 Project Management 0PM Task 6.4 Real world requirements for SPD-based systems 1PM Task 7.1 Dissemination 0PM
Effort actual or spent in this period:	Task 1.1 Project Management 2PM Task 6.4 Real world requirements for SPD-based systems 0.5PM Task 7.1 Dissemination 1PM
% of work completed at the end of the period (indicative):	Task 1.1 Project Management 100% Task 6.4 Real world requirements for SPD-based systems 100% 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
  - Administrative project leadership of pSHIELD, established leader team, received excellent support from Przemek Osocha, Andrea Fiaschetti, Elisabetta Campaiola, and Francesca Matarese in all matters.
  - Changed from BSCW to Semantic Mediawiki for consistency of information.
  - Increased the responsibilities of the Norwegian contribution towards an SPD-enabled prototype

  Results:
    - Agreements on how to successful collaborate
    - Successful review in September 2011
    - Semantic MediaWiki platform: http://pshield.unik.no
- Task 6.4:
  - pSHIELD prototypical demonstrator have been demonstrated
  - Real-life experience has been gathered.
  - Support for Norwegian Rail Administration towards location identification.
  - Multi-technology (phone and personal node) platform integration and demonstration.

  Results: Prototypical demonstration of node (micro & power node) integration to Telenor Object platform
- Task 7.1:
  - Contribution to journal article
  - Presentation of pSHIELD at several national/international workshops
  - Participation at the ITEA/Artemis Co-Summit
  - Targeted industrial dissemination towards ABB, FFI and SIMLINK

Description of criticalities met during the period: ➢ Regain of momentum in pSHIELD, after a period of non-collaboration ➢ Technology: The results from the life-demonstration on the locomotive ”Roger” from the Norwegian Rail Admin (JBV) showed the requirements for fully-autonomous operation “automatic boot” and an secondary provision of location. A description of these issues was provided by CWIN.
Corrective actions: ➢ Agreed to take over responsibility as project manager. Contributed to a collaborative project management with an excellent team consisting of Przemek Osocha, Francesca Matarese, Elisabetta Campaiola and Josef Noll. Technical responsibility was transferred back to the experts in the field, resulting in prototypical demonstrations. ➢ Re-focus in pSHIELD towards the prototypical implementation of technologies, and reduced focus on the deliverables. These prototypes were successfully demonstrated during the additional review in Kjeller/Oslo. ➢ Discussion and guidelines towards CWIN for the 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
- phone conferences

Previous **Results 1– 20** Next **(20** | 50 | 100 | 250 | 500)

	Date
PSHIELD PhC 20120125	2012-01-25T11:30:00
PhC WP6 - Task 6.4	2012-01-09T14:30:00
PhC WP3-15Dec2011	2011-12-15T11:30:00
PSHIELD PhC 20111214	2011-12-14T11:30:00
PSHIELD PhC 20111124	2011-11-24T11:30:00
PhC WP6 - Tasks 6.3 and 6.4	2011-11-22T11:00:00
TA-update-WPall	2011-10-13T11:30:00
WP3 phone conf	2011-10-12T11:00:00
PSHIELD PhC 20111006	2011-10-06T11:00:00
PSHIELD PhC 20110921	2011-09-21T14:30:00
PSHIELD PhC 20110915	2011-09-15T11:00:00
WP3 PhC 20110909	2011-09-09T11:30:00
PSHIELD PhC 20110902	2011-09-02T11:30:00
D2.3.1 PhC 20110728	2011-07-28T11:00:00
OpenIssue PhC 20110718	2011-07-18T11:00:00
TMC PhC 20110711	2011-07-11T11:00:00
PA PhC 20110706	2011-07-06T11:00:00
PhC 20110701	2011-07-01T10:00:00

- meetings

Review-September2011	29 September 2011	Kjeller/Oslo	Project Review
PreReview-September2011	28 September 2011	Kjeller, Norway	Project pre meeting, incl. video/travel info
Agenda-September2011	29 August 2011	Kjeller	Review Meeting, Detailed Agenda
PA Rome 20110712-13	12 July 2011	University of Rome "La Sapienza"	pSHIELD-PA

Deviations between actual and planned person-months:

- WP1 (management): The project members asked the Movation representative to take over the administrative leadership, which requires being much more involved in administrative matters
- WP6 (prototypical demonstrations): Focus was on prototypical demonstrations, and thus more effort was spent in this work package.
- WP7 (: 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. Movation used in Q3-Q4 about five times the foreseen budget, which was taken from internal funds. The total expenses in Movation were about double (211 kEUR) as compared to the planned budget (108 kEUR).

Dissemination activities and exploitation perspectives:

- Movation (MAS) was responsible for targeted industrial dissemination.
- Discussions with ABB in order to expand the pSHIELD approach into the industrial energy environment. Main focus is to gain a common understanding of the security metrics as suggested in pSHIELD.
- Discussions with FFI (Research Institute of the Norwegian Defense) to enhance the SPD matrix into an attribute-based access authentication for the Internet of Things. The results of the discussion were taken as input for a strategic research project in FFI.
- Ongoing collaboration with SIMLINK the use of an encrypted platform, the WlanSIM, as a potential future pSHIELD demonstrator. Current work tends towards a technology demonstrator for home energy control in collaboration with Danfoss.
- 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.
- 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. This activity is handed over to nSHIELD.

3.11 Slovenia

3.11.1 THYIA Tehonlogije

Beneficiary:	**THYIA**
Work Package(s)	WP1 – Project management (total 2) 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 6 PM)
Task(s)	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 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 6.1 Multi Technology System Developments Task 6.2 Multi-Technology Validation & Verification Task 6.4 Real world requirements for SPD-based systems Task 7.1 Dissemination Task 7.2 Exploitation
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 2.3 Multi-technology architectural design (0,5 PM) Task 3.1 Nano, micro/personal node (2.5 PM) Task 3.3 Dependable self-x and cryptographic technologies (2 PM) Task 4.1 Smart SPD driven transmission (1.6 PM) Task 4.2 Trusted and dependable Connectivity (1,5 PM) Task 5.1 SPD driven Semantics (0.9 PM) Task 5.2 Core SPD services (1.99 PM) Task 5.4 Overlay monitoring and reacting system by security agents (2.62 PM) Task 6.1 Multi-Technology System Developments (3 PM) Task 6.2 Multi-Technology Validation & Verification (3 PM) Task 6.4 Real world requirements for SPD-based systems- (14 PM) Task 7.1 Dissemination (1.4 PM) Task 7.2 Exploitation (1.65 PM)

Effort actual or spent in this period:	Task 2.3 Multi-technology architectural design (0,5 PM) Task 3.1 Nano, micro/personal node (5.5 PM) Task 3.3 Dependable self-x and cryptographic technologies (5 PM) Task 4.1 Smart SPD driven transmission (1.6 PM) Task 4.2 Trusted and dependable Connectivity (1,5 PM) Task 5.1 SPD driven Semantics (0.9 PM) Task 5.2 Core SPD services (1.99 PM) Task 5.4 Overlay monitoring and reacting system by security agents (2.62 PM) Task 6.1 Multi-Technology System Developments (3 PM) Task 6.2 Multi-Technology Validation & Verification (3 PM) Task 6.4 Real world requirements for SPD-based systems- (8 PM) Task 7.1 Dissemination (1.4 PM) Task 7.2 Exploitation (1.65 PM)
% of work completed at the end of the period (indicative):	Task 2.3 Multi-technology architectural design (100%) Task 3.1 Nano, micro/personal node (220%) Task 3.3 Dependable self-x and cryptographic technologies (250%) Task 4.1 Smart SPD driven transmission (100%) Task 4.2 Trusted and dependable Connectivity (100%) Task 5.1 SPD driven Semantics (100%) Task 5.2 Core SPD services (100%) Task 5.4 Overlay monitoring and reacting system by security agents (100%) Task 6.1 Multi-Technology System Developments (100%) Task 6.2 Multi-Technology Validation & Verification (100%) Task 6.4 Real world requirements for SPD-based systems (57%) Task 7.1 Dissemination (100%) Task 7.2Exploitation (100%)

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

Task 2.3 Multi-technology architectural design

- Contributions in D2.3.2 for SPD nano, micro/personal (NMP) & Legacy nodes and SPD & Legacy Networks
- Results:
  - D2.3.2 the requirements and results from WP3, WP4, and WP5.
- Results:
  - Completion of D2.3.2

Task 3.1 Nano, micro/personal node

- Contributions in D3.1 for SPD NMP & Legacy Nodes, SPD & Legacy Networks, prototypes developments
- Intensive work on the SPD Node & Network technology prototypes, proof-of-concepts
- Results:

- NMPS Nodes prototypes
- Trusted NMP sensor (NMPS) Node prototypes
- Elliptic Curve Cryptography (ECC) and RSA Cryptography comparisons
- WSN composed of Trusted NMPS Nodes evaluation
- Study on SPD and other functionalities for WSNs
- Poof-of-concept for confidentiality, integrity, authenticity and system integrity

Task 3.3 Dependable self-x and cryptographic technologies

- Intensive work on dependable self-x and cryptographic technology with emphasis on HW and SW crypto technologies, comparison of different cryptography algorithms, SW-TPM.
- Results:
  - RSA Cryptography
  - ECC Cryptography
  - ECC and RSA Cryptography implementation issues
  - ECC & RSA implementation for NMPS nodes
  - Poof-of-concept for confidentiality, integrity, authenticity and system integrity

Task 4.1 Smart SPD driven transmission

- 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 compared
  - SPD mechanisms for cognitive radio
  - A final study on smart driven SPD transmission

Task 4.2 Trusted and dependable Connectivity

- 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.
- A final study for trusted and dependable connectivity with emphasis on SPD, network management and QoS issues over a hybrid heterogeneous pSHIELD networks

Task 5.1 SPD driven Semantics

- Further studies, analysis and R&D activities for detailed specifications regarding semantic ontology based on the WP2, WP3 and WP4 requirements and specifications are performed.
- Results:
  - OWL technologies

Task 5.2 Core SPD services

- Further studies, analysis and R&D activities for detailed specifications regarding core SPD service based on the WP2, WP3 and WP4 requirements and specifications are performed.
- Results:
  - Semantic Web Services
  - Service Composition

Task 5.4 Overlay monitoring and reacting system by security agents

- Further studies, analysis and R&D activities for detailed specifications regarding security agents

based on the WP2, WP3 and WP4 requirements and specifications are performed.

- Results:
  - Security agents in overlay

Task 6.1 Multi-technology system developments

- THYIA's work includes different NMPS Node prototypes, Trusted NMPS Node solutions, WSNs composed of SPD & Legacy Nodes.
- Results:
  - Some prototypes of NMPS nodes with TPM and SW-TPM are validated & verified

Task 6.2 Multi-technology validation

- THYIA's work includes different NMPS Node prototypes, Trusted NMPS Node solutions, WSNs composed of SPD & Legacy Nodes.
- Results:
  - Performance validation of some prototypes of NMPS nodes with TPM and SW-TPM with respect to the interfaces

Task 6.4 Real world requirements for SPD-based systems

- THYIA's work includes:
  1) Real-life requirements from industrial implementations,
  2) Lessons-learned for the adaptation of lab prototypes towards quasi-autonomous operations, and
  3) Analysis of industry-readiness for pSHIELD-based monitoring

for the envisaged pilot NMPS nodes and its WSNs demonstrators, developed in WP2-WP5, were integrated and demonstrated in T6.1 and T6.2.

- Results:
  - A summary of recommendations for further industry-related developments of SPD NMPS Nodes and Networks

Task 7.1 Dissemination

- Dissemination versus national authority, external communications with industry and academy (notional and international)

Task 7.2 Exploitation

- A concept for case study model for showroom for pSHIELD projects is completed

A summary progress towards objectives.

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

- completed D2.1.2
- completed D2.2.2.
- completed D2.3.2
- THYIA's pSHIELD SPD NMPS Nodes and WSNs for the Demonstrator
- Enhanced-SPD nano, mikro/personal sensor (NMPS) node system solutions
- Evaluation of the NMPS Node (HW and SW), Security and Dependability Metrics

- Evaluation of the pSHIELD WSN architecture composed of NMPS nodes for the Demonstrator
- Final study on the TinyOS, Contiki and Hydra sensor node solutions and their possible up-grade to SPD Nodes
- Final study on the pSHIELD NMP NODE Gateway (GW) solution
- The final contributions for D3.1 and D3.3 are developed
- SPD core module that include TPM, SW-TPM and MTM futures
- Secure firmware and bootstrapping with key management
- SPD NMPS prototypes are proposed for sensor nodes based on the IEEE 802.11, IEEE 802.15.4 standards
- Self-x technologies are studied in details, and possible solutions are identified -ongoing work
- Elliptic Curve Cryptography (ECC) techniques are proposed for NMPS Nodes and WSNs
- 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
- Cognitive Radio and SDR are taken in consideration for the future WSNs composed of SPD NMPS & Legacy Nodes
- Security technologies for SPD NMPS & Legacy Node & Networks are presented in details
- OWL technologies
- Lange based support for service oriented architecture – future direction
- AOA architectures
- A study on secure agent system using delegation based trust management – ongoing work

Clearly significant and tangible results

- Completion of THYIA's work in WP1, WP2, WP3, WP4, WP5, WP6 and WP7
- Responsibility for repository BSCW server development and administration
- Contributions to WP1, WP2, WP3, WP4, WP5, WP6, WP7 deliverables
- SPD system solutions for NMPS & Legacy Nodes & Networks
- NMPS Node & WSN prototype architectures (HW and SW) with Security, Privacy and Dependability Metrics
- Definition of the pSHIELD reference architecture for the Demonstrator
- Enhancements in SPD technologies for NMPS & Legacy Nodes & Networks that are used for the Demonstrator
- Elliptic Curve Cryptography (ECC) and RSA Cryptography implementation on TPM and SW-TPM
- A pSHIELD Demonstrable Network as WSNs composed of NMPS Nodes.
- Interoperability of Legacy TiniOS, Contiki and Hydra sensor nodes and their possible up-grade to SPD NMPS Nodes
- The pSHIELD Gateway (GW) solution based on micro/personal and power nodes
- An architectural solution of nano node to be implemented with 3D integration
- Cognitive Radio and SDR as new candidate for designing reconfigurable NMPS Nodes that composed a flexible pSHIELD Network with strong SPD features and a new Overlay system solution
- Studies on Semantic Ontology and Services for NMPS Nodes and Networks
- Significant contributions for the following up project nSHIELD where an original and innovative SMN (Social Mobility and Networking) scenario is proposed as a future proof-of-concept for SPD composability features, SPD functionalities and SPD core services over a SPD Networks composed

of SPD and legacy network elements and networks.

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 July 2011 – 31st December 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 = 100 % (Planned: 100%) Task 1.2 – Actual = 100 % (Planned: 100%)

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

- Task 1.1 – Project Management
  - This final project period was given to the project from the PO as an extension to the original duration. This extension needed to be managed without any extra budget to deliver this. Once the extension was approved the project needed to be replanned to ensure there was effort available to deliver the project management activities for the full project period. This was done and a large focus was spent during this period ensuring the work was delivered utilising only the available budget.
  - Within this period, the national grant agreement from FCT was completed and signed (*Fundação para a Ciência e Tecnologia*). Until this had been resolved and agreed, Critical Software regularly spent resources chasing FCT to see the status of this and pushing to get the situation finalised.
  - The second project review was held during September 2011 in Oslo. Preparation activities were carried out to prepare for this review and the required documentation that was delivered
  - *Through*out this period of the project CS ensured that, when required, a representative was available to join with the scheduled Management and Planning meetings.

- Task 1.2 – Liaisons
  - Within Critical the liaisons within this period have been done to help pSHIELD plan and execute the extension on the project without receiving further budget. The liaisons were used to take the knowledge from other projects that have done this and to apply to pSHIELD.
  - The liaison effort has helped the project gather best practice in terms of dissemination of the work done within pSHIELD. Meeting with other funded FP7 projects within Critical helped to utilise the knowledge available on best practice which was then utilised within WP7.

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 July 2011 – 31st December 2011
Effort planned in this period:	Task 2.1 – 0,0 PM Task 2.2 – 0,1 PM Task 2.3 – 0,1 PM
Effort actual or spent in this period:	Task 2.1 – 0,0 PM Task 2.2 – 0,1 PM Task 2.3 – 0,1 PM
% of work completed at the end of the period (indicative):	Task 2.1 – Actual = 100 % (Planned: 100%) Task 2.2 – Actual = 100 % (Planned: 100%) Task 2.3 – Actual = 100 % (Planned: 100%)

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

- Task 2.1
  - Work completed before the start of period 3.

- Task 2.2; Task 2.3
  - Participation in WP2 meetings (phone conferences organised by WP leader and Task leaders).
  - Review and contribution to deliverables:
    - D2.2.2 "SPD Metrics Specification" (e.g. final review and contribution to SPD metrics composition);
    - D2.3.2 "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 CS's participation in this WP was to ensure that we participated in the discussions and within the document elaboration that formed the basis of the pSHIELD work, namely the work performed within WP3, WP4, WP5 and WP6.
- In the WP Kick-Off Meeting, it was decided that CS's main task would be related with the discussion and review of the three deliverables that were to be produced. Nevertheless, CS also provided contribution to the deliverables in areas of its expertise.

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 July 2011 – 31st December 2011

Effort planned in this period:	Task 3.1 – 0,2 PM Task 3.3 – 1,1 PM
Effort actual or spent in this period:	Task 3.1 – 0,2 PM Task 3.3 – 1,1 PM
% of work completed at the end of the period (indicative):	Task 3.1 – Actual = 100 % (Planned: 100%) Task 3.3 – Actual = 100 % (Planned: 100%)

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, CS 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).
  - In this last period, the proposed work for WP3 was completed with the conclusion of the complementary studies to test the cryptographic algorithms implementation on the hardware of a micro node (TelosB mote).
  - The output of this task was used as input to the work performed in WP6 that exhibited, by means of a physical setup, a cryptographic scheme deployed on a WSN platform, allowing to demonstrate pSHIELD's composability functionality.

Beneficiary:	Critical Software - CS
Work Package(s)	**WP4 - SPD Network**
Task(s)	Task 4.2 Trusted and dependable Connectivity
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 4.2 – 2,7 PM
Effort actual or spent in this period:	Task 4.2 – 2,7 PM
% of work completed at the end of the period (indicative):	Task 4.2 – Actual = 100 % (Planned: 100%)

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 were 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.
  - The work in this task contributed to the implementation of secure communications within pSHIELD application scenario, where a cryptographic scheme deployed on a WSN platform allowed demonstrating pSHIELD's composability functionality.

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 July 2011 – 31st December 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 – 6,5 PM Task 5.3 – 0,0 PM Task 5.4 – 0,0 PM
Effort actual or spent in this period:	Task 5.2 – 6,5 PM Task 5.3 – 0,0 PM Task 5.4 – 0,0 PM
% of work completed at the end of the period (indicative):	Task 5.2 – Actual = 100 % (Planned: 100%) Task 5.3 – Actual = 100 % (Planned: 100%) Task 5.4 – Actual = 100 % (Planned: 100%)

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).
  - Implementation and validation of pSHIELD adapter bundles to allow the integration of cryptographic functionalities deployed on TelosB motes to interact with pSHIELD middleware.
  - Participation in SPD services' specification and contribution to pSHIELD demonstrator, namely in the demonstration of composability functionality.
  - The output of this task was used as input to the work performed in WP6 that exhibited, by means of a physical setup, a cryptographic scheme deployed on a WSN platform, allowing to demonstrate pSHIELD's composability functionality.

- Task 5.3
  - Work completed before the start of period 3.

- Task 5.4
  - This task was not addressed within the CS contribution (see section "Additional Information").

Additional information:

- Instigated by CS, our participation in WP5 was re-evaluated. This issue was discussed in the PA meeting held in Norway and CS 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.

Beneficiary:	Critical Software - CS
Work Package(s)	**WP6 - Platform integration, validation & demonstration**
Task(s)	Task 6.1 Multi-Technology System Developments Task 6.2 Multi-Technology Validation & Verification Task 6.3 Multi-Technology Pilot Demonstration Task 6.4 Real World Requirements for SPD-based Systems
Period:	1st July 2011 – 31st December 2011
Effort planned in this period:	Task 6.1 – 5,5 PM Task 6.2 – 1,0 PM Task 6.3 – 1,0 PM Task 6.4 – 1,0 PM
Effort actual or spent in this period:	Task 6.1 – 5,5 PM Task 6.2 – 1,0 PM Task 6.3 – 1,0 PM Task 6.4 – 1,0 PM
% of work completed at the end of the period (indicative):	Task 6.1 – Actual = 100 % (Planned: 100%) Task 6.2 – Actual = 100 % (Planned: 100%) Task 6.3 – Actual = 100 % (Planned: 100%) Task 6.4 – Actual = 100 % (Planned: 100%)

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

- Task 6.1; Task 6.2; Task 6.3; Task 6.4
  - Participation in WP6 meetings (task management and prototype setup).
  - Discussion, identification and analysis of integration of CS work within the pSHIELD application scenario: "Middleware prototype for the demonstration of composability".
  - Implementation of cryptographic algorithms and communication in wireless sensor network to support the demonstration of pSHIELD's concept of composability.
  - Design and development of pSHIELD middleware's adapter bundles to allow the interaction between the physical setup and the middleware's core SPD services (Orchestration, Composition and Discovery).
  - Integration activities within the scope of "Middleware prototype for the demonstration of composability".
  - Execution of internal validation and verification activities (internal integration) and contribution to overall scenario validation and verification activities.
  - Documentation of WP6 activities and results, and creation of video demonstration.

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 July 2011 – 31st December 2011

Effort planned in this period:	Task 7.1 – 0,1 PM Task 7.2 – 1,1 PM
Effort actual or spent in this period:	Task 7.1 – 0,1 PM Task 7.2 – 1,1 PM
% of work completed at the end of the period (indicative):	Task 7.1 – Actual = 100 % (Planned: 100%) Task 7.2 – Actual = 100 % (Planned: 100%)

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

- Task 7.1
  - As part of the Dissemination of the pSHIELD information one of the CS project team, Pedro Polonia completed and presented his Master thesis. This was based upon the work done within pSHIELD, "Abstract: this thesis provides a research study of asymmetric cryptography in the context of Embedded System."
  - In accordance with Reviewer Open Issue 7, CS reviewed pSHIELD public website and sent a list of corrections/updates to task leader.

- Task 7.2
  - Integration of results in the CS eXception Product - add capabilities in the development of safety critical design - CS is well-known by its V&V services in the safety critical domain. With pSHIELD results in SPD methods and framework it is expected that this product can go a step forward and increase general security capabilities in the design and production of high integrity software development services, targeted at testing embedded software SPD characteristics through fault injection.
  - CS built and markets a dedicated command-and-control platform for civil protection, space and security application – designated as the C&C framework – this framework also considers the integration with intelligent networked objects e.g. WSN networks. As such the integration of pSHIELD SPD features in C&C for networked embedded contexts is a strong possibility in the C&C technical roadmap.

A summary progress towards objectives.

Within **WP1** CS has worked within the project and ensured that is has been able to fulfil all of its agreed tasks within the extended duration of the project. This has been done by utilising knowledge learned through similar projects that have been through similar circumstances.

In this last period, the work performed in **WP2** focused on the review and contribution to the final versions of this WP deliverables. CS participated in WP2 meetings and contributed to the alignment of the final deliverables with the work performed in this project.

In accordance with CS's contribution shown within the Technical Annex, CS's main contribution to pSHIELD was within the areas of "*Cryptography for low cost nodes*" and "*Dependable authentic key distribution mechanisms*". These activities were 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 was performed in parallel and also involved activities within **WP5** and **WP6**.

The proposed work for WP3 and WP4 was completed with the conclusion of the complementary studies to implement and test the cryptographic algorithms implementation on the hardware of a micro node (TelosB

mote), contributing to the implementation of secure communications within pSHIELD application scenario. These activities, along with the work performed in WP5, namely in the implementation and validation of pSHIELD adapter bundles to allow the integration of cryptographic functionalities deployed on TelosB motes to interact with pSHIELD middleware, were used as input to the work performed in WP6 that exhibited, by means of a physical setup, a cryptographic scheme deployed on a WSN platform, allowing to demonstrate pSHIELD's composability functionality. This demonstration was materialised in the "Middleware prototype for the demonstration of composability". WP6 activities included not only the design, implementation and documentation of the prototype but also its validation and verification. Within WP7 CS has focused on 2 main ways to disseminate and exploit the pSHIELD results. This approach has been done following a) "General use of PSHIELD results and knowledge horizontally e.g. in current projects, with the expected value of improved methodologies and tools (indirect use);" and b" Through new products, tools and services that can be marketed directly to other organizations (direct use)."
Deviations between actual and planned person-months: 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, CS 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 were managed at the WP level by the WP leaders and by the Technical Manager.

4 Deliverables and milestones tables

4.1 Deliverables (excluding the periodic and final reports)

Table 2 – 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
D3.1	SPD node technologies prototype	3	SESM	P,O	PP	15	Yes	15	
D5.1	pSHIELD semantic models	5	TRS	R	PP	15	Yes	15	
D5.2	SPD middleware and overlay functionalities prototype	5	UNIROMA1	P,O	PP	15	Yes	15	
D2.1.2	System Requirements and Specifications	2	ASTS	R	PU	15	Yes	15	
D2.2.2	SPD Metrics Specifications	2	TEC	R	PU	15	Yes	15	
D2.3.2	System Architecture Design	2	HAI	R	PU	15	Yes	15	
D3.2	SPD nano, micro/personal node technologies prototype report	3	THYIA	R	PU	16	Yes	16	
D3.3	SPD power node technologies prototype report	3	ETH	R	PU	17	Yes	17	

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
D3.4	SPD self-x and cryptographic technologies prototype report	3	AS	R	PU	16	Yes	16	
D4.1	SPD network technologies prototype	4	SE	P,O	PP	13	Yes	13	
D4.2	SPD network technologies prototype report	4	MGEP	R	PU	16	Yes	16	
D5.3	pSHIELD semantic models report	5	SE	R	PU	16	Yes	16	
D5.4	SPD middleware and overlay functionality report	5	SE	R	PU	16	Yes	16	
D6.1	Platform development report	6	HAI	R	PU	17	Yes	19	
D1.1.5	Quality Control Report	1	MAS	R	PU	19	Yes	19	
D1.2.1	Liaisons Report	1	SESM	R	PU	19	Yes	19	
D6.2	Platform component validation and verification	6	SE	R	PU	18	Yes	18	
D6.3	pSHIELD pilot demonstrators	6	ASTS	R,P,O	PU	17	Yes	18	
D6.4	Real world requirements for SPD-based systems	6	ASTS	R	PU	19	Yes	19	
D7.1.2	Dissemination Report	7	SESM	R	PU	19	Yes	19	

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
D7.2.1	Exploitation Plan	7	MAS	R	PU	19	Yes	19	

4.2 Milestones

Table 3 – 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
M4	SPD Metrics, system architecture design and preliminary SPD prototypes	WP2, WP3, WP5	SESM, TRS, UNIROMA1, TEC, HAI	15	Yes	15	
M5	SPD prototypes	WP3, WP4	SESM, AS, MGEP	16	Yes	16	
M6	SPD prototypes and pSHIELD platform integration	WP3, WP6	ETH, HAI	17	Yes	16	
M7	pSHIELD platform validation and verification	WP6	SE, ASTS	18	Yes	19	
M8	Final demos	WP6	ASTS	19	Yes	19	

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 planned, the meetings and phone conferences (described below) of appropriate level were scheduled, the technical description of the work and the Consortium Agreement were maintained, the electronic media were maintained including website, collaborative tools, document repository and e-mail list. 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. Official acceptance of PC change has been communicated by Project Officer on 5 August 2011. MAS took the administrative part of the coordination including correspondence to internal agreement mentioned in the Annex I to the JU Artemis Grant Agreement, while SESM took care of the technical part of the coordination.

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):

In 3rd reporting period of the pSHIELD project, as well as in previous periods, Project Phone Conferences (PhCs) and Project Meetings were organised on regular basis. Depending on necessity some of PhCs were at Project Assembly level, or TCM level. Those regular events allowed on smooth information exchange between project consortium. Lists of events with dates are given below.

List of meetings:

- 12-13 July 2011 Consortium Meeting in Rome
- 28 September 2011 Pre-Review Meeting in Oslo
- 29-30 September 2011 2nd Review Meeting in Oslo

List of Phone Conferences:

- 2 September 2011 Project PhC,
- 15 September 2011 Project PhC,
- 6 October 2011 Project PhC,
- 12 October 2011 Project PhC,
- 24 November 2011 Project PhC,

- 14 December 2011 Project PhC.
- 25 January 2012 Project PhC.

5.5 Project planning and status

Project activities ended with seven months of delay, according to the extension that has been requested 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 got 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 Cost deviations

5.8 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.

5.9 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.

5.10 Dissemination and exploitation activities

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

5.11 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 into the 3th period

Here below Person-Month Status and Cost tables are reported. Explanations on deviations in the use of resources are reported in § 7 and related beneficiaries forms.

Table 4 – Person-Month Status Tables

Person-Month Status for the Period																			
Contract N. 100204																			
Acronym: pSHIELD																			
Period: 01/07/2011-31/12/2011																			
		Total	SESM	ASTS	SE (ex ED)	ETH	SE (ex SCOM)	TRS	UNIGE	UNIROMA1	AS	TECNALIA	MGEP	ATHENA	HAI	CWIN	MAS	THYIA	CS
Work package 1:	Actual WP total	**23,87**	16,00	2,00	0,60	0,50	0,50	0,25		0,40	0,50	0,10	0,12				2,00		0,90
Management	Planned WP total	**21,37**	16,00	2,00	0,60	0,50	0,50	0,25		0,40	0,00	0,10	0,12				0,00		0,90
Work package 2:	Actual WP total	**4,55**		1,85								1,00			1,00			0,50	0,20
SPD Metrics, requirements and system design	Planned WP total	**4,55**		1,85								1,00			1,00			0,50	0,20
Work package 3:	Actual WP total	**41,80**	10,00			9,00					8,50					2,50		10,50	1,30
SPD Node	Planned WP total	**30,80**	10,00			9,00					6,00					0,00		4,50	1,30
Work package 4:	Actual WP total	**11,90**					4,00		1,00			0,10	1,00					3,10	2,70
SPD Network	Planned WP total	**10,40**					2,50		1,00			0,10	1,00					3,10	2,70
Work package 5:	Actual WP total	**30,91**			12,90			2,00		4,00								5,51	6,50
SPD Middleware & overlay	Planned WP total	**30,91**			12,90			2,00		4,00								5,51	6,50
Work package 6:	Actual WP total	**72,44**	9,00	17,94	8,00	2,00	0,50							3,50	5,00	3,50	0,50	14,00	8,50
Platform integration, validation & demonstration	Planned WP total	**95,94**	9,00	17,94	8,00	2,00	0,50							4,00	20,00	5,00	1,00	20,00	8,50
Work package 7:	Actual WP total	**16,23**	4,00	3,75	1,00		1,00					0,13	0,10	0,50		0,50	1,00	3,05	1,20
Support activities	Planned WP total	**15,73**	4,00	3,75	1,00		1,00					0,13	0,10	0,50		1,00	0,00	3,05	1,20
	Actual total	**201,70**	**39,00**	**25,54**	**22,50**	**11,50**	**6,00**	**2,25**	**1,00**	**4,40**	**9,00**	**1,33**	**1,22**	**4,00**	**6,00**	**6,50**	**3,50**	**36,66**	**21,30**

Tables 4.1 – Personnel, Subcontracting And Other Major Direct Cost Items

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SESM FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 3, 6, 7	Personnel costs		66.513,95 €	131.500,00 €	198.013,95 €	Internal staff
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs		9.472,00 €		9.472,00 €	Equipment
TOTAL DIRECT COSTS			75.985,95 €	131.500,00 €	207.485,95 €	
TOTAL INDIRECT COSTS			33.256,98 €	65.750,00 €	99.006,98 €	Overhead for personnel costs (rate 50%)

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ASTS FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,6,7	Personnel costs		86.361,33	46.537,82	132.899,15	Salaries of 3 engineers and 6 senior engineers.
	Subcontracting		31.205,23		31.205,23	Two subcontracting for development and experimentation of demonstrator
	Other costs			5719,1	5719,1	Materials for realization of demonstrator (sensor kit)
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			117.566,56	52.256,92	169.823,48	
TOTAL INDIRECT COSTS			43.180,66	23.268,91	66.449,57	Overhead rate 50% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SELEXELSAG (EX-ELSAGDATAMAT) FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,5,6,7	Personnel costs		€158.756		€158.756	22,5 PM for 3 senior researchers and 2 analysts
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			€158.756		€ 158.756	
TOTAL INDIRECT COSTS			€ 79.378		€ 79.378	Overhead for personnel costs (rate 50%)

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ETH FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 3, 6	Personnel costs		30000 €	22000 €	52000 €	Salary of engineers involved in research, design and development activities. Salary of personnel involved in management activities.
	Subcontracting		102602 €	74056,43 €	176658,43 €	Rugged mechanical enclosure design, internal rack mechanical design, cold plate mechanical design, PCB design and development, final prototypes development and production.
	Consumable		32000 €	14915,27 €	46915,27 €	Prototypes design and production
TOTAL DIRECT COSTS			164602,00 €	110971,70 €	275.573,70 €	
TOTAL INDIRECT COSTS			15000 €	11000 €	26000 €	Overhead for personnel costs (rate 50%)

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY SELEXELSAG (EX-SCOM) FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
2, 4	Personnel costs		33600€		33600€	
	Subcontracting		21000€		21000€	Development of embedded experimental platform.
	Major cost item 'X'					
	Major cost item 'Y' …….					
	Remaining direct costs					
TOTAL DIRECT COSTS			54600€		54600€	
TOTAL INDIRECT COSTS			16800€		16800€	overhead rate 50% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TRS FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,5	Personnel costs		€ 1.123,66	€ 8.221,42	€ 9.345,08	Salaries of 1 senior systems engineer, 2 junior systems engineer and one director for a total of 6 months
	Subcontracting					
	Consumables					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			€ 1.123,66	€ 8.221,42	€ 9.345,08	
TOTAL INDIRECT COSTS			€ 561,83	€ 4.110,71	€ 4.672,54	Overhead rate 50% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIGE FOR THE PERIOD 01/07/2011 – 31/12/2011						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
4	Personnel costs		2500.00		2500.00	0.5 PM Assistant Professor
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			2500.00		2500.00	
TOTAL INDIRECT COSTS			975.00		975.00	overhead rate 39% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY UNIROMA1 FOR THE PERIOD 01/07/2011 – 31/12/2011						
Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 5	Personnel costs		34.490,45		34.490,45	4,4 PM for 4 professors and 3 researchers
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs (Adjustment to previous period)					
TOTAL DIRECT COSTS			34.490,45		34.490,45	
TOTAL INDIRECT COSTS			17.245,23		17.245,23	overhead rate 50% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY AS FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1, 3	Personnel costs		36.728,51 €		36.728,51 €	Salaries for project manager and project engineer
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			36.728,51 €		36.728,51 €	
TOTAL INDIRECT COSTS			7.360,39 €		7.360,39 €	overhead rate 20% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY TECNALIA FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,4,7	Personnel costs		9.630,38€		9.630,38€	Salaries cost for 1,23 p/m
	Subcontracting					
	Major cost item 'Travel'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			9.630,38€		9.630,38€	
TOTAL INDIRECT COSTS			1926,08€		1926,08€	overhead rate 20% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY MGEP FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,4,7	Personnel costs		6246,4€		6246,4€	Salary researchers
	Subcontracting					
	Major cost item 'X' ……..					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			6246,4€		6246,4€	
TOTAL INDIRECT COSTS			1249,28€		1249,28€	20% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY ATHENA FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
6,7	Personnel costs		11.000,00€		11.000,00€	Internal staff
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' ……..					
	Remaining direct costs					
TOTAL DIRECT COSTS			11.000,00€		11.000,00€	
TOTAL INDIRECT COSTS			2.200,00€		2.200,00€	Overhead for personnel costs (rate 20%)

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY HAI FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,6	Personnel costs		28.483 €		28.483 €	Salaries (6,5 PMs)
	Subcontracting					
	Major cost item 'X'					
	Major cost item 'Y' …….					
	Remaining direct costs					
TOTAL DIRECT COSTS			28.483 €		28.483 €	
TOTAL INDIRECT COSTS			3.370 €		3.370 €	11,83% of personnel costs

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY CWIN FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
3,6,7	Personnel costs		60.511 €		60.511 €	salary for researchers
	Subcontracting					
	Remaining direct costs					
TOTAL DIRECT COSTS			60.511 €		60.511 €	
TOTAL INDIRECT COSTS						

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY MAS FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,6,7	Personnel costs		€ 10.621		€ 10.621	Salary for researchers
	Subcontracting					
	Other direct costs					
	Remaining direct costs					
TOTAL DIRECT COSTS			€ 10.621		€ 10.621	
TOTAL INDIRECT COSTS						

these numbers are wrong and do not coincide with the numbers in the word report (v7.doc), sent from Antonio to Spase on Wednesday, February 29, 2012 11:56 AM

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY THYIA FOR THE PERIOD 01/07/2011 – 31/12/2011*

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3,4,5, 7	Personnel costs		€ 347190		€ 347190	Salary of THYIA employees: 3 senior managers, 4 young researchers and administrative supporting personnel
	Subcontracting as defined in TA		€ 51248		€ 51248	
	Other direct cost		€ 53603		€ 53603	Travels, consumable, materials,buildings,indirect
TOTAL DIRECT COSTS			€ 452041		€ 452041.	
TOTAL INDIRECT COSTS			0		0	

TABLE 4.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY CS FOR THE PERIOD 01/07/2011 – 31/12/2011

Work Package	Item description	Amounts				Explanations
		Fundamental research	industrial research	Experimental development	Total	
1,2,3,4,5, 7	Personnel costs		€ 81.033,06		€ 81.033,06	This has corresponded to the full resources used within the scope of the pSHIELD project during this reporting period.
	Subcontracting					
1	Travel costs		€ 1.919,00		€ 1.919,00	These costs have been incurred during CS 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			€ 82.952,06		€ 82.952,06	
TOTAL INDIRECT COSTS			€ 16.206,61		€ 16.206,61	20% of personnel costs

7 Deviation of the use of the resources

This section has been included in order to give to the officer a clarification about some cost/resources discrepancies found during the final pSHIELD meeting on Feb14th 2012 held in Brussels. As indicated into the "pShield-FinalReview_ClosingRemarks.doc" section *final assessment*,

"Globally the outcome of the work packages justify the effort. There are some discrepancies in the effort figures which need justification. This is expected in a resubmitted final project progress report, deadline: End of February 2012. Please remember that any deviation planned/actual of more than 10% requires explicit explanation. Also the subcontractor efforts needs clarification". The aims of this section is to give a better visibility about any effort deviation as well as use of subcontracting, made by any partners overall the project, from 31th June 2010 until 31th December 2011.

The table 5 includes detailed information about the MM spent by the partner in every WP as well as during the full duration of the project. An additional row "Actual Total" reports Actual Total effort spent. Analizying the table 5, we have that the project required an extra effort of 2.63 MM.

The total 2.63 MM of extra effort comes from the overspending of some partners. In other words, not all the partners have spent more than it was estimated. In particular, the list of the partners that have generated such deviation are:

- UNIGE
- UNIROMA
- SE (ex SCOM)
- ASTS
- MAS
- AS
- EUROTECH
- THYIA

Almost all of the partners, listed above, had an overspending condition due of prototypical demonstrators' development. Even though, the project aims to demonstrate some of SHIELD concepts and its theoretical validity; at certain point, the project turned into a deeper analysis and a more sophisticated prototypes implementation. Such kind of project re-orientation has been necessary to overcome the critical point reached by the project during its first stage.
Nevertheless, there is a double positive effect of such overspending, first, the extra effort spent by the all the partners gave a clear sign of validity of the SHIELD idea, and, second, it gave a better input and a stable starting point for the new project nSHIELD.

Every partner listed above has indicated a ration justification of that extra effort.

1. UNIGE
University of Genova and Selex Elsag worked on the pSHIELD project more than initially expected mainly because of the internal WP4 prototypical demonstrator. This activity was not initially expected within this pilot project that was more focused on theoretical studies. After the first phase of the roject however, the whole consortium and WP4 agreed that a real running implementation of cognitive radio concepts on an embedded system would have been useful for preliminary demonstrating the feasibility and effectiveness of the proposed approach.

2. UNIROMA
The deviation from the planned effort by UNIROMA1 is due, first of all, to additional work performed after the first review meeting, necessary to produce the extra deliverables which were requested by the reviewers to justify the prosecution of the project. Since UNIROMA1 has conceived most of the pSHIELD concepts (that are basically at WP5 level), it has been responsible of most of the contributions to the documents M0.1 (Formalized Conceptual Models of the Key pSHIELD Concepts) and M0.5 (the pSHIELD focus areas, the key innovations and project outputs). The additional resources were used to elaborate formal models of pSHIELD concepts and to formalize the key innovations and focus areas. These outputs have been used by all the other participants as guidelines for the prosecution of pSHIELD and will be utilized also by the nSHIELD consortium.

Secondly, during the project execution, Middleware technologies have shown to be the major pSHIELD enablers and their importance increased so much that focused architectural and Verification/Validation activities (tailored on WP5 outputs and agreed with the WP5 leader), have been introduced to consolidate the already achieved results and to put strong basis to the future nSHIELD research, in a strategic perspective. In particular:
- regarding the architectural activities, some additional UNIROMA1 work was necessary to review/enrich the pSHIELD requirements and to elaborate, in a formal language like UML, the reference architecture for pSHIELD system and components, compliant with the composability mechanism implemented at middleware level.
Even if these activities have been performed in the scope of WP5, their outputs have been collected by WP2 partners as inputs to D2.1.1 (System Requirements and Specifications) and D2.3.1 (Preliminary System Architecture Design);
- regarding the validation and verification activities, the UNIROMA1 additional effort was motivated by the lack of an integrated demonstrator able to validate in a common platform all the developed technologies; in fact UNIROMA1 has spent some extra effort to set up a specific WP5 demonstrator (OSGI platform interoperable with Critical Software nodes and enriched by TRS reasoner), to achieve the validation and verification of Middleware technologies included in no other platform.
Even if these activities have been performed in the scope of WP5, their output has been adopted by WP6 partners as inputs to D6.2.1 (Platform validation and verification) and D6.3 (pSHIELD Pilot Demonstrators).

3. SE (ex SCOM)

University of Genova and Selex Elsag worked on the pSHIELD project more than initially expected mainly because of the internal WP4 prototypical demonstrator. This activity was not initially expected within this pilot project that was more focused on theoretical studies. After the first phase of the project however, the whole consortium and WP4 agreed that a real running implementation of cognitive radio concepts on an embedded system would have been useful for preliminary demonstrating the feasibility and effectiveness of the proposed approach.

4. ASTS

The increase of the effort by Ansaldo STS is mainly motivated by the choice – not planned since the beginning – to implement and test a working prototype of the demonstrator (i.e. the freight car monitoring system) in a real railway environment. That choice, also shared with the project officer, allowed both us and the potential end-users (i.e. the Italian railway authority) to clearly appreciate in a crucial project phase the benefits achievable from the adoption of the pSHIELD architecture. The on-the-field experimentation requested an extra effort as well as a different skill category of the resources employed. Those resources had a significantly lower profile with respect to the average planned in the proposal phase; however, their commitment has been higher due to the many tasks associated to safety documentation, sensor installation, trial runs, data monitoring, acquisition and analysis. The actual amount of effort we spent in the project is 70,44 MM instead of the 75,29 MM considered in the final review meeting

Considered that the quality of results fulfilled the expectations of project evaluators as arose during the final project review and that the overall costs have not significantly increased, Ansaldo STS is confident that the justifications here reported can satisfy the clarifications requested by the project evaluators and is fully available to provide any additional information

5. MAS

Both the increased effort in prototypical demonstration and the new role as administrative project manager caused the overspending. Movation used in Q3-Q4 about five times the foreseen budget, which was taken from internal funds. The total spendings in Movation were about double (211 kEUR) as compared to the planned budget (108 kEUR).

6. AS

The design, engineering and manufacturing of the developed modules has required more effort than initially planned, due to the nature of the associated works and the different trials performed. Nevertheless, the total budget has not been modified.

More than one prototype has finally been manufactured, and this had lead to more effort. We have spent around 3PM more than originally planned but have not reported any components cost. Our total budget according to the proposal was 115.800€, and we have finally justified 121.629 €. The deviation is around 5% of the budget. And the modification between concepts (personal-consumables) around 11%.

7. Eurotech

The costs for subcontracting activities have been increased with respect to the planned budget as a consequence of the inadequacy of the external service selected for the production of the Power Node prototypes. The external service was selected because Eurotech has two contracts already ongoing with the service before pSHIELD project beginning. Unfortunately, the experience acquired with these contracts was very negative. The situation emerged about at M6 and, considering the duration of the project (only one year) and the time required to identify another external service that fully satisfies project requirements, Eurotech decided to try to produce the Power Node prototypes internally. The company of the Group identified for this task is Advanet (Japan): the background and the production facilities of this company are the more suitable in Eurotech Group for Power Node prototypes production. However, the additional effort required to acquire the missing expertise, to setup a development team, to setup a production process and to adapt the production facilities translates in additional costs. Eurotech was aware of the difficulties of this approach and of the possible ineligibility of the increased costs but, considering the urgency of the situation and the importance of the Power Node for the company, decided to proceed with this solution. The results of the project activities and the final value demonstrated by the Power Node prototype, that will be included in the Eurotech product portfolio, demonstrated that this decision has been a good choice for pSHIELD project and for Eurotech Group.

8.THYIA

The National Funding Authority (NFA) not accepted cost claims for the full extension ofthe project as it was approved by the JU Artemis. THYIA's claimed cost period that was accepted by NFA is only 15 months instead 19 months. This difference introduced inconsistence between the costs reported to NFA and JU Artemis (as above). Also the cost categories between NFA and JU Artemis as they are defined in the NGA and GA are not exactly the same.

Table 5 – Person-Month Status Tables

Person-Month Status for the Project																			
Contract N. 100204																			
Acronym: pSHIELD																			
Period: 01/06/2010-31/12/2011																			
		Total	SESM	ASTS	(1)SE (ex ED)	(2)ETH	SE (ex SCOM)	TRS	UNIGE	UNIROMA1(3)	AS	TECNALIA	MGEP	ATHENA	HAI	CWIN	MAS	THYIA	CS
Work package 1:	Actual WP total	**62,50**	36,00	4,00	3,00	2,00	4,00	1,00	0,00	1,90	1,00	1,10	0,50	0,00	0,00	0,00	3,00	2,00	3,00
Management	Planned WP total	**61,50**	36,00	3,00	3,00	2,00	4,00	1,00	0,00	2,00	1,00	2,00	0,50	0,00	1,00	0,00	1,00	2,00	3,00
Work package 2: SPD Metrics, requirements and system design	Actual WP total	**86,80**	7,00	22,00	8,00	12,00	1,00	0,00	0,00	0,00	0,00	6,30	0,00	3,00	9,00	3,00	0,50	11,00	3,00
	Planned WP total	**76,00**	9,00	14,00	8,00	12,00	1,00	0,00	0,00	0,00	0,00	2,00	0,00	3,00	9,00	4,00	0,00	11,00	3,00
Work package 3:	Actual WP total	**155.50**	30,00	0,00	0,00	43,00	0,00	0,00	0,00	0,00	23,00	0,00	0,00	4,00	0,00	9,00	1,50	17.80	18,00
SPD Node	Planned WP total	**143,80**	29,00	0,00	0,00	42,00	0,00	0,00	0,00	0,00	20,00	0,00	0,00	4,00	0,00	7,00	2,80	21,00	18,00
Work package 4:	Actual WP total	**67,30**	0,00	0,00	0,00	0,00	20,50	0,00	16,60	0,00	0,00	0,20	8,00	2,00	0,00	0,00	0,00	6.40	12,00
SPD Network	Planned WP total	**61,00**	0,00	0,00	0,00	0,00	18,00	0,00	12,00	0,00	0,00	1,00	8,00	2,00	0,00	0,00	0,00	8,00	12,00
Work package 5:	Actual WP total	**114,30**	0,00	0,00	37,00	0,00	0,00	14,00	0,00	26,30	0,00	1,00	0,00	0,00	0,00	4,00	1,00	9,76	20,00
SPD Middleware & overlay	Planned WP total	**116,00**	0,00	0,00	37,00	0,00	0,00	14,00	0,00	22,00	0,00	1,00	0,00	4,00	0,00	7,00	0,00	11,00	20,00
Work package 6: Platform integration, validation & demonstration	Actual WP total	**123,42**	9,00	38,69	13,00	4,00	1,00	0,00	0,00	0,00	0,00	0,00	0,00	3,50	5,00	8,50	2,50	18,00	9,00
	Planned WP total	**128,50**	9,00	29,00	13,00	4,00	1,00	0,00	0,00	0,00	0,00	3,00	0,00	5,00	20,00	6,00	4,50	25,00	9,00
Work package 7:	Actual WP total	**31,08**	7,00	5,75	2,00	0,00	1,00	0,00	0,00	0,00	0,00	0,33	0,50	1,00	0,00	1,50	3,00	6,00	3,00
Support activities	Planned WP total	**27,20**	6,00	4,00	2,00	0,00	1,00	0,00	0,00	0,00	0,00	1,00	0,50	1,00	0,00	2,00	0,70	6,00	3,00
	Actual total	**616,63**	**89,00**	**70,44**	**63,00**	**61,00**	**27,50**	**15,00**	**16,60**	**28,20**	**24,00**	**8,93**	**9,00**	**13,50**	**14,00**	**26,00**	**11,50**	**70,96**	**68,00**
	Planned total	**614,00**	**89,00**	**50,00**	**63,00**	**60,00**	**25,00**	**15,00**	**12,00**	**24,00**	**21,00**	**10,00**	**9,00**	**19,00**	**30,00**	**26,00**	**9,00**	**84,00**	**68,00**

(1) The total number of man month spent is smaller than presented in the previous version of table 5, due to an error in the second Beneficiary Report. The second Beneficiary Report had an error into the "Effort Planned for the Period" (46.5MM) as well into the "Effort actual or spent in this period" sections (40.5). The correct value is indicated into the "PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY

ELSAGDATAMAT FOR THE PERIOD 1.01.11 – 30.06.11" 15.99 MM. The extra effort was generate by the set of wrong data used into the final report. Now the final report has been updated with reviewed data.
(2) The total number of man month actually spent is smaller than the one presented in the previous version of table 5, because of an error in the second Beneficiary Report. The second Beneficiary Report considers the man months spent during the first 12 months (not the second semester) and reports the totals of the first year of project

(3) This summary of effort table includes also some UNIROMA1 activities performed in the period M1-M7 that have correctly been reported in the individual participant report uploaded on the BSCW server, but that went lost in the integration of the first management report. As final adjustment, they are mentioned again here in the final report. In particular, they are: 0.3 PM for 1 professor and 1 researcher for management activities in the scope of WP1. The associated personnel costs are € 1.531,00 (direct costs) plus € 765,50 (indirect costs) of industrial research.

8 Beneficiaries without a corresponding National Grant Agreement Financial statements – Form C and Summary financial report

Separate financial statement (Form C) from each beneficiary not having concluded a Grant Agreement with the respective National Authority will not be submitted in the frame of this periodic report.

7.1 Certificates

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