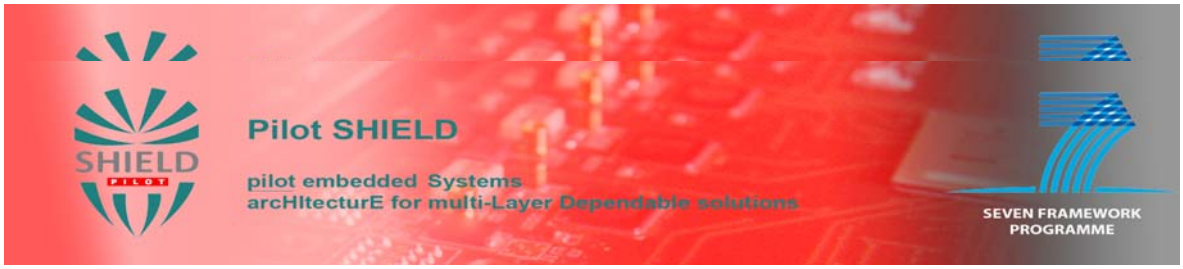

Project no: 100204

p-SHIELD

pilot embedded Systems architecture for multi-Layer Dependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems (including railways)

M0.5
The pSHIELD focus areas, key innovations and project outputs

Due date of deliverable: M9
Actual submission date: M9

Start date of project: 1st June 2010 Duration: 19 months

Lead Editor: Movation AS

Reviewed v1.0

Document Authors and Approvals			
Authors		**Date**	**Signature**
Name	**Company**		
Przemek Osocha	SESM		
Fabrizio M. de Seta	Elsag Datamat		
Andrea Fiaschetti	University of Rome		
Paolo Azzoni	ETH		
Jose Verissimo	Critical Software		
Mohammad M. R. Chowdhury	CWIN		
Spase Drakul	THYIA		
Gordana Mijic	THYIA		
Renato Baldelli	Elsag Datamat		
Andrea Morgagni	Elsag Datamat		
Francesco Flammini	ASTS		
Nikolaos Pappas	HAI Corp		
Josef Noll	Movation		
Reviewed by			
Name	**Company**		
Vincenzo Suraci	UNIROMA1		
Paolo Azzoni	ETH		
Approved by			
Name	**Company**		
A.Di Marzo	SESM		

Modification History		
Issue	**Date**	**Description**
Draft v05	30 March 2011	TOC established and work distribution
Draft v06	4 April	consolidated inputs
Draft v07, v08	12-13 April	Incorporated WP contributions and new timeline, gant
Draft v090-096	14 April	Merged all comments
Reviewed v1.0	15 April	Review comments included

Contents

Executive Summary

During the MidTerm Review, performed on 22. March 2011 at the JU premises in Brussels, the consortium was requested to produce and deliver 6 additional documents lasted by 15.4.2011.

This document M0.5 answers the request for *delivering a document listing – for each of the focus areas – which lists the key innovations which the project commits to deliver by its completion; the project outputs and its tangible results with a delivery time plan to allow close and timely monitoring of the project evolution.*

The document first provides first a listing of the six focus areas, and then provides for each of the focus areas a listing of the key innovations and the outcome. The main deliverables carrying the information of these documents are listed, and followed by a description on how the topics are going to be implemented in pSHIELD.

The final chapter of this document provides in a concise way the monitoring capabilities for the pSHIELD project through tables. Table 1 provides a link between focus areas and workpackages, and table 2 lists the main innovations in these key areas. An own section lists the new milestones of the project, points out the achievements and the list of deliverables due at that point in time. Based on these milestones an updated gant chart is presented, and finally a list of deliverables is provides, including the name of the responsible author.

We believe that this document provides a list of innovations and outcomes which the project commits to deliver by its completion. It further provides the tangible results with a delivery time plan to allow close and timely monitoring of the project evolution.

1 Introduction

The **overall objective** of the pSHIELD project is to design and implement a modular, composable framework able to provide enriched Security, Privacy and Dependability (SPD) in the context of heterogeneous Embedded Systems, aiming at achieving target SPD levels identified on the grounds of the requirements of the considered scenarios. In addition, the pSHIELD project has the ambitious long-term objective of enabling and easing the Security, Privacy and Dependability certification for all the future systems developed in compliance with the pSHIELD reference guidelines.

The pSHIELD consortium has proposed (see technical Annex) to achieve the above-mentioned overall objective through the development of **six innovative key concepts**, namely:

- an ad hoc SPD multi-layered approach allowing to define, at each layer, the pSHIELD-specific functionalities necessary to be installed, at such layer, in a legacy Embedded System Device (ESD), so that it becomes "pSHIELD-compliant" and can hence take advantage of the features introduced by pSHIELD;
- the introduction of a pSHIELD-specific layer referred to as Overlay, able, on the basis of the monitoring of SPD related inter-layer information, to take consistent and coordinated SPD decisions impacting on all the SPD layers;
- a so-called Seamless approach able to hidden Embedded Systems heterogeneity;
- the so-called Composability, namely the possibility to compose different (even heterogeneous) SPD functionalities so that the resulting composed framework achieves a target SPD level;
- the introduction of innovative SPD functionalities able to enrich the SPD features of the legacy Embedded System Devices;
- the definition of SPD Metrics, fundamental for measuring the achieved SPD enhancements, for comparing the obtained SPD levels with the target ones, for enabling SPD certification, etc.

In order to actually realize the above-mentioned six key concepts, the pSHIELD consortium will make use of eight "enabling technologies". Since pSHIELD is a pilot project, it will only design and implement a subset of the functionalities necessary to fully realize the six key concepts under discussion. Nevertheless, this subset of functionalities will be carefully selected in order to provide a preliminary, but exhaustive demonstration of the effectiveness of the above-mentioned six concepts. In particular, a Railway scenario (including hazardous material monitoring) has been selected in order to validate the overall objective; so, pSHIELD should demonstrate that, thanks to the realization of the six key concepts, the achieved SPD levels succeed in matching the target SPD levels required by the considered Railway scenario.

The aim of this document is to provide the relation between the focus areas and the innovations in these focus areas which the project commits to deliver by its completion. It further provides the project outcomes and its the tangible results with a delivery time plan to allow close and timely monitoring of the project evolution. The final part of the document contains an updated list of milestones, gant chart, and the updated list of deliverables.

2 pSHIELD Focus Areas and Innovations

pSHIELD has identified 6 focus areas, where major innovations have to take place in order to achieve the goal of addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as “built in” functionality and demonstrating the data flow from sensors to “dependable access” in a collaboration infrastructure.

2.1 Focus Areas

Thus pSHIELD project will be focused on:

1) Demonstrate composability: The main novelty is the composability of SPD functionality at different layers among different technologies. The mechanism behind the composability could be investigated as well in this pilot project, at least limited to the design level

2) New technologies: A sub-set of the previous SHIELD technologies will be used to be the very first significant example of SPD composability

3) Modularity and expandability: As well as SHIELD, pSHIELD will maintain the same features, by preserving the work breakdown structure proposed in SHIELD

4) Innovative, modular, composable, expandable and high-dependable architectural framework: the pilot project will be in charge of designing the core of this architectural framework, thus leaving to a future project its refinement and development

5) Metrics: metrics are the other novelty in the SHIELD project. They can be investigated in the pSHIELD project and used to validate the first basic functionalities of the framework

6) Validate the SHIELD integrated system in one application scenario: the pilot project will validate the architectural framework by means of a reduced number of use case.

2.2 Demonstrate composability

2.2.1 Introduction

One of the most innovative pSHIELD concepts is the composability of SPD functionalities at different layers among different technologies. Composability of SPD functionalities is mandatory when designing complex architecture composed by Embedded Systems (ES). While standard procedures (common criteria1) can be adopted at design time, composability of ES SPD functionalities both at design and runtime are still under investigation and open to innovations. This is exactly the unexplored field where pSHIELD pilot aims to put the first milestones. In order to achieve the composability of SPD functionalities, it is necessary to investigate novel key innovations which are on the basis of the composability concept.

2.2.2 Key Innovations

Composability of SPD functionalities requires first of all to dominate the heterogeneity of a system of Embedded System. Different ESs provide heterogeneous node, network and middleware technologies, SPD functionalities, connection interfaces, etc. Different ESs

[1] Common Criteria Portal - http://www.commoncriteriaportal.org/

talk different languages, uses different protocols, have a different semantic knowledge of the surrounding environment and of the SPD concepts and methodologies. Heterogeneity can be dominated defining and formalizing common shared Semantic Models to have an homogenous, common understanding of the whole domain. The semantic model can be used to design the different aspects related to the Embedded Systems, using a holistic top-down approach, covering the architectural aspects, as well as the interfacing aspects. The definition of a common semantic is also precious to define common SPD metrics, in terms of identifiable and quantifiable parameters. The use of ontologies allows to abstract from the technology dependent aspects and to focus exclusively on the SPD aspects. Thus describing in an homogeneous way heterogeneous SPD functionalities, capabilities and services, by means of homogeneous SPD metrics, allows pSHIELD to compose the different SPD components, in order to guarantee a desired level of SPD, in compliance with the scenario SPD requirements.

The system abstraction obtained from a logical point of view using the ontologies must be interfaced with the real world, formed by heterogeneous technology dependent components. The pSHIELD composability concept is thus put into operation by another innovation element of the project: the Overlay interoperation with the pSHIELD Node, Network and Middleware layer Adapters. As their name suggests, these elements adapt the technology dependent legacy node capabilities, legacy network services and legacy middleware services to become innovative SPD functionalities that are pSHIELD compliant. Being pSHIELD compliant, they can be discovered and composed on the basis of measurable SPD metrics. Being innovative they can provide additional or completely novel SPD solution. The Overlay applies proper control strategies to ensure that the application scenario requested SPD level is guaranteed finding the best configuration of the available node, network and middleware SPD component, each characterized with its own SPD status. The Middleware Adapter apply the decisions taken by the Overlay, thus actuating the pSHIELD composability concepts.

A key technology enabler of composability are the core SPD services, residing in the pSHIELD Middleware adapter, which are in charge to apply the real composition of the available SPD components. Being part of the pSHIELD middleware, the core SPD services take advantage from the use of a common semantic models describing the available SPD components, their SPD functionalities, services, interfaces, context and status. The core SPD service apply two main enabling functionalities: they “sense” the system, discovering the available SPD functionalities and orchestrate their operational status and they “actuate” the Overlay decision, applying a real composition of the SPD components. The core SPD services are dynamically configured by the pSHIELD Overlay in order to apply locally the best tactic, in accordance with the global strategy planned by the Overlay.
Thus composability can be demonstrated both at design time and at runtime applying the combination of:

- discovery (static at design time, dynamic and context-aware at runtime) of available SPD functionalities, over the whole ES framework, at all level: node, network, middleware;
- composition (or re-composition in case of runtime) of the discovered SPD functionalities to best match the required SPD level of the composed functionalities;
- orchestration (only in case of runtime) of the running functionalities, to monitor their status and to collect dynamically aggregated and semantic information to be sent to the overlay to assess the current SPD level of the whole system.

2.2.3 Expected outcome

The composability concept can be demonstrated providing:

- A conceptual description of the Overlay;
- A conceptual description of the Control Algorithms;
- A conceptual description of the pSHIELD Node, Network and Middleware Adapters
- A conceptual description of the SPD components;
- A conceptual description of the Core SPD services;
- A prototypical set of composable SPD services' interfaces and functionalities specifications;

2.2.4 pSHIELD implementation

The composability concept will be demonstrated within the pSHIELD scenario, with special focus to the application scenario requirements and peculiarities. For this purpose only a limited part of the pSHIELD framework will be developed as a software architecture, providing:

- a prototypal software based middleware configuration and execution environment;
- a prototypal software implementation of the core SPD services for a design time and runtime limited to the scope of the application scenario:
  - Secure Service Discovery;
  - Service Composition;
  - Service Orchestrator;
- Node SPD Services emulator;
- Network SPD Services emulator.
- A prototypal testbed integrating the developed software component aiming to test the composability features provided by the pSHIELD core SPD services.
-

2.3 New technologies

2.3.1 Introduction

The new technologies at node level represent enabling factors on which the pSHIELD SPD "stack" can be constructed and can grow. These technologies are focused on the enrichment of pSHIELD hardware infrastructure with new SPD Nodes and on the use of their hardware SPD intrinsic features in order to provide new low level SPD functionalities.

The activities will include the demonstration of the functionalities of Nodes prototypes with no extended market use up to now (from Micro/Nano to Power) and especially their synthesized function. An important aspect will consist in the promotion of research on new technologies.

2.3.2 Key Innovations

Key innovations at node level are intended to provide SPD intrinsic features improving the hardware capabilities of the nodes. This objective is achieved designing the nodes with SPD in mind that translates in two possible approaches, both in terms of innovation and implementation: introduce onboard components that directly provide SPD features (i.e. a power supply control chip or a protected BIOS) or provide hardware elements that enable the implementation of new SPD features and that will be used indirectly at higher levels (i.e. an FPGA). On this side, the innovation moves on the solutions that exploit these hardware elements to provide new low level SPD features (i.e. cryptography or self configurability).

From the infrastructure point of view, the innovation consists in the introduction of new embedded nodes with intrinsic SPD features, functionalities and capabilities.

The key innovations at node level include:

- Introduce an embedded device, the Power Node, that provides HPC class computing power with SPD native features directly on the field, without the needs of controlled environmental conditions
- Enrich the onboard peripherals of the Power Node, in order to provide hardware components that can be exploited at the hardware level and in upper layers to increase node SPD in a more simple way (i.e. the FPGA or the IBMC) .
- Design an enclosure and a cooling system that increase the SPD of the Power Node, both in terms of environmental issues and in terms of possible physical intrusions or tampering.
- Increase the physical composability of the power node through a specific physical interface and a high speed programmable interconnection system.
- Simplify the possibility to create redundant set of Power Nodes. The redundancy increases the dependability of the pSHIELD hardware infrastructure exploiting execution segregation through hardware virtualization that, in turns, allows for protection, monitoring, disabling and replacement of malfunctioning or compromised nodes.
- Cryptography in lightweight and networked embedded devices.
- Methodologies against distributed denial of service attacks applicable to embedded devices.
- Improved cryptographic key exchange algorithm.
- Security built-in hardware mechanisms in pSHIELD node for: access control, integrity protection, secure boot, secure upgrade, secure connection, TPM compliance.
- Dependability built-in mechanisms in pSHIELD node for: recover and reconfigurability, availability, safety and integrity assurance, preventive and corrective maintenance, uninterruptible power supply assurance.

2.3.3 Expected outcome

The expected outcome follows the directions identified in the previous section:

- Implementation of a Power Node following the conceptual model defined in the document “Formalized Conceptual Models”, respecting the pSHIELD architecture definition D2.3 and satisfying the requirements identified in D2.1.1 chapter 8 "Node Requirements and Specifications".
- Provide support in terms of drivers and operating system to the Power Node hardware.
- Introduce a development kit that allow the developer to take advantage of the advanced hardware features of the Power Node, among which SPD low level features and functionalities.

- R&D within the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme:
  - o Evaluation of asymmetric cryptography algorithms and their suitability to pSHIELD;
  - o Evaluation of symmetric cryptography algorithms and their suitability to pSHIELD;
  - o Evaluation of message authentication codes algorithms and their suitability to pSHIELD.
- Software optimization of cryptographic algorithms.
- Implementation of asymmetric cryptography algorithms such as elliptic curve cryptography ECC.
- New cryptographic key exchange algorithm called “Controlled Randomness”.
- Use of packet marking and deep packet inspection methodologies that enable a node to mitigate an ongoing DoS attack through reconfiguration of the node operation characteristics as well as the network ones.
- 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.
- Development of extensive set of Node requirements that exactly follow goals of Annex I. Results contributed to deliverable D2.1.1 chapter 8 "Node Requirements and Specifications" with subchapters containing detailed references to Annex I.

2.3.4 pSHIELD implementation

pSHIELD implementation at node level will cover a subset of the node categories identified in pSHIELD and will be extended and enriched in nSHIELD project. The activities will be focused on the implementation of a Power Node class device and on the SPD feature “enrichment” of an existing Nano Node class device. In parallel, on the Power Node side, the focus will cover also new SPD technologies implemented exploiting the capabilities and features of the on board FPGA. The implementation at node level will include hardware and software prototypes.

More in details, the implementation activities will include:

- High performance embedded node, the Power Node, intended to provide high performance computing capabilities on the field with intrinsic SPD functionalities and SPD enabling features for further SPD aware development (i.e. the FPGA).
- Cryptographic scheme deployed on a WSN platform (to be later integrated in pSHIELD’s application scenario) including key exchange, authentication and secure communication.
- SPD node hardware and software implementation deployed on a FPGA platform (to be later integrated in pSHIELD’s application scenario) including selected pSHIELD features.

The most important documents related to the previous topics are:

- D2.3.2 – System Architecture Design,
- D3.2 – SPD nano, micro/personal node technologies prototype report,
- D3.3 – SPD power node technologies prototype report,
- D3.4 – SPD self-x and cryptographic technologies prototype report,
- D5.1 – pSHIELD semantic models.

2.4 Modularity and expandability

The possibility of abstracting parts of the whole pSHIELD network (forming a sub-network with the desired properties), as well as the integration of different components (per different sets of two, three etc.), will prove modularity of the pSHIELD platform. The main focus in the pilot is to show components of the architecture, allowing the demonstration of functionality such as composability and heterogeneity, which can then be integrated by the business and liaison partners.

2.4.1 Introduction

One of the biggest improvements provided by the innovative design of pSHIELD architecture is the use of a layered approach and the decomposition into atomic SPD Functionalities (see document M0.1). This allows the definition of a (very) complex system starting from its basic (decoupled) components, making their investigation more efficient. In fact the components are organised in three logical layers that are referable to the most significant industrial segment (hardware manufacturers, network devices producers and software developers) and all of them can be addressed quite independently (on a technological perspective). This approach will not lower the value of the final result, because, the formal semantic description of components as well as the composability mechanism will allow to build them together in a seamless way. This represents the modularity of our architecture.

Then, since each technology has been clearly identified and isolated, it can be enriched with further investigations and many other technologies can be added to the framework given the fact that they respect the composability features defined above. This represents the expandability of our architecture

2.4.2 Key Innovations

Key innovations for demonstrating modularity and expandability include

- the possibility of abstracting parts of the whole pSHIELD system (forming a sub-system with the desired properties), thanks to the semantic (enabling) technologies
- the possibility of composing components by means of core SPD services

2.4.3 Expected outcome

- Formal ontological model to describe the generic pSHIELD component and the SPD functionalities (limited in scope to some instances of the application scenario)
- Architectural design of a generic pSHIELD component highlighting the features that enable the composability

- Middleware services to enable discovery and composition of pSHIELD components

2.4.4 pSHIELD implementation

Handled in WP2

- Formal conceptual model of pSHIELD component

Handled in WP5

- Prototype of semantic models to describe pSHIELD components

The documents to address the issue are

D2.2.1 – pSHIELD Architecture

D5.2 - SPD middleware and overlay functionalities prototype

2.5 Innovative, modular, composable, expandable and high-dependable architectural framework

2.5.1 Introduction

Depicting Application Scenario framework and Reference Architecture design in demonstration activities addresses pSHIELD context limits definition.

The ambitious long term objective of pSHIELD is to design a framework obtained by the composition of devices and services enriched with SPD functionalities that is:

- Innovative: in the sense that the provided functionalities are a step behind the state of the art
- Modular: as described above, in the sense that SPD functionalities can be added or removed in a seamless way
- Composable: meaning that the final result is obtained by the orchestrated composition of individual (enriched) elements
- Expandable: as described above, in the sense that the design paradigm allows further enrichments and refinements.
- High-dependable: meaning that the presence of a closed loop control scheme will allow the continuous monitoring of system status and consequent continuous assuring of SPD levels to satisfy the user needs.

2.5.2 Key Innovations

The main innovations are within the definition of a reference framework, including

i) For Embedded Systems environment

ii) Obtained by the composition of individuals elements (dynamically changing)

iii) pSHIELD SPD Sub-Networks (like WSN) tailored for an application scenario

iv) Interoperability and extendibility of the PSHIELD SPD network with Legacy Nodes and Networks

v) Self-x functionality at node and network level

2.5.3 Expected outcome

- The formalization of SPD metrics as input for the composition mechanism, both at individual and overall level
- The design of closed-loop algorithms to assure the desired SPD levels
- The design of Middleware core services that enable the composition of individual pSHIELD components
- The enrichment of some SPD functionalities making them innovative

2.5.4 pSHIELD implementation

Handled in WP2

- pSHIELD reference architecture

Handled in WP5

- overlay mechanism to enable the composability
- handled in WP5, 4 and 3
- enriched SPD functionalities to provide the innovativeness of the components

Documents to address the issue

- D2.2.1 pSHIELD architecture
- D5.2 PSHIELD Middleware and overlay

2.6 pSHIELD Metrics

2.6.1 Introduction

The project aims to create a common SPD metrics capable of improving the overall SPD measure in any specific application domain. In particular pSHIELD metrics will be use to validate the first basic functionalities of the framework.

To address Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) it is essential to define the assets that these kinds of systems aim to protect.

Generally the SHIELD project assets can be categorised in two principal group, logical and physical asset. Inside these categories it is possible to define information, services and software as logical assets and human beings, hardware or particular physical objects as physical assets.

SHIELD project assets are characterized by the SPD attributes.

The importance of such assets SPD attributes is usually expressed in terms of the consequential damage resulting from the manifestation of threats .

According to the pSHIELD approaches we have built SPD metrics based on fault tolerance of pSHIELD SPD functionalities.

What does it mean? Each identified SPD functionality will be characterized by a measure that will indicate how much is valid the implementation of that particular functionality to increment the fault tolerance of a defined SPD attribute of pSHIELD system.

To obtain the SPD measure that must be attributed to the whole pSHIELD system the SPD measure of individual functionalities are composed following a defined rule.

2.6.2 Key Innovations

List of key innovations

Security, Privacy and Dependability Integration: it is proposed a feedback control system, shown in Figure 1 as a framework that can generically integrate Dependability and Security (Privacy is considered as a Family of functionality of Security as defined by the Common Criteria approach).

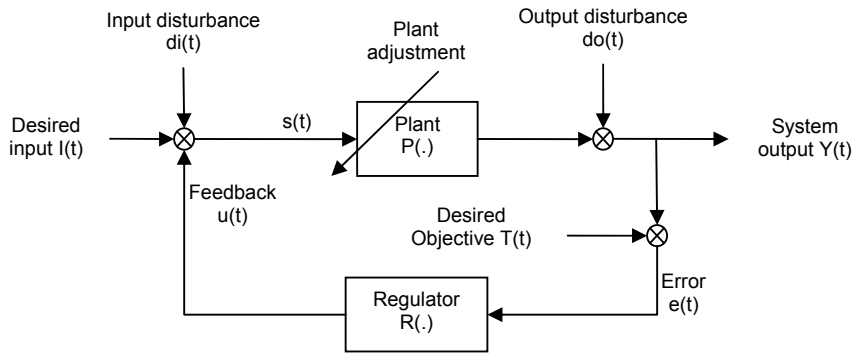

Figure 2: Feedback control system

The conventional attributes of dependability and security description can be integrated using the proposed framework.

Common Criteria (ISO15408) approach: the description of each pSHIELD SPD functionality is extracted by a catalogue of functional components that met the SHIELD compliant requirements defined for a specific system (pSHIELD). The definition of functional components follows the Common Criteria approach which categorize SPD functional components in classes and families. The Common Criteria approach is finalized to define a measure for pSHIELD SPD functionalities as shown in the following figure.

Figure 3: SPD functionality measuring process

Composability:

- We quantify the SPD of a composed system by first quantifying the SPD of its components according to Common Criteria approach and in a second step, by calculating the overall SPD following a given method. This method starts with an intuitive graphical representation of the system, and then it is converted into an algebraic expression using abstract MIN, OR and MEAN operators.

2.6.3 Expected outcome

Expected outcome is to obtain a SPD metric:

- expressed as a cardinal number;
- suggestions to achieve context-awareness;

and a consistent method to compose SPD measure which can be represented semantically.

2.6.4 pSHIELD implementation

The feasibility to obtain a measure of SPD level for pSHIELD system, will be demonstrated:

- defining a set of possible attack scenario for some SPD functionalities implemented in the pSHIELD demonstrator for the operational environment;
- achieving a vulnerability assessment and a penetration test for each defined attack scenario;
- achieving a LCSE (Life-Cycle Support Element) analysis for each available guidance;

thanks to these activities obtaining for each functionality a SPD measure and then applying the composability method proposed to have the SPD measure of the pSHIELD system.

2.6.5 handled in WPx

The handling of topics identified by “pSHIELD metrics” are WP2 and WP5.

2.6.6 Top documents to address the issue

The documents to address issue identified by “pSHIELD metrics” are D2.2.1 and D5.1.

2.7 Validate SHIELD integrated

The key innovations in validation of the integrated system is on prototypical demonstration of key aspects, covering both the demonstration of SPD-metrics as well as secure interworking at different levels. The following text outlines the approach for the architectural level.

2.7.1 Introduction

Platform Integration, Validation and Demonstration of pSHIELD system are summarized in WP6, which is highly dependent on previous technical development in WP2, WP3, WP4 and WP5. The extent of demonstration, based on actual HW in the framework of this pilot program is ongoing work.

However, consortium is exerting efforts to conduct a complete feasibility study and achieve progress towards specific developments (in all layers), preparing, also, the background for the future work in the investigation field of Security, Privacy and Dependability in the context of Embedded Systems.

Several key concepts and activities, essential for the focus of pSHIELD and the completion of a successful integration and demonstration, are presented in the next chapter, primarily as a result of the collaboration among partners and the knowledge derived.

2.7.2 Key Innovations

The key innovations in validation of the integrated system is on prototypical demonstration of key aspects, covering both the demonstration of SPD-metrics as well as secure interworking at different levels. The following text outlines the approach for the architectural level.

A basic prerequisite for Integration is the definition of a conceptual demo architecture and the description and clear definition of the modules, which are the objectives of integration. The main structure of pSHIELD system architecture is the 4 layers architecture (Node, Network, Middleware, Overlay) described thoroughly in the Technical Annex. From each layer’s basic features, the shell of the architecture is formed. These substantial characteristics provide also the project’s focus points.

Apart from the pSHIELD node, the holistic approach imposes the need to include other collaborative nodes, that we call Legacy (e.g. Legacy Embedded Devices). The modules that compose a pSHIELD node are mainly and possibly (apart from its physical entity, its HW): Operating System, Protocol Stack (SPD services, metrics, functionalities), RF component (for its communication capabilities), SW-HW Interfaces, I/O Interfaces, CPU, Sensing, Power management and other HW/SW for dedicated functions.

What is important for WP6 is the clear definition of Interfaces between different protocol layers or dedicated modules across homogeneous or heterogeneous components. The

type and nature of these interfaces, as well as, the method of implementing them, are dependent on the specific characteristics of each (per application) integration. This technology merging could concern different aspects and be implemented in HW, SW or both. For example, in case of homogeneous nodes that run different SW (serving different needs), the integration is about merging these SW modules, under the restrictions the node nature imposes (e.g. resources, memory and energy).

Network layer: pSHIELD Network performs the tasks of interconnecting subsystems and Routing information (and thus includes the suitable Communication Protocols and Standards), incorporating and propagating SPD metrics-functionalities-services. As Security is a primary focus in communication networks and in our project, Trusted data transfer is the conclusive task the whole pSHIELD architecture.

In pSRSA we have the distinction and communication between 3 elements: Legacy Embedded Device↔SPD Embedded Device↔SPD GateWay or Embedded Device↔ Poer Node ↔GateWay.

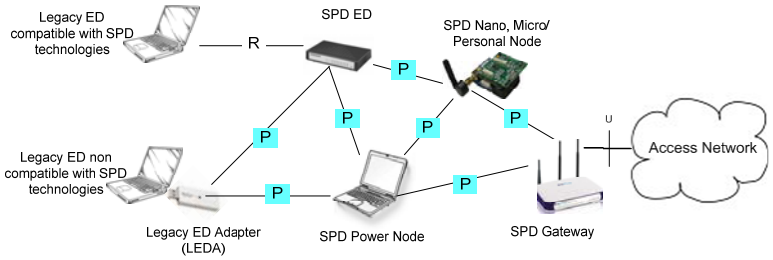

Figure 1: Communication between pSHIELD elements

Middleware layer: Middleware represents the connective software layer that provides resource management, service discovery and interoperability. It offers programming abstractions, in the service of distributed applications and is facilitated with SOA (Web Services and Stack) architectural logic. Realizations of SOA are the provided Web Services, which constitute a uniform way of discovery and provision of network services. The Web Services can be complemented with the use of Semantics. Semantics are used to achieve a more machine-oriented information representation and assist greatly Web Service lifecycle. A Policy management scheme is adopted.

Overlay layer: The notion of Security Agent is introduced to orchestrate composability functionality in pSHIELD platform. An Agent is responsible for the selection and abstraction of components that will form a functional pSHIELD subsystem, fulfilling desirable levels of SPD performance. Combining with Application Scenario, we can foresee the formation of several Security Agents to administrate the efficient SPD functionalities distribution throughout the System. As an example we can refer to the usage of IPsec protocol suite, as a “global” securing mechanism of these synthesized subsystems, whereas every component possesses its own security scheme.

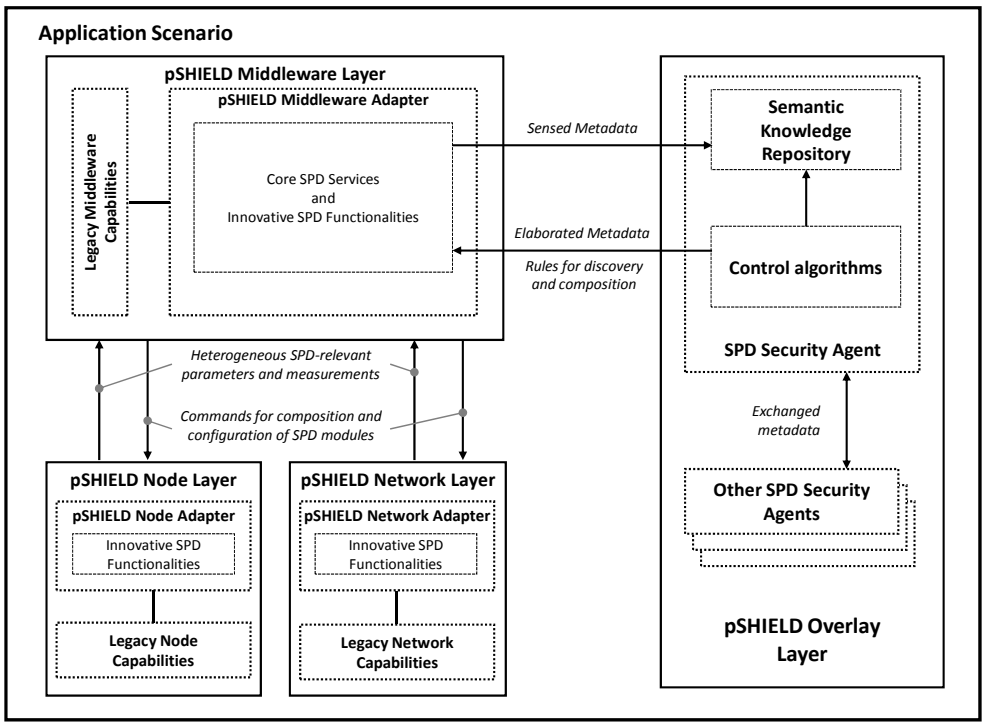

Figure 2: pSHIELD functional component architecture

Network Protocol Stack: pSHIELD proposal includes the concept of dividing the communication network in layers in a similar way the 7-layers OSI model is structured. Here the layers are four (as analysed in innumerable points in the current study): Node, Network, Middleware, Overlay. Adopting such an architectural view poses the advantages of greater modularity, robustness and ease of design of the communication system. Moving a step forward and in view of further optimization, pSHIELD proposes Cross Layer Architecture (CLA). CLA violates typical structure and rules of communications and services between layers in classical layered architectures, in favor of network performance gain. Reflection of CLA in demonstration is very important, as the inter-interface communication (whose scheme defines the exact CLA model) determines the integration of components in a multi-technology platform.

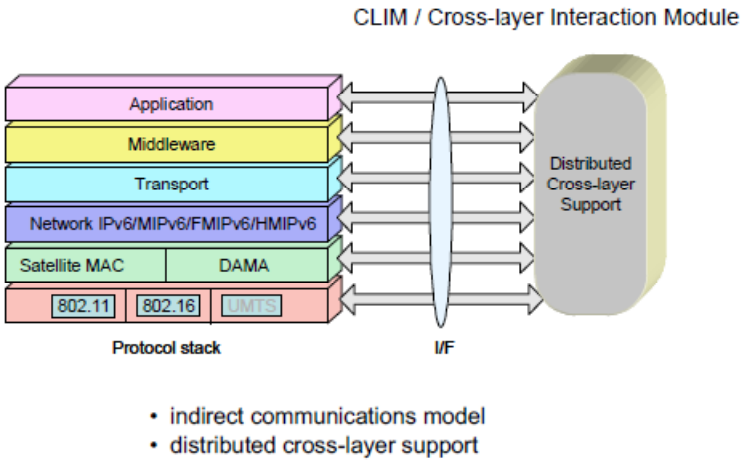

Figure 3: Cross layer interaction module

In order to demonstrate results in pSHIELD, the focus is on implementation of core components and to prototypically demonstrate the functionalities. The following section describes what can be expected from the implementation.

2.7.3 Expected outcome

The main outcome of the pSHIELD system are the multi-technology embedded system (ES) components that constitute a

- unified pSHIELD system platform which is
  - functional,
  - fulfills SPD concepts and provides an
  - usable control and application environment

In the pSHIELD system the implementation focus is on prototyping the core components. The notion of "component" of the overall architecture (which will result from the integration of all components) is mainly represented in the form of the pSHIELD node. The "final" platform construction phase begins with these components' development. Each responsible working team develops the corresponding node: a HW/SW platform, comprised from the basics and possibly extra hardware (e.g. FPGAs, Boards) or software (e.g. security algorithms), to encompass all necessary SPD capabilities.

The following components will be demonstrated in pSHIELD, subject to successful implementation.

2.7.4 pSHIELD implementation

pSHIELD implementation is handled in WP3-WP5, with an overall prototypical demonstration being handled in WP6. The most critical step in the demonstrator development is a successful system and SPD integration. Firstly, the demonstration context and extent should be defined. This is a function of available and affordable equipment, available time, components' development, careful planning, partners' collaboration efficiency. Especially concerning the technical work that has to be conducted previous to integration, all individual modules have to be described, be functional, tested separately and work properly as stand-alone entities. For example,

let's assume a set of pSHIELD Nodes with their protocol stack, choosing from a set of functionalities two, implemented with routing and security protocols (e.g. routing + intrusion detection correspondingly). They should be tested against efficient information transfer and tolerance to malicious acts.

For the pSHIELD demonstration we concentrate on SPD metrics, semantic functionality and system interoperability. The propagation of Alarms in case of abnormal environmental or operational conditions or Intrusion is one of the scenarios. It is part of a protection system that specifically addresses: Fire, Opening doors or windows, or Movements. These aspects are taken care of through the modelling and implementation of innovative aggregating SPD services. We expect to test HW components, i.e. nodes on their capability of handling SPD requirements, but the main focus is on the software. Algorithms and semantic reasoning are the means to check the SPD metrics during the integration phase.

Further aspects of the demonstrations include a HW platform enabling sensor interworking with control systems, based on a semantic middleware. The envisaged service scenario is threat protection on a system level.

Platform interoperability will demonstrate the secure interworking of prototypical platforms, from sensors over proprietary network (here JBV) over to standardised M2M platforms (here TelenorObjects)

3 Implementation in pSHIELD

The main goal of pSHIELD is addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as "built in" functionality and demonstrating the data flow from sensors to "dependable access" in a collaboration infrastructure. In order to reach the goal, advances have to be performed in six focus areas, identified in the following section.

3.1 Matrix representation of focus areas

The following table provides a summary of the focus areas, and the corresponding WPs dealing with the topics. The first focus area "composability" is a core concept in pSHIELD, and represented in all WPs. However, the main focus is in WP2, where the requirements are defined, and in WP5 where the semantic model is developed. As the pilot project focuses on prototypical implementations, the resulting composability will be demonstrated in a lab prototype (as part of WP5). A similar representation is valid for all other technical work packages, and represented in table 1.

Table 1: Focus areas and their respective workpackages

Focus area	WP2	WP3	WP4	WP5	WP6
1. Composability	++	+	+	++	+
2. New Tech	+	+++	+	+++	+
3. Modularity	+	++	+	+++	+
4. Framework	+	+	+	+	+
5. Metrics	+++	++	++	+++	++
6. Validation	+	+	+	++	+++

3.2 Focus areas and Key Innovations

The following table 2 provides a summary of the key innovations in pSHIELD, related to the identified focus areas. The table also contains the three most relevant deliverables documenting the outcome of pSHIELD, where detailed descriptions are provided in the footnotes following the table.

Table 2: Summary of key innovations per focus area

Focus area	Deliverable	Del. date	Key innovations
1. Composability	D2.2.1	M13	Metrics for security, privacy and dependability
	D5.1	M15	Semantic Model for heterogeneous environments
	D5.2	M15	Lab prototype to demonstrate composability
2. New Tech	D3.2,3.3	M17	Cryptography in lightweight and networked embedded devices; (*4)
	D4.2	M16	Intrusion detection system for wireless sensor networks (*5)
	D5.1	M15	Semantic model for secure service discovery, composition and orchestration

3. Modularity	D2.3.1 D5.2 D5.4	M13 M15 M16	System architecture for SPD functionality Concepts for heterogeneous integration through semantic technologies Policy-based management and mapping for pSHIELD (*6)
4. Framework	D2.3.1 D2.3.2 D6.4.1	M13 M16 M18	System architecture for SPD functionality Upgraded and refined system architecture Verified system architecture, integrated
5. Metrics	D2.2.1 D5.1	M13 M15	Security, Privacy and Dependability integration Common Criteria approach Definition of a composability method for SPD measure of composed system
6. Validation	D5.1 D3.4 D6.4.1 D6.2.1	M15 M16 M18 M18	Demonstrate composability Security function & behaviour testing based on intrusion detection (*7) Real Hardware platform running pSHIELD middleware (*8) Platform interoperability (*9)

Footnotes
*4 Innovations in cryptography also include improved key exchange algorithms and test of methodologies for denial of service attacks to embedded devices. For further details see M0.1, section 5.2
*5 The intrusion system will contain the metrics information, allowing for detection of abnormal behaviour
*6 Policy-based management is known from dynamic environments. However, the applicability in semantic systems has some limitations. We believe that semantic technologies need to be extended towards dynamic or quasi-dynamic environments, and will propose methods for further investigation.
*7 A combination ot nano, micro and personal node is used to demonstrate the pSHIELD security function assuming for intrusion detection
*8 Ansaldo provides a HW platform enabling sensor interworking with control systems, based on a semantic middleware. The envisaged service scenario is threat protection on a system level
*9 Platform interoperability will demonstrate the secure interworking of prototypical platforms, from sensors over proprietary (here JBV) over to standardised M2M platforms (here: TelenorObjects)

Given the current status of developments in pSHIELD, we have revised the document delivery dates and identified milestones, which are presented in the next chapter.

3.3 Milestones and Deliverables

The milestones identified in pSHIELD will ensure a monitoring capability of the achieved results in pSHIELD. The milestones support the pSHIELD goal of addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as “built in” functionality and demonstrating the data flow from sensors to “dependable access” in a collaboration infrastructure.

Milestone - M1: Project collaborative working environment established

Deliverables due at M1 (month M09): D1.1.1, D7.1.1

Milestone - M2: Draft System Requirements defined

Deliverables due at M2 (month M09): D1.1.2, D2.1.1

Milestone - M2bis: Work distribution leading to pSHIELD outcome defined in detail

Deliverables due at M2bis (month M09): M0.1, M0.2, M0.3, M0.4, M0.5, M0.6=D1.1.3.

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D1.1.1	Collaborative tools and document repository	**M09**	SESM
M0.1	Formalized Conceptual Models of the Key pSHIELD Concepts	**M09**	ED
M0.6	Management Report	**M09**	THYIA
M0.2	Proposal for the aggregation of SPD metrics during composition	**M09**	ED
M0.5	pSHIELD Focus and Outcome	**M09**	Movation
M0.4	Request for Extension of the Project	**M09**	THYIA
M0.3	Signed Endorsement	**M09**	THYIA
D7.1.1	The Project Website	**M09**	SESM

Milestone - M3: Draft design of Architecture, Prototypes for nodes identified

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D2.2.1	Preliminary SPD metrics specifications	**M13**	ESI
D2.3.1	Preliminary system architecture design	**M13**	HAI
D3.1	SPD node technologies prototype	**M13**	ETH
D4.1	SPD network technologies prototype	**M13**	SCOM

Milestone - M4: System Architecture established, Semantic Model defined

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D2.1.2	System Requirements and Specifications (Update)	**M15**	ASTS
D2.2.2	SPD metrics specifications	**M15**	THYIA
D2.3.2	System architecture design	**M15**	THYIA
D5.1	pSHIELD semantic models	**M15**	TRS
D5.2	SPD middleware and overlay functionalities prototype	**M15**	THYIA

Milestone - M5: Prototypes of micro- and personal nodes, Functional blocks of middleware defined

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D3.2	SPD nano micro or personal node technologies prototype report	**M16**	THYIA
D3.4	SPD self-x and cryptographic technologies prototype report	**M16**	CS
D4.2	SPD network technologies prototype report	**M16**	MGEP
D5.3	pSHIELD semantic models report	**M16**	ED
D5.4	SPD middleware and overlay functionality report	**M16**	ED
M1.0	Management Report at Supplementary Review	**M16**	THYIA

Milestone - M6: Prototype of power node technology, Prototype of platform

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D3.3	SPD power node technologies prototype report	**M17**	ETH
D6.1.1	Platform integration report	**M17**	HAI
D6.3.1	Lifecycle and SPD Support Report	**M17**	ATHENA

Milestone - M7: pSHIELD platform is validated against selected scenario

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
D6.2.1	Platform validation and verification	**M18**	ED
D6.4.1	pSHIELD demonstrator	**M18**	ASTS

Milestone - M8: Final reporting performed

Having reached this milestone, the following deliverables document the achievements:

	Title	Due date	Lead partner
M1.1	Annual Report	**M19**	SESM
D1.1.5	Quality Control Report	**M19**	SESM
D1.2.1	Liason Report	**M19**	SESM
D7.1.2	Dissemination Report	**M19**	SESM
D7.2.1	Exploitation Plan	**M19**	CWIN

3.4 Gant chart

These milestones lead to the updated GANT chart, provided on the next page.

ID	Task Name	Start	Finish	Duration
1	WP1 NANAGEMENT	6/1/10	12/30/11	414d
2	1.1 Project Management	6/1/10	12/30/11	414d
3	1.2 Liasons	7/1/10	12/30/11	392d
4	WP2 SPD METRICS, REQUIREMENTS AND SYTEM DESIGN	01/06/2010	31/08/2011	327d
5	2.1 Multi-technology requirements & specification	6/1/10	8/31/11	327d
6	2.2 Multi-technology SPD metrics	8/2/10	8/31/11	283d
7	2.3 Multi-technologyarchitectural design	8/2/10	8/31/11	283d
8	WP3 - SPD NODE	02/07/2010	31/10/2011	347d
9	3.1 - Nano, microlpersonal node	7/2/10	10/31/11	347d
10	3.2 - Power node	7/2/10	10/31/11	347d
11	3.5 - Composable interfaces	7/2/10	10/31/11	347d
12	WP4 - SPD NETWORK	02/07/2010	30/09/2011	326d
13	4.1 - Smart SPD driven transmission	7/2/10	9/30/11	326d
14	4.2 - Trusted and dependable Connectivity	7/2/10	9/30/11	326d
15	WP5 - SPD MIDDLEWARE & OVERLAY	02/07/2010	30/09/2011	326d
16	5.1 - SPD driven Semantics	7/2/10	9/30/11	326d
17	5.2 - Core SPD services	7/2/10	9/30/11	326d
18	5.3 - Policy-based management	7/2/10	9/30/11	326d
19	5.4 - Overlay monitoring and reacting system by security agents	7/2/10	9/30/11	326d
20	WP6 - PLATFORM INTEGRATION, VALIDATION & DEMONSTRATION	01/12/2010	30/11/2011	261d
21	6.1 - Multi-Technology System Integration	2/1/11	10/31/11	195d
22	6.2 - Multi-Technology Validation & Verification	2/1/11	11/30/11	217d
23	6.3 - Lifecycle SPD Support	4/1/11	10/31/11	152d
24	6.4 - Multi-Technology Demonstration	12/1/10	11/30/11	261d
25	WP7 - SUPPORT ACTIVITIES	01/07/2010	30/12/2011	392d
26	7.1 - Dissemination	7/1/10	12/30/11	392d
27	7.2 - Exploitation	2/1/11	12/30/11	239d
28	M1	2/28/11	28/02/2011	0d
29	M2	3/31/11	31/03/2011	0d
30	M2bis	4/15/11	15/04/2011	0d
31	M3	6/30/11	6/30/11	0d
32	M4	8/31/11	31/08/2011	0d
33	M5	9/30/11	30/09/2011	0d
34	M6	10/31/11	31/10/2011	0d
35	M7	11/30/11	30/11/2011	0d
36	M8	12/30/11	30/12/2011	0d
37	Mid-term review	3/17/11	17/03/2011	0d
38	Supplementary review	9/30/11	30/09/2011	0d
39	Final review	12/30/11	12/30/11	0d

rview over the
Dependability
ctionality and
collaboration

Dissemination level

Restricted

Restricted

Public

Public

Public

V1.0

D2.1.2	System Requirements and Specifications (Update)	M15	ASTS	Public
D2.2.1	Preliminary SPD metrics specifications	M13	ESI	Public
D2.2.2	SPD metrics specifications	M15	THYIA	Restricted
D2.3.1	Preliminary system architecture design	M13	HAI	Restricted
D2.3.2	System architecture design	M15	THYIA	Restricted
D3.1	SPD node technologies prototype	M13	ETH	Restricted
D3.2	SPD nano micro or personal node technologies prototype report	M16	THYIA	Restricted
D3.3	SPD power node technologies prototype report	M17	ETH	Public
D3.4	SPD self-x and cryptographic technologies prototype report	M16	CS	Public
D4.1	SPD network technologies prototype	M13	SCOM	Restricted
D4.2	SPD network technologies prototype report	M16	MGEP	Public
D5.1	pSHIELD semantic models	M15	TRS	Restricted
D5.2	SPD middleware and overlay functionalities prototype	M15	THYIA	Restricted
D5.3	pSHIELD semantic models report	M16	ED	Public
D5.4	SPD middleware and overlay functionality report	M16	ED	Public
D6.1.1	Platform integration report	M17	HAI	Public
D6.2.1	Platform validation and verification	M18	ED	Public
D6.3.1	Lifecycle and SPD Support Report	M17	ATHENA	Public
D6.4.1	pSHIELD demonstrator	M18	ASTS	Public
D7.1.1	The Project Website	M09	SESM	Public
D7.1.2	Dissemination Report	M19	SESM	Public
D7.2.1	Exploitation Plan	M19	CWIN	Public
M0.1	Formalized Conceptual Models of the Key pSHIELD Concepts	M09	ED	Restricted
M0.2	Proposal for the aggregation of SPD metrics during composition	M09	ED	Restricted
M0.3	Signed Endorsement	M09	THYIA	Restricted
M0.4	Request for Extension of the Project	M09	THYIA	Restricted
M0.5	pSHIELD Focus and Outcome	M09	Movation	Restricted
M0.6	Management Report	M09	THYIA	Restricted
M1.0	Management Report at Supplementary Review	M16	THYIA	Restricted
M1.1	Annual Report	M19	SESM	Public

4 Conclusions

pSHIELD is an international research project. The scientific and technical works of the project are going to be performed by the partners from several countries. The goal of pSHIELD is addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as “built in” functionality and demonstrating the data flow from sensors to “dependable access” in a collaboration infrastructure.

This document has provided the main outcomes of pSHIELD in the six focus areas: 1. Composability, 2. New Technology, 3. Modularity, 4. Framework, 5. Metrics and 6. Validation.

Key innovations include: Metrics for security, privacy and dependability; a Semantic Model for heterogeneous environments; the prototype to demonstrate composability; Cryptography in lightweight and networked embedded devices; Concepts for heterogeneous integration through semantic technologies and finaly the function and behaviour testing of the pSHIELD middleware.

It has further defined the milestones leading to a successful implementation and prototypical demonstration of the pSHIELD architecture.