ARTEMIS JOINT UNDERTAKING

SUB-PROGRAMME SP6

### Industrial Priority Addressed (in order of importance)

#	Industrial Priority	Thematic Area
IP1	Composability	*Reference designs and architectures*
IP2	Architectural Dependability	*Reference designs and architectures*
IP3	Test, validation and verification tools	*Design methods and tools*
IP4	Resource management	*Seamless connectivity and middleware*

Grant agreement for:

"Technical Annex"

Project acronym: *pSHIELD*
Project full title: *pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions*
Grant agreement no.: *100204*
Date of preparation of Technical Annex (latest version): *28th January 2010*
Date of approval of Technical Annex by the Joint Undertaking:

List of Beneficiaries

Beneficiary Number *[1]	Beneficiary name	Beneficiary short name	Country	Date enter project	Date exit project
1	SESM - FINMECCANICA	SESM	IT	month 1	month 19
2	Acorde Seguridad	AS	ES	month 1	month 19
3	Ansaldo STS	ASTS	IT	month 1	month 19
4	ATHENA	ATHENA	GR	month 2	month 19
5	Critical Software	CS	PT	month 1	month 19
6	Center for Wireless Innovation	CWIN	NO	month 2	month 19
7	Elsag Datamat	ED	IT	month 1	month 19
8	Fundación Tecnalia Research & Innovation	Tecnalia	ES	month 1	month 19
9	Eurotech	ETH	IT	month 1	month 19
10	Hellenic Aerospace Industry	HAI	GR	month 1	month 19
~~11~~	~~Integrated Systems Development~~	~~ISD~~	~~GR~~	~~month 1~~	~~month 12~~
12 (Coord.)	Movation AS	MAS	NO	month 1	month 19
14	Mondragon Goi Eskola Politeknikoa	MGEP	ES	month 1	month 19
15	Selex Communications	SCOM	IT	month 1	month 19
20	THYIA Tehnologije	THYIA	SL	month 1	month 19
21	Tecnologie nelle Reti e nei Sistemi	TRS	IT	month 1	month 19
22	Università di Genova	UNIGE	IT	month 2	month 18
23	Università degli studi di Roma "La Sapienza"	UNIROMA1	IT	month 1	month 19

Table of Contents

PART A

Grant Agreement Preparation Forms

ARTEMIS Joint Undertaking

A1: Summary

Project number[ii]	100204	Project acronym[iii]	pSHIELD

ONE FORM PER PROJECT

GENERAL INFORMATION

Project title[iv]	pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions		
Starting date[v]	1st June 2010		
Duration in months[vi]	12		
Call (part) identifier[vii]	ARTEMIS-2009-1		
Activity code(s) most relevant to your topic[viii]	ARTEMIS ASP6		
Free keywords[ix]	Composability, Architectural Dependability, Enhanced ES Security		

Abstract[x] (max. 2000 char.)

The pSHIELD project aims at being a pioneer investigation to address Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as “built in” rather than as “add-on” functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ES.

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

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

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

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

Person in charge of the Consortium coordination

Family name	Noll	First name(s)	Josef
Participant legal name	Movation AS		
Title	Mr.	Gender (Female - F / Male - M)	M
Position in the organization	Chief Technologist		
Department/Faculty/Institute/Lab name	Chief Technologist		

Address *(if different from the legal address in form A2)*

Street name	Nedre Vollgate	Number	8
Town	Oslo		
Postal Code / Cedex	N-0158		
Country	Norway		
Phone 1	+47-9083-8066	Phone 2	----
e-mail	josef.noll@movation.no	Fax	----

Grant Agreement Preparation Forms

ARTEMIS Joint Undertaking

A1: Summary

Costs and funding

Participant n	Organization Short Name	Country	Total eligible costs (in €)	Maximum ARTEMIS JU contribution (€)	Maximum national contribution (€) (where applicable)[xi]
1	SESM	IT	705.250,00	117.776,75	195.847,55
2	AS	ES	115.800,00	19.338,60	0,00
3	ASTS	IT	590.000,00	98.530,00	154.318,25
4	ATHENA	GR	121.200,00	20.240,40	0,00
5	CS	PT	255.600,00	42.685,20	85.114,80
6	CWIN	NO	249.040,00	41.589,68	110.822,80
7	ED	IT	591.207,50	98.731,65	161.427,36
8	Tecnalia	ES	62.400,00	10.420,80	0,00
9	ETH	IT	536.000,00	89.512,00	164.589,97
10	HAI	GR	198.940,00	33.222,98	0,00
~~11~~	~~ISD~~	~~GR~~	~~248.750,00~~	~~41.541,25~~	~~0,00~~
12 (Coord.)	MAS	NO	108.161,00	18.062,89	32.015,66
14	MGEP	ES	56.296,00	9.401,43	0,00
15	SCOM	IT	576.343,75	96.249,41	164.464,61
20	THYIA	SL	505.402,30	84.402,18	294.649,54
21	TRS	IT	107.415,52	17.938,39	24.328,66
22	UNIGE	IT	124.992,00	20.873,66	39.996,36
23	UNIROMA1	IT	240.012,00	40.082,00	77.499,96
Total			**5.392.810,07**	**900.599,28**	**1.505.075,52**

PART B

Abbreviations

AAA	Authentication Authorization Accounting
AAGR	Average Annual Growth Rate
AC	Access Control
ACM	Association for Computing Machinery
ADAS	Advanced Driver Assistance Systems
ADR	European Agreement concerning the international carriage of Dangerous goods by Road
AODV	Ad Hoc On-Demand Distance Vector Routing Protocol
ASAP	Advanced Service in AirPort
API	Application Program Interface
ATx	ARTEMIS Target x
CDMA	Code Division Multiple Access
CHOP	Configuring, Healing, Organizing, Protection
COTS	Commercial Off-the-Shelf
DDoS	Distributed Denial-of-Service
DDS	Data Distribution System
DM	Device Management
ES	Embedded System
HAL	Hardware Abstraction Layer
IDE	Intrusion Detection Event
IDS	Intrusion Detection Systems/Schemes
I-ES Node	Intelligent Embedded System Node
IP	Intellectual Property / Internet Protocol
IPx	Industrial Priority x
MANET	Mobile Ad Hoc Network
NMA	Network Management Authority
OLSR	Optimized Link State Routing Protocol
OTA	Over-The-Air
P2P	Peer to Peer
QOS	Quality of Service
SOA	Service Oriented Architecture
SOC	System On Chip
SPD	Security, Privacy and Dependability
TCG	Trusted Computing Group
TPM	Trusted Platform Modules
GA	General Assembly
PB	Project Board
PM	Project Manager

SP6	Sub Programme 6
TETRA	Terrestrial Trunked Radio
TM	Technical Manager
TMC	Technical Management Committee
UCN	Ubiquitous Computing Network
UWCN	Ubiquitous Wearable Computing Network
WCN	Wearable Computing Networks
WLAN	Wireless Local Area Network
WPL	Work Package Leader
WWSN	Worldwide Wireless Sensor Network

Proposal abstract[1]

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

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

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

In the following the original SHIELD abstract is reported, quoting the most relevant parts that will be covered by the pilot.

The SHIELD project aims at addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ESs) as "built in" rather than as "add-on" functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ES.

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

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

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

To achieve these challenging goals the project aims to create an **innovative, modular, composable, expandable and high-dependable architectural framework**, concrete tools and common SPD **metrics** capable of improving the overall SPD level in any specific application domain, with minimum engineering effort. The whole ESs lifecycle will be

[1] In order to facilitate the comparison between the SHIELD pSHIELD proposals, grey boxes with notation has been inserted to explain the main differences and to add some remarks.

supported to provide the highest cross-layer and cross-domain levels of SPD and guaranteeing their maintenance and evolution in time.

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

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

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

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.

Section 1 - Relevance and contributions to the content and objectives of the Call

Since pSHIELD is the starting point for implementing the concepts of SHIELD, it maintains the same relevance of the original proposal reported below.

1.1 - Relevance

This section highlights the relevance of the SHIELD project with respect to the addressed Sub-Programme Priority (SP) 6, the relevant Industrial Priorities (IPs) and the ARTEMIS Targets (ATs). In the following the SP, IPs and ATs text (as appears in the Work Programme) is reported in grey and the corresponding SHIELD contribution is discussed.

1.1.1 - Relevance in relation to the Sub-Programme 6 Priority

SP6 - Security, Privacy and Dependability in Embedded Systems for Appliances / Networks / Services: The main goal of this sub-programme is to ensure that security, privacy and dependability (SPD) can be ensured in the context of integrated and interoperating heterogeneous services, applications, systems and devices. Systems and services must be robust in the sense that an acceptable level of service is available despite the occurrence of transient and permanent perturbations such as hardware faults, design faults, imprecise specifications, and accidental operational faults..

SHIELD strategy is conceived to increase the technological development in the supply of Embedded Systems (ESs) technologies. To this aim, SHIELD will conceive and design a reference SPD-based architecture that will be able to support product development in a diversity of application domains while reducing implementation costs.

SHIELD proposes an holistic framework aiming at ensuring the SPD level which is required by each considered application domain, regardless of the nature of the Embedded System (ES), i.e. the SHIELD solutions can be applied to any heterogeneous, possibly interconnected, managed and/or unmanaged Embedded Systems. In other words, SHIELD will design and develop a flexible SPD architecture and a related set of advanced SPD functionalities which could be engineered with minimal effort and adapted to many application domains.

In the framework of SHIELD, the developed SPD-based solutions will be proved in a set of ambitious application scenarios aiming at verifying the achieved SPD performance, measured in terms of properly defined SPD metrics.

Main goal, in SHIELD view, will be to enhance, both at societal and industrial level, people’s feeling and knowledge of complete protection from threats making them more confident in performing everyday activities (e.g. take the train to reach the office), as well as in participating in public socialization events (e.g. mass gathering sport events).

1.1.2 - Relevance in relation to the Industrial Priorities

IP1 – Composability: The ability to derive instantiations of architecture from a generic platform that support the constructive composition of large systems out of components and sub-systems without uncontrolled emergent behavior or side effects

The SHIELD architecture composability[1] relies on the so-called *SPD modules*. Indeed the SHIELD architecture is composed by a mosaic of innovative SPD functionalities, each one included in a proper SPD module, *transparently* embedded into one of the considered layers. The SHIELD architecture is able to derive application-driven instantiations of the general framework, selecting statically (at design time) and dynamically (at runtime) the best SPD functionalities for achieving the required SPD levels. In particular, referring to the above-mentioned layers, the SPD modules will implement the following functionalities:

- At node layer, intelligent hardware and firmware SPD;
- At network layer, secure, trusted, dependable and efficient data transfer based on self-configuration, self-management, self-supervision and self-recovery;
- At middleware layer, (i) secure and efficient resource management, (ii) inter-operation among heterogeneous ES networks;
- At overlay level, composability, as detailed in the following.

The SHIELD layered approach to SPD eases the process to assure the needed SPD levels, as well as to restore these SPD levels in case of SPD failures due to any possible cause (malfunctions, external attacks, etc.).

As a matter of fact, the layer (node, network or middleware) which is subject to failure can usually recover it normal operative level by itself, thanks to the mentioned SPD functionalities.

Nevertheless, in case this is not possible, the overlay can "compose" in a proper way different SPD modules belonging to all the three layers (node, network, middleware) in order to globally solve the SPD hole; so, whenever one of the rings of the overall secure service chain breaks at node, network or middleware level the overlay reacts to mitigate the consequences.

It is worth stressing the fundamental role of the overlay layer in the implementation of the "composability" concept, namely one of the most innovative issues of the SHIELD project. In this respect the proposed advanced cognitive approach will be the monitoring from the overlay layer of the SPD levels at node, network and middleware layers. Basing on this monitoring, the overlay layer will be able to detect when the present SPD level is no more satisfactory. In this case, the overlay network, being aware of the presently available SPD modules and related performance, can decide which SPD modules at the various layers have to be activated (or possibly deactivated in case they are recognized as "corrupted") and how these modules have to be configured, aiming at recovering the desired overall SPD levels. Finally, the overlay layer decisions are actuated at the various layers.

A critical issue of the proposed approach is the interfacing of the overlay layer with heterogeneous node/network/middleware layers and many SPD modules; moreover, SPD monitoring and SPD level assessment require the definition of proper SPD metrics. SHIELD will overcome these problems by the extensive use of semantic ontological descriptions which will allow to describe heterogeneous functionalities in a homogenous way. In this respect, a first fundamental step will be the definition of SPD metrics and their ontological description. Homogeneous metrics will ease the monitoring of the current SPD levels of the various layers and of the overall system, as well as the assessment of the various SPD levels.

[1] "*Composability*" is a system design principle that deals with the inter-relationships of components. A highly composable system provides recombinant components that can be selected and assembled in various combinations to satisfy specific user requirements. The essential attributes that make a component composable are that it be self-contained (modular) and stateless

IP2 - Architectural Dependability: To ensure secure, reliable and timely system services despite accidental failure of system components and/or the activity of malicious intruders.

In SHIELD view, the creation of an innovative intrinsically dependable framework will consolidate the state of the art in SPD, thus becoming the reference milestone for all the future development.

To reach this goal, *SHIELD will select the most appropriate SPD algorithms, technologies and procedures, will improve them and develop the missing ones*, and will *integrate and harmonize them in* a modular, composable, expandable and *high-dependable architectural framework.*

This goal will be achieved by designing an architecture consisting of a subset of intrinsically SPD enhanced layers: **node**, **network**, **middleware** and **overlay**. Innovative SPD functionalities belonging to each of the above mentioned layers will be designed. The architectural dependability will be achieved at each single layer (embedded node, network of embedded systems and middleware running on the embedded systems), as well as at system level (by means of the overlay layer, as detailed later).

If a system component is affected by an accidental failure or is under attack by malicious intruders, the SHIELD architecture proposes different level of dependability. If the component is SHIELD-compliant, it has been designed to be the best SPD solution to carry out the specific task, so the dependability is intrinsically built-in in such component. Conversely, if the component is a legacy one, or if the cause of its failure was due to advanced intruders' techniques or to unexpected accidents, the SHIELD architecture reacts at the layer such components belongs to. Indeed, SHIELD will develop intelligent SPD functionalities acting in the scope of the layer. For example, at node layer, automatic access control and denial of service countermeasures will be developed; at network layer intrusion detection and self-CHOP techniques will be applied.
If even the intrinsic layer dependability is overcome, the overlay layer intervenes: this layer, by continuously monitoring the SPD level of the other layers, has a global visibility of the present SPD level of the ES.. So, if the failure is not resolved within the layer in which occurred, the overlay tries to adopt proper countermeasures in order to overcome the temporary SPD hole.

This multi-layered dependability will be taken into account in each single phase of the project. From the design of the system, to the development of new technology prototypes, from the system integration to the verification phase in proper application scenario demonstrators.

IP3 - Test, validation and verification tools: Test, validation and verification tools to support compositional design that can be integrated into the complete process flow to support concurrent verification and validation at the product level as an integral part of the design process

The SHIELD project aims at addressing SPD in the context of ESs as "built in" functionalities, proposing and perceiving with this strategy the first step towards SPD certification for future ESs.

To achieve these challenging goals, SHIELD will identify, starting from a set of real ambitious application scenarios and by exploiting properly defined SPD semantic ontological descriptions, homogeneous SPD metrics, as well as methodologies for defining SPD requirements and SPD specifications in any application scenario.

In this respect, it is important stressing that SHIELD will conceive and realize a set of methodologies and tools to guide the design, the development and the implementation of a SHIELD framework instance *independently* from the specific application scenario. This means that the SHIELD architecture and related solutions will be so flexible that with a minimum engineering effort can be applied to any application scenario.

Nevertheless, in the framework of SHIELD, the proposed solutions will be validated through proper testbeds and demonstrators relevant to the four considered ambitious scenarios: **railway, health, cruise liners and flow-meters**.

In particular, the key composability concept of the various implemented SPD functionalities will be validated during the integration phase of the project on the basis of system requirements and specifications derived from the analysis of the four considered application scenarios. The composability of the overall SHIELD architecture will be verified in four different demonstrators corresponding to each of the above mentioned scenarios.

Finally, the whole system lifecycle will be supported guaranteeing the highest cross-layer and cross-domain level of SPD.

IP4 - Resource management: To ensure seamless connectivity between ES in a physical and logical environment more and more subject to changes, and to dynamically adapt to such changes. Resource management should ensure high utilization of the system resources such as CPU, memory, network, and energy, and guarantee operation within resource reserves or budgets.

SHIELD overall aim is to address ambitious, but indispensable challenges that are threatening European competitiveness in ESs such as cost-effectiveness, interoperability, reliability, re-usability. R&D efforts will be focused in designing innovative components, tools and methodologies that makes more effective use of resources.

Therefore, a great effort will be put to develop a technology-independent intrinsically secure and dependable architectural framework that allows seamless exploitation of SPD resources in heterogeneous domains: industrial systems (e.g. manufacturing plants), nomadic environments (e.g. mass gathering events), private spaces (e.g. home) and public infrastructures (e.g. railway stations). To achieve this challenging objective SHIELD will design and develop a convergent, technology-neutral middleware layer, where dynamic, composable and adaptive resource management procedures will optimize the use of the available resources (CPU, memory, network, battery, etc.) while guaranteeing the desired constraints on such resources.

In this respect, the proposed advanced cognitive approach will resemble the one adopted for the overlay layer. As a matter of fact, this approach is based on proper technology-independent middleware layer modules including advanced *resource management algorithms* which, basing on the monitoring of appropriate aggregated parameters coming from all the four considered layers, will decide the most appropriate actions to be enforced at the various layers to optimize resources, while respecting the desired constraints.

Note that ontological description of the various parameters will be a key issue for describing heterogeneous parameters coming from different layers, in an homogeneous, technology-independent way. So, this description will allow, in a natural way, the monitoring of heterogeneous parameters, their dynamic composition and the use of the resulting aggregated parameters as key inputs for the above-mentioned technology independent *resource management algorithms*. The technology independence of these algorithms favors the adoption of advanced abstract methodologies (e.g. bounded optimization, adaptive control, predictive control…) which could solve the complex resource optimization problems.

1.1.3 - Relevance in relation to the Artemis Targets

In this section is described the relevance of the SHIELD project with respect to the ARTEMIS Targets. The correspondent impact of SHIELD for each ARTEMIS target is instead detailed in Section 4.1.

AT1 - Reduce the cost of the system design.

The definition of the SHIELD conceptual framework pertains to the cost-reduction target in system design by greatly facilitating the adoption of built-in SPD solutions. Expenditures saving while designing a new system will be evident providing the availability of a validated, SPD-intrinsic framework to improve and modify rather than designing the whole system and its SPD functionalities from scratch.

AT2 – Reduce the costs of development cycles, especially in sectors requiring qualification or certification.

The definition of semantic enabled SPD metrics and the development of proper tools for the management of SPD lifecycle pertain to the ESs' development cycles improvement and will ease the qualification and certification of the generated system. SPD metrics in particular are considered the indispensable basement for building standardized methods and industry-wide accepted parameters for certificability in security, privacy and dependability field.

AT3 - Manage the complexity with effort reduction.

The static (at design time) and dynamic (at runtime) composability offered by the SHIELD framework addresses the increasing complexity of providing SPD in ESs with less effort during the whole SPD lifecycle. Flexibility and interoperability provided by the use of SHIELD-compliant solutions will allow tackling with the improving challenges in future ESs' systems due to improved complexity coming from the foreseen higher functions' integration on the single board and the more dynamic communication and linking between the board functionalities in the ES's network.

AT4 - Reduce the effort and time required for re-validation and recertification after change.

The effort of SPD re-validation and re-certification processes will be reduced by two innovations introduced in SHIELD: the definition of common SPD metrics and the development of tools to support the SPD lifecycle over the whole ES. Integrated with a validated SPD framework the further will allow to deploy standard method of quality assessment for the ES solution while the latter will controls the SPD quality conformance of the system thru its upgrades during the years it will be deployed and operational on the field.

AT5 - Achieve cross-sectorial reusability of Embedded Systems devices developed using the ARTEMIS JU results.

Static/dynamic composability and modularity are the main characteristics of the SHIELD framework. They allow reusability of the innovative ARTEMIS JU results on SPD functionalities and technologies over heterogeneous sectors: the architecture, will be validated in four different pilot scenarios, and liaisons with other application scenarios (Transport with safety relevance or Communication with seamless connectivity, for instance) will be considered during the project, but many other applications scenarios could use and benefit from the SHIELD results.

Section 2 - R&D innovation and technical excellence

Concept and objectives are almost the same, but they will be validated only in a single and reduced scenario instead of the previous foreseen four scenarios.

2.1 - Concept and objectives

The SHIELD project aims at addressing ***Security***, ***Privacy*** and ***Dependability*** (SPD) issues in the context of Embedded Systems (ESs) as “built in” rather than as “add-on” functionalities.

SPD Certification aspects covered by SHIELD will be appointed by future R&D investigations

To reach this goal the project aims at establishing an innovative approach in the SPD market, based on availability of a flexible architectural framework that will respond to different application needs. The main assumption which drives SHIELD activities is that intelligent functions embedded in components and devices will be the key factor in empowering next generation industrial processes and markets in Europe. As a consequence, the design of an innovative SPD-based framework where new functionalities and improved quality of existing solutions co-exist with the capability of delivering such architecture in a competitive cost-effective time frame, will impact on European competitiveness in a large range of domains as automotive, defense, health, industry and energy.

2.1.1 - SHIELD Concepts

The leading SHIELD concept is to demonstrate the composability of heterogeneous SPD technologies and solutions in the so called Secure Service Chains (SSC). The concept is to provide system’s functionalities, from the SPD perspectives, in a tightly integrated way at node, networks and middleware layer. Starting from SPD state of the art in ESs, the project will develop new technologies and solutions, as well as consolidating the available ones in a solid basement that will be part of the framework and become the reference milestone for a new generation of “SPD-ready” ESs.

This goal will be achieved approaching SPD at four levels: node, network, middleware and overlay and assessing the results in selected application scenarios. For each level, the project will improve the state of the art of the most promising SPD technologies and solutions (hardware and communication technologies, cryptography, middleware, smart SPD applications, etc.) and will integrate other technologies at their state of the art. Finally all of them will be enriched with composable functionalities for coordinating and harmonizing the various SPD solutions.

Figure 2.1 shows how these ambitious goals can be obtained through the SHIELD framework development. Four layers have been identified at design level: *Node, Network, Middleware* and *Overlay*. The output of each layer will be available at the upper level (white arrows in Figure 2.1) which will take advantage of SPD features developed at a lower level empowering SPD features of all SHIELD architecture in a transparent but manageable way. Moreover, such an approach will affect ESs design cost-effectiveness ensuring that future architecture will have the capability of being conceived and/or designed according to SHIELD SPD requirements in a scalable and interoperable way. In particular SHIELD compliance both at *Node*, *Network* or *Middleware* layer will represent a significant step forward to reduce the development costs of ESs-based technologies. Indeed, as detailed in Section 4.1, partners have estimated a 10% cost reduction at each layer, that leads to an overall optimal estimation of 30% for a full SHIELD oriented design methodology, by taking advantage from the intrinsic SPD features of each layer and avoiding expensive design methodologies due to lacks of security, privacy and dependability features in one or more “rings” of the Secure Service Chain (SSC). Finally SPD features and services at middleware and overlay level will be at disposal of selected application scenarios aiming at increasing overall systems performances.

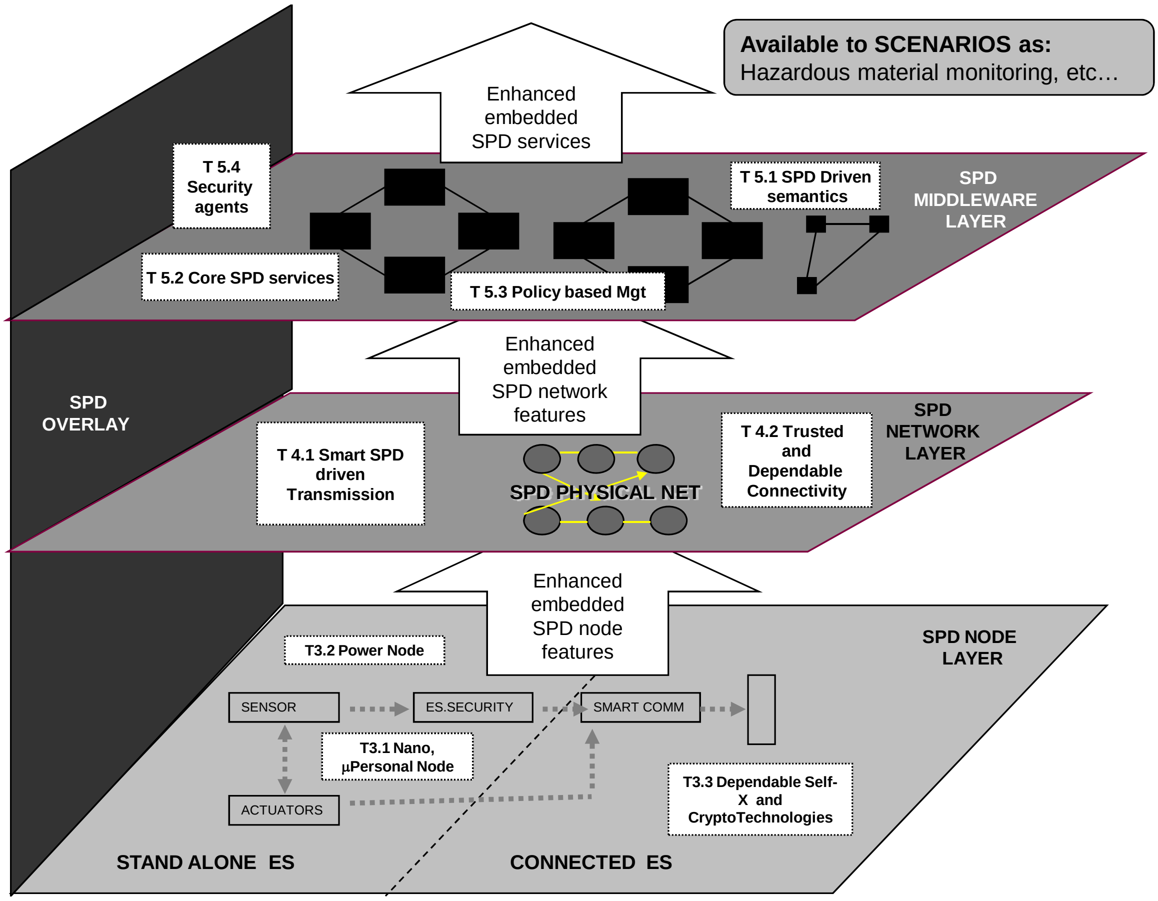

Available to SCENARIOS as:
Hazardous material monitoring, etc…
Enhanced embedded SPD services
T 5.4 Security agents
T 5.1 SPD Driven semantics
SPD MIDDLEWARE LAYER
T 5.2 Core SPD services
T 5.3 Policy based Mgt
Enhanced embedded SPD network features
SPD OVERLAY
T 4.1 Smart SPD driven Transmission
SPD PHYSICAL NET
T 4.2 Trusted and Dependable Connectivity
SPD NETWORK LAYER
Enhanced embedded SPD node features
T3.2 Power Node
SPD NODE LAYER
SENSOR
ES.SECURITY
SMART COMM
T3.1 Nano, µPersonal Node
ACTUATORS
T3.3 Dependable Self-X and CryptoTechnologies
STAND ALONE ES
CONNECTED ES

Figure 2.1 - SHIELD functional architecture overview

To reach the above mentioned objective, a set of highly challenging research and development actions will be realised. First of all the project, starting from the analysis of the application scenario, will identify SPD requirements, SPD specifications and proper SPD metrics to univocally measure SPD levels. So, for each of the selected scenarios the desired SPD levels will be univocally identified in terms of the introduced SPD metrics.

Then, the project will conceive and realize a set of methodologies, algorithms and tools (hereinafter, simply referred to as *SPD functionalities*), in order to achieve, in any considered application scenario, the desired SPD level, thus realizing a set of SSC instances. The developed SPD functionalities will be integrated in a complete platform which will be validated in the previously mentioned meaningful scenario (hazardous material monitoring). Finally, tools will be developed in order to support the whole ES lifecycle aiming at guaranteeing the maintenance of the desired SPD level during the ES evolution in time.

The expected level of SPD in the target scenarios will be achieved by implementing the specific application and its SSC components according to the SHIELD reference framework by using the developed methodologies and tools, as well as the lifecycle support.

2.1.2 - SHIELD Objectives

The project main objective is to conceive and design a preliminary, innovative, modular, composable, expandable and high-dependable architectural framework (see Figure 2.2) 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:

- Monitoring of freight trains transporting hazardous material (Railway)

The SHIELD main objective will be achieved attaining the following concepts:

2.1.2.1 SHIELD System Architecture

Figure 2.2 shows the preliminary SHIELD System Architecture (SA) highlighting in grey the parts which will be specifically conceived, designed and implemented in the SHIELD project.

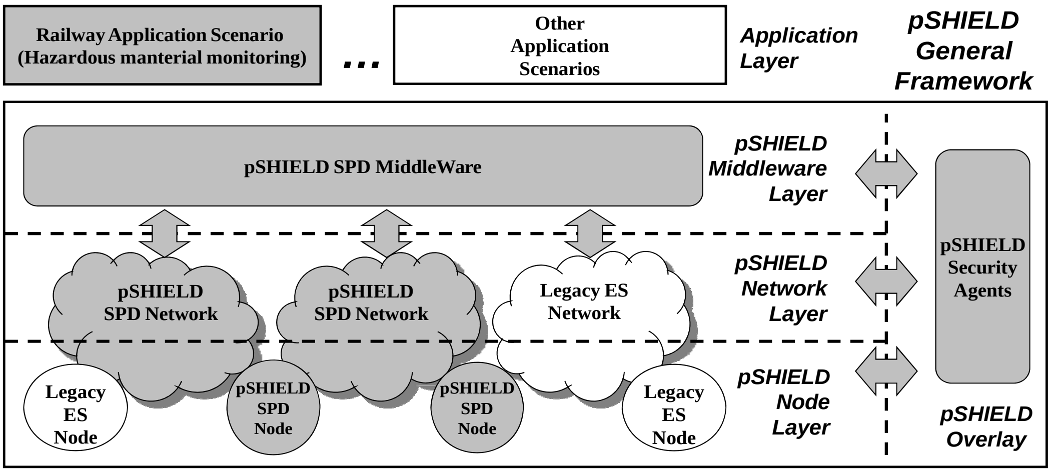


Figure 2.2 - SHIELD Architectural View

The white blocks represent the legacy solutions that will be integrated by SHIELD in a unique framework. The figure also shows some key interfaces among the various parts.

2.1.2.2 SHIELD Multi-layer approach

The organization of the overall secure service chain architecture has been done according to three basic layers, namely the *Node Layer*, the *Network Layer* and the *Middleware Layer* (see Figure 2.2). This splitting is motivated by the peculiarities of the SPD solutions to be implemented namely at node (hardware and firmware), network (protocol) and middleware (software) level and by the actual industrial contest of embedded system suppliers, which are mainly organized in these three major sectors. Innovative SPD solutions will be sought at each of the above-mentioned layers, as well as in an Overlay which will be detailed later. As detailed in Section 3 of the proposal, such layering architecture is reflected in the Work Package (WP) organization. The figure also highlights that the SHIELD architecture will be conceived even to work in conjunction with legacy networks and nodes not provided with SHIELD SPD modules.

2.1.2.3 SHIELD seamless approach

The SHIELD SPD functionalities will be conceived to be seamlessly introduced in the existing embedded systems. In particular, such functionalities will be embedded in SHIELD SPD modules which will be transparently inserted in each of the previously mentioned layers; transparency means that the insertion of these modules does not entail any modification of the pre-existing algorithms and procedures. Each SPD module will implement a specific set of SHIELD SPD functionalities which can be dynamically enabled/disabled and, in case of activation, properly configured following the decisions of the SHIELD Overlay (see the next issue).

2.1.2.4 SHIELD composability

In the scope of the pilot project, only the composability of some specific components will be demonstrated, while in a more complete project a general framework for composability could be designed and demonstrated

The SHIELD SPD modules will be designed and developed to be seamlessly composable by means of open, dependable interfaces that allow both a static and dynamic composability of SPD functionalities over different application scenarios, to guarantee the agreed level of measured SPD metrics of the overall system.

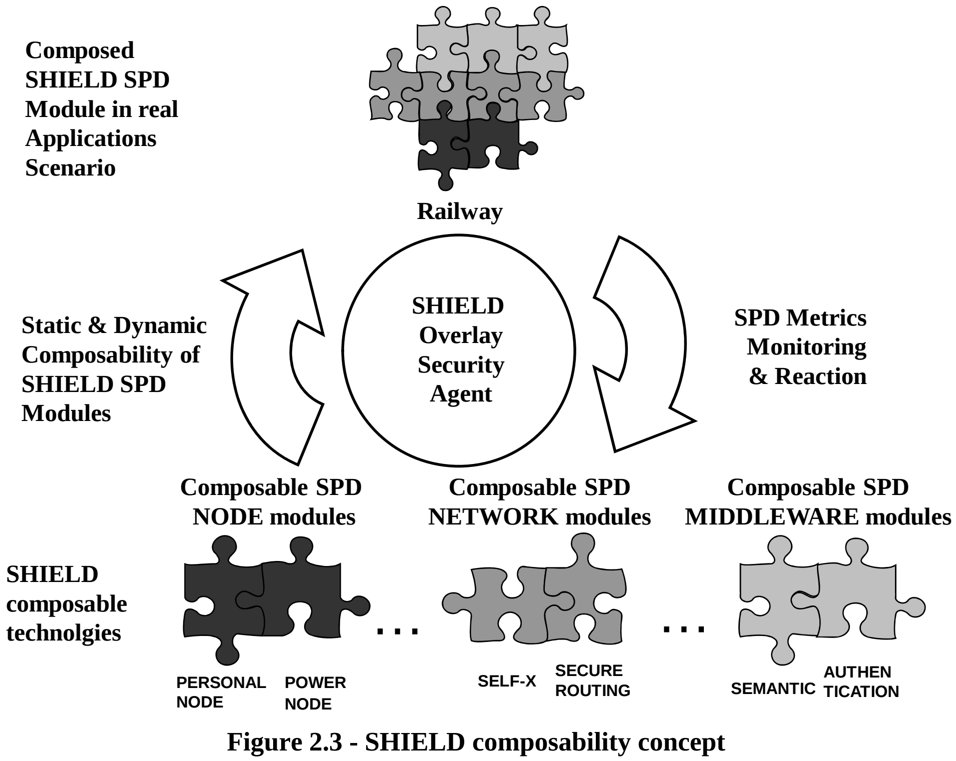

Composed SHIELD SPD Module in real Applications Scenario
Railway
Static & Dynamic Composability of SHIELD SPD Modules
SHIELD Overlay Security Agent
SPD Metrics Monitoring & Reaction
Composable SPD NODE modules
Composable SPD NETWORK modules
Composable SPD MIDDLEWARE modules
SHIELD composable technolgies
PERSONAL NODE
POWER NODE
SELF-X
SECURE ROUTING
SEMANTIC
AUTHEN TICATION

Figure 2.3 - SHIELD composability concept

As shown in Figure 2.3 the SHIELD SPD modules can be compared to pieces of a puzzle, which perfectly fits each other thanks to common interfaces. Each module implements a SPD technology or a specific SPD functionality, as an example in Figure 2.3 at node level there are two modules: personal node and power node modules. Modules belonging to different SPD layers (node, network or middleware) can be composed statically or dynamically by the SHIELD overlay. Single SHIELD SPD modules can be replaced once the measured SPD metrics do not satisfy the required SPD levels. Indeed the SPD metrics are continuously monitored by the security agents and in case of failure, the security agent reacts discovering, composing and configuring the available SPD modules.

2.1.2.5 SHIELD innovative SPD functionalities

Starting from the state of the art, SHIELD will propose new SPD functionalities based on innovative composition of existing leading technologies and new approaches. In this respect, some SPD functionalities will be thoroughly conceived, designed and developed in the project and will be completely new for the SPD context. For instance, the SHIELD Overlay will be thoroughly conceived, designed and implemented for this project. Other designed and implemented modules will remarkably enhance existing SPD solutions by means of innovative approaches, trying to foster seamless integration and legacy support. Whenever appropriate, already existing SPD functionalities will be integrated and reused. A complete list of the SHIELD SPD functionalities and technologies, highlighting the percentage of their design and development, in respect of the state of the art, which will be carried out in SHIELD (and, hence, the percentage which will be made available to SHIELD with no charge), will be presented in the next section.

2.1.2.6 SHIELD overlay

In the scope of the pilot project the overlay, one of the main innovation, could be addressed at architectural level, by a feasibility study, requirements and specifications. The full implementation of these ideas will be later developed and realized in the project follow up.

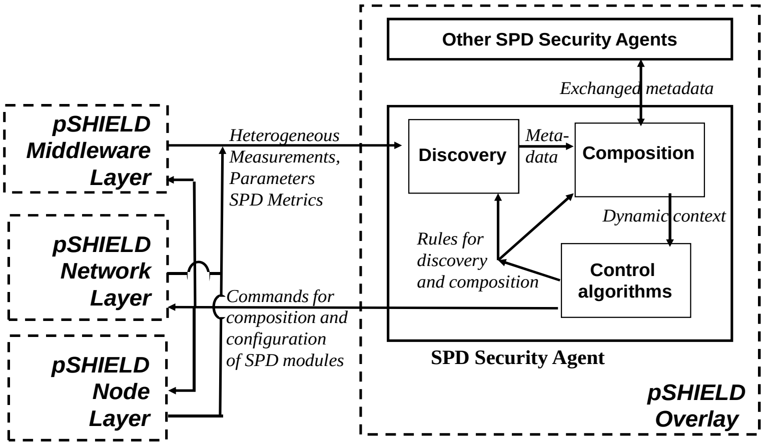


Figure 2.4 - SHIELD Overlay

The SHIELD project will design and implement overlay security agents which will implement the key *composability* concept (see Figure 2.3). The security agents will be placed in appropriate network entities to be properly selected according to appropriate criteria which take into account the considered scenario. Each security agent monitors a set of properly selected measurements and parameters taken at any of the three above-mentioned layers (see the arrows labelled as *measurements* in Figure 2.4). These heterogeneous measurements and parameters are converted by the security agents in *homogeneous metadata* by extensively using properly selected semantic technologies; the use of homogeneous metadata makes easy the metadata exchange among different security agent (see Figure 2.4). Each security agent, thanks to metadata homogeneity, can aggregate the available metadata (the ones relevant to monitored measurements and parameters, as well as the ones coming from other security agents), in order to deduce aggregated metadata which form the so-called *dynamic context.*

The latter is used as basic input for a set of *control algorithms* responsible of dynamically deciding which SPD modules have to be composed and enabled/disabled at any of the three above-mentioned layers, as well as how the activated modules have to be configured in order to achieve the desired SPD level. These decisions are enforced in the interested SPD modules lying at the three above-mentioned layers (see the arrows labelled as *commands* in Figure 2.4). The above-mentioned control algorithms are also in charge of possibly updating the rules to form the dynamic context (i.e. which measurements and parameters have to be monitored, which metadata have to be exchanged with other security agents, how the available metadata have to be aggregated, etc.).

Note that the strength of the presented composability concept lies in the possibility of *jointly* deciding at the Inter-layer manager, basing on information gained at all layers, which SPD provisions have to be performed at each layer in order to achieve the *overall* desired SPD level. This approach has the evident advantage of allowing taking SPD provisions which are coordinated among the different layers and of permitting to decide on these provisions on the basis of aggregated information coming from all layers.

2.1.2.7 SHIELD SPD metrics

In the scope of the pilot project a subset of SPD metrics will be carried out; while a complete set of metrics for security, dependability and privacy will be developed during the project follow up, in order to cover all the SHIELD concepts as described below. The selected metrics will validate the approach of a metric-compliant SPD framework.

	STATIC			**DYNAMIC**		
Problem dimensions **Classes**	**Cinematic State (e.g. movement)**	**Not Cinematic State (e.g. shape)**	**Identity (e.g. person, vehicle)**	**Behavior (e.g. fleeing crowd)**	**Assessment (e.g. panic)**	**Prediction (e.g. threat)**
Objects	Estimate Precision	Estimate Precision	Classification (POD / FAR)	Precision +Classification		
Situations		Estimate Precision	Classification (POD / FAR)		Precision +Classification +Assessment	
Threats			Classification (POD / FAR)			Precision +Classification +Assessment +Prediction

Table 2.1 – SPD Metrics examples

SPD metrics will be a SHIELD key issue. First of all, the SHIELD project will identify static and dynamic SPD metrics driven by the requirements coming from the selected industrial scenarios, at each of the considered layers, as well as for the overall system. Then, the SHIELD project will identify the embedded system desired SPD level at the above-mentioned layers and for the overall system with respect to these metrics. The table below describes a possible approach for the selection of SHIELD metrics. Key parameters of each considered problem have been identified as dimension, class and static and/or dynamic nature. Moreover, an example of several metrics is presented with respect to the proposed problem dimensions. For instance, considering SHIELD railway application scenario such metrics will be applied to evaluate the required SPD levels in case of an act of terrorism as a malicious attack against the network of cameras which guarantees the surveillance of railway stations or the detection of a potentially dangerous unattended luggage (e.g. a bomb). Thus, in the proposed example, SHIELD framework situational-aware and context-aware capabilities will be analyzed with respect to precision, classification and assessment required metrics in order to provide a quantitative and qualitative evaluation of obtained SPD performances. Finally, it is relevant to point out that presented metrics can be applied to a large range of application scenarios aiming at validating and defining performance of SHIELD framework in terms of required SPD levels independently from a specific domain

2.1.2.8 SHIELD effectiveness

Finally, the SHIELD project will test the effectiveness of the proposed SPD functionalities: comparing, by means of the above-mentioned metrics, the required SPD levels (at each single module, as well as for the overall system) with the levels achieved by the SHIELD SPD solutions; integrating them in a complete platform; testing such platform in the previously mentioned meaningful demonstrator (railway), carefully selected in an industry exploitation perspective in order to cover a view of the foreseen industrial needs.

2.1.2.9 SHIELD improved technologies

On the light of the above concepts, from the SHIELD perspective, Security Privacy and Dependability are related to each layer and controlled by means of an overlay using proper metrics. The SPD levels needed by specific applications are achieved composing SPD technologies. Even though interoperability and composability of state of the art SPD technologies will be itself a result of paramount value, the holistic vision perceived by SHIELD leads furthermore to include in the framework the development of innovative SPD technologies as requested by the market

In the following table an outline is given on how Security, Privacy and Dependability are realized improving specific SPD features and technologies that will be detailed in Section 2.2.

Layer	Features & Technologies		
	Security	Privacy	Dependability
Node This layer provides SPD intrinsic capabilities at node level through the creation of an intelligent hardware and software platform consisting of different kinds of intelligent ES Nodes.	- TPM and Smartcard - Asymmetric cryptography for low cost nodes - Intrinsically secure ES firmware	- Automatic Access Control - Asymmetric cryptography for low cost nodes	- Power Supply Protection - Self-re-configurability and self-recovery of sensing and processing tasks
Network This layer designs and implements a secure, trusted, dependable and efficient data transfer for network centric sensible applications.	- Reputation-based schemes for secure routing and intrusion detection - Reputation based Secure Resource Management Procedures at transmission level	- Anonymity and Location-privacy techniques - Dependable authentic key distribution mechanisms	- Waveform-agile and reliable transmission methodologies - Distributed self-management and self-coordination schemes for unmanaged and hybrid networks

Middleware This layer designs and implements secure resource management techniques, secure service management functionalities, lifecycle support and highly-dependable interfaces.	- Secure Resource Management Procedures at middleware level - Secure service discovery, composition and delivery protocols	- Secure Offline Authentication with mobile devices	
Overlay This layer includes the so-called security manager; each manager controls a given ES.	- Semantic representation of the security knowledge domain	- Semantic representation of the privacy knowledge domain	- Semantic representation of the dependability knowledge domain

Table 2.2 - SHIELD SPD Features & Technologies to be improved

2.2 - Progress beyond the state-of-the-art

Even though one of the main reductions in the pSHIELD project affects the number of technologies involved in R&D activities, the selected technologies will constitute a valuable improvement beyond the state of art in SPD field.

2.2.1 - Beyond the state-of-the-art of Embedded Systems security

Modern ICT are experiencing a growing need for secure solutions: systems are more and more vulnerable because of the increased complexity and interconnection of components and networks with varying and often undefined security levels. Embedded security is the next product differentiator for embedded devices! The standard design and requirements are not enough anymore, since there is a huge expansion of innovative technologies, which are emerging as new ones in many business sectors, such as Telecom, Health, Automotive, etc, where "security" is required. This multi-technology landscape is demanding security mechanisms in physical concepts, intrinsic micro-technology designs, SW&HW architectures, protocols and applications especially in the fields of use where security is requested.

The SHIELD project aims at filling these gaps by means of an innovative holistic multilayer integrated approach to SPD, not only a middleware layer as in currently available solutions.

In current state-of-the-art systems, adding security to the software architecture has often the negative impact of collapsing the levels of abstraction in the architecture and elevating low-level design decisions to a higher and often incorrect level. The security architecture work is primarily integration work, where existing legacy systems have commercial security solutions grafted on to existing insecure architectures. Estimating the components current security and its influence on other system components is often neglected, thus the overall security level of architecture remains undefined. The main reason for this is often lack of reliable and useful metrics for assessing the security level.

In contrast to current practice, SHIELD will take security into account from the early stages of system design as an integral part of the system architecture, including the architecture analysis from a security point of view and measuring the current state, to be able to propose architectural improvements for the system. In particular, SHIELD proposes a new method in the way to approach "security", based on the idea that it is not possible to wrap security around an application that has not been designed with security in mind; however, it is possible to offer a set of basic modular features that help the application designer to accomplish specific security-related tasks in a standard way and without requiring the designer to reinvent them. Such approach is based on the provision of a set of basic modules (not provided in a "one-size-fits-all" fashion, but reconfigurable from the designer) which the designer can use to secure the application in question, like cryptographic algorithms and key distribution facilities.

The *SHIELD Security Platform* lets designers choose for each service/application *which* security modules are needed and *where* (i.e. in which network entity) such modules have to be placed, in order to optimally balance the cost-performance trade-offs in the specific environment. As an example, consider the case of choosing a secure transport protocol optimized for resource consumption; this protocol is used to protect truly important messages while not wasting resources in those that are not sensitive. Then, the splitting of security functions into separate, small-and-flexible modules allows the designer to decide in a flexible way upon their placement. Thus, depending on characteristics of the environment, like the network topology and the criticality of each service requiring security functions, the appropriate modules can be optimally placed in the appropriate network entities.

SHIELD will progress beyond the state-of-the-art in the identification of SPD metrics at each architectural layer, as well as for the overall system (i.e. at inter-layer level). As a matter of fact, at present, only a few SPD features can be actually measured in an effective way.

A further fundamental key by which SHIELD progress beyond the state-of-the-art, is the design and the implementation of the Overlay Security Agents (that is a completely new concept) able to measure, according to the above-mentioned SPD metrics, the actual achieved SPD level at each layer, as well as for the overall system. These measurements, which will be performed according to a technology-independent, service-independent, semantic based approach, will permit to test the effectiveness of the various proposed SPD solutions, thus allowing the identification of possible SPD weak points in the secure service chain which need further work. Even more, the Security Agents will also perform an active role since, basing on the SPD measurement elaboration, they will decide the actions (e.g. re-tuning of a given parameter, reconfiguration of a given network element, ...) necessary to recover possible identified SPD deficiencies.

In the following section, additional SHIELD progresses beyond the state-of-the-art which are more specific of the various layers are outlined.

2.2.2 - Progress in specific SPD technologies as expected output of the project

As introduced in the previous section and as it will be widely described in Section 3, the expected output of the project is a holistic Platform to address Security, Dependability and Privacy at different layer and for different purposes, ready to be tailored on (but not limited to) the selected application scenarios.

Some technologies has already been identified to be the *basic SHIELD modules*: they will be assessed, improved to provided added value respectively in Security, Dependability or Privacy and adequately refined to be “SHIELD” compliant, i.e. able to realize SHIELD innovative functionalities (composability, overlay, measurement,…).

While the *“SHIELD” compliant* capability constitutes itself an improvement beyond the state-of-the-art and has already been discussed, the other specific improvements for each technology should be defined in the following paragraphs.

TPM and Smartcard for Trust ESs

The Trusted Platform Module (TPM) is a secure crypto-processor that can generate and store cryptographic keys, generate pseudo-random numbers and that includes capabilities such as remote attestation and sealed storage.

The technology around the TPM has been developed for few years now through the Trusted Computing Group (TCG)'s initiative. Initially driven by its application for the PC platforms, the component could provide interesting functionalities to a large panel of devices and in particular to embedded systems. Unfortunately, those applications are not really developed for the moment (with the notable exception of the mobile phones) despite the important opportunities that this approach could open. Working for more general platforms than the PC and mobile phones generates new requirements not really covered by the current specifications. Some flexibility has been included in the specification of the next generation of TPM (TPM.next supports for instance more general model of asymmetric key storage) but first, the specification is not expected in the next 2 years and second, it does not cover all the aspects of those new platforms.

→The contribution of SHIELD would cover a big part of those new requirements. In particular SHIELD will:

- improve the global architecture of the embedded SW of the TPM to support future evolutions of cryptographic/hash functionalities,
- add alternative communication interfaces better adapted to the embedded applications than the LPC currently supported,
- add some specialized/dedicated commands (e.g. to further develop on-the-fly encryption)
- implement additional cryptographic protocols (e.g. elliptic curves)
- Implement additional mechanisms to improve product endurance and increase product lifespan

To be in line with TCG guidelines, SHIELD will also address the following issues:

- Protection against attacks on the integrity of the TPM, particularly against physical attacks
- Inexpensive implementation in order to allow widespread use.
- Compliance with global export control regulations in order not to restrict international trade with TC platforms (PCs).

Last, but not least, it is also in SHIELD objectives to propose those innovations in the framework of the TCG activities to ensure the proper standardization of the approach.

Intrinsically Secure ES Firmware

For many ES market like military and avionics the dependability is one of the most important aspects. Generally the common way to achieve a high dependability is to apply the concept of HW redundancy. The trade off of HW redundancy is that system's cost rising up drastically.

A different approach can be applied to the some ES like FPGA that are intrinsically redundant. In details the concept of Runtime reconfiguration is applicable to FPGAs. Runtime reconfiguration is the capability to modify or change the functionality configuration of the device during normal operation or fault, though either hardware or software changes. That capability can be specialized in different way in order to reduce component count, power consumption, reusing, fault tolerance, etc.

→The goal of this Project is to develop a new approach for FPGA runtime reconfiguration that is capable to increase the nodes dependability.

Automatic Access Control and Denial-of-Service

ES nodes could be reached by the network: automatic access control and denial of services mechanisms are in charge of preventing non authorized/malicious people to access the physical resources of the node.

There are several ways to implement an Access control in a network, depending on the "intelligence" of the nodes, the memory capabilities and the predefined profiles. Those methods are based on:

1) Profile authentication: If the node has some characteristics, it can join to the network.
2) Access Code (programmable or configurable): Typical password access, based on memory data, switch configuration, or any other procedure
3) Predefined topology: Only pre-established nodes can join to the network, like MAC filtering in a WiFi

Denial of Service[1] on an embedded node or a network of nodes is the act of consuming the nodes' resources like power, processing power, network bandwidth and memory either by exploiting certain vulnerabilities on the nodes' software/firmware, or by flooding the nodes' network bandwidth with unwanted incoming flow. The past years revealed the fact that poor design decisions in network protocols and operating systems can become a serious obstacle in DoS and Distributed DoS resilient systems and services. The IP protocol is vulnerable to such attacks and basic software design methodologies don't take into account security requirements that would enable DDoS resilient services[2].

→As part of the activities in SHIELD, it is planned to address the critical design steps that will enable node firmware/software as well as network protocols in an SPD node environment which are resilient to DDoS attacks in conjunction with the implementation of basic access control mechanisms that a node should provide to the applications.
Another step is to realize and handle DDoS vulnerabilities in a shared node environment where the possible attacker is an insider who already has the necessary credentials and wants to degrade service availability of part of the node network for his own purposes (per example shared face recognition devices installed on airport gates).

Power Supply Protection

Power Supply Protection must take into account three key points for its implementation:

- Be able to provide a continuous power supply source, without any cut in time neither in the power, voltage or current levels, to correctly bias the devices
- Monitor and prevent any system power supply risk, which might affect to the system behavior
- In case of failure of any of the countermeasures, being able to protect all the electronics and devices, in order to avoid further damages into the system

This is something which is critical in a standard system, but even more in a security application, where the system availability has to be one of the key points.
There are works based on the use of the UPS[3] (Uninterruptible power supply), and some control electronics, but this is feasible in big systems, but it is a real challenge in small nodes, where back-up batteries are to luxury, and new technologies based in supercapacitors, or energy scavenging combined with micro-power generators are more suitable.

→There are a set of several alternatives that could be taken into account, but the research to be performed under the SHIELD project must combine both countermeasures in case of failure, together with protection circuits of the power supply units. Under the first topic, concepts such as microgenerators, supercapacitors, remote powering and secondary power sources will be investigated, while under the second topic, the research must focus on the selection of different operative modes, being able to plug or unplug critical and non-critical sections of the nodes, or disconnect any damage sub-system which fails or works in a suspicious mode (minimizing the risk of leakages). This part of the work will be of close interaction with the node architecture tasks, because it will be required to know who the

[1] R. R. Kompella, S. Singh, and G. Varghese, "On Scalable Attack Detection in the Network," *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, 2007.
G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-Service Attack Detection Techniques," *IEEE Internet Computing,* vol. 10, no. 1, 2006.

[2] K. Stefanidis and D. N. Serpanos, "Implementing Filtering and Traceback Mechanism for Packet-Marking IP-Based Traceback Schemes against DDoS Attacks," in *IEEE International Conference on Intelligent Systems*, Varna, Bulgaria, 2008.

[3] Uninterruptible Power Supply to Ensure Continuous Electrical Flow – 212 Electronics Articles

system works, and characterize the degree of importance of any of the sub-systems on the architecture.

There are a set of available technologies being able to provide alternative power supply sources to the systems, but they must fit the specifications, environmental conditions and operative modes of the nodes. Therefore a vibration generator can feed a mobile unit, but is not suitable for a static device, while micro-solar cells can bias an outdoor mobile or fixed unit, but can be too risky for indoor scenarios.

Another alternative that will be investigated will be the possibility to perform remote powering in case of failure of the main power supply unit of the device, being able at least to allow some operational features to the device.

Self-re-configurability and self-recovery of sensing and processing tasks

Self-reconfigurability can be used to increase the function density of a processing node, to make a node more secure against side-channel attacks through measurement of EM radiation, and to implement self-healing properties. Although some of these techniques have already been published in the literature, to this date they have not been used in marketed products.

Self-recovery can be implemented through reallocation of functional blocks that will replace and mark faulty resources, through device re-programming in the case of programmable devices (self-reconfigurability), or through degradation of service.

→SHIELD plans to implement embedded system architecture based on field-programmable gate arrays (FPGAs) with the support of partial runtime reconfiguration to research practical usability of self-reconfigurability and self-recovery. The starting point will be an existing FPGA-based UTIA platform[1] for floating-point digital signal processing. The platform is built of a number of a so-called basic computing elements (BCE) grouped around a 32-bit microprocessor (MicroBlaze) that controls the system. The BCE combines a programmable reconfigurable datapath and a simple reprogrammable microcontroller. A computation is decomposed into three layers: the lowest level implements autonomously elementary vector operations in hardware. This level is represented by the reprogrammable reconfigurable datapath unit. The middle level is represented by the BCE that combines the datapath unit with a simple microcontroller. This level sequences autonomously batches of the elementary vector operations to implement elementary DSP operations such as matrix multiplication, FIR, LMS or QR. The highest level is represented by the 32-bit microprocessor that executes user programs and performs some calculations in the BCE.

The architecture of the UTIA platform uses similar features like the object-oriented approach adopted in software development: uniformity of interfaces, encapsulation, polymorphism and composition leads to high productivity and design robustness.

Due to these features the UTIA platform is suitable for testing both self-reconfigurability and self-recovery for both CPU-based devices and for FPGA-based devices.

Embedded Camera Array auto-calibration and auto configuration techniques

[1] Daněk Martin, Kadlec Jiří, Bartosinski Roman, Kohout Lukáš: Increasing the Level of Abstraction in FPGA-based Designes , *International Conference on Field Programmable Logic and Applications* , Eds: Kebschull Udo, International Conference on Field Programmable Logic and Applications, (Heidelberg, DE, 08.09.2008-10.09.2008)
Kadlec Jiří, Bartosinski Roman, Daněk Martin: *Accelerating MicroBlaze Floating Point Operations, Proceedings* 2007 International Conference on Field Programmable Logic and Applications (FPL) , Eds: Bertels Koen, Najjar Walid, Genderen Arjan, Vassiliadis Stamatis, International Conference on Field Programmable Logic and Applications. FPL 2007, (Amsterdam, NL, 27.08.2007-29.08.2007)

It consists of a series of embedded camera with the following functionalities: 3D model identification of the scene and High precision tracking algorithms and motion detection techniques, usually for surveillance purposes.

Surveillance is monitoring of the behavior, activities, or other changing information, usually of people and often in a surreptitious manner. Surveillance may be applied to observation from a distance by means of electronic equipment such as embedded CCTV cameras.

Today's video surveillance market is one of the fastest growing markets in the field of security applications. Camera systems are found more and more often both in public spaces, especially in large cities, and at private premises. The state-of-the-art systems implement embedded intelligence directly in the camera (e.g. license plate recognition). Many systems, however, (especially those at private premises) just record video data for an off-line processing. Complex video systems use a central monitoring point with personal "passive" inspection, with no means for on-line processing and/or analysis of the video sequences. While the current surveillance systems are able to detect car registration plates or the ADR sign plates (at a known area in an image), they are not able to detect potentially dangerous situations such as an abandoned luggage and to raise an on-line alarm. Also, they do not really comply with the privacy and dependability standards.

As digital cameras become cheaper and more easily managed (and high resolution devices become available), more and more surveillance systems contain large camera arrays. Specific technologies consist of auto-calibration and configuration of camera arrays, 3D model identification of the scene, foreground and background discrimination. High precision foreground object tracking based on motion detection from multiple cameras have to be developed for the purposes of such systems.

Camera auto-calibration[1] is a process where multiple un-calibrated images are used to directly determine internal camera parameters. In contrast to classic camera calibration[2], auto-calibration does not require any special calibration objects in the scene. The camera calibration is a technique related to model based 3D scene identification. Different camera auto-calibration algorithms cover different situations (number of images, constant or varying internal camera parameters, knowledge of some camera parameters, knowledge about the scene). Camera auto-calibration is an active research because many of the available algorithms are very noise-sensitive, or produce multiple solutions, and also because there are many particular cases that deserve special attention.

Essential part of a video surveillance system is an ability to track moving foreground objects against a relatively static background. Conceptually it consists of a three-stage video processing pipeline:

1. A foreground/background discriminator which labels each pixel as either foreground or background.
2. A blob detector which groups adjacent "foreground" pixels into blobs.
3. A blob tracker which assigns ID numbers and other properties to blobs and tracks their motion frame-to-frame.

Almost all the sophistication in this facility is devoted to the first stage, which uses state-of-the-art algorithms[3]. The second stage uses relatively unsophisticated, commonly known

[1] Richard Hartley and Andrew Zisserman: Multiple View Geometry in computer vision, Cambridge University Press, 2003, ISBN 0-521-54051-8

Zhaoxiang Zhang; Min Li; Kaigi Huang; Tieniu Tan: Practical camera auto-calibration based on object appearance and motion for traffic scene visual surveillance, Computer Vision and Pattern Recognition, 2008. CVPR 2008.

[2] Z. Zhang: A flexible new technique for camera calibration, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.22, No.11, pages 1330–1334, 2000

Liyuan Li, Weimin Huang, Irene Y.H. Gu, and Qi Tian: Foreground Object Detection from Videos Containing Complex Background, ACM MM2003

P. KadewTraKuPong and R. Bowden, An improved adaptive background mixture model for real-time tracking with shadow detection, in Proc. 2nd European Workshop on Advanced Video-Based Surveillance Systems, 2001 algorithms. Sophisticated methods are required for the third stage especially if a moving object is tracked using multiple cameras.

The intelligent video surveillance systems have a huge potential to prevent dangerous situations by signaling a problem before it has mounted and become dangerous. They can recognize an unusual behavior or situation and inform a guard. The result is an increased efficiency and economy of the system, since the guard can focus on an active solution of problematic situations rather than tedious passive watching of a monitor screen. Also, since the need to record huge amount of dumb video data is eliminated and only the problematic situations are saved for future detailed analysis, privacy concerns will be better satisfied.

→In this field, SHIELD will develop further advanced calibration techniques based on lines and planes aiming cross-camera color calibration and both panoramic and stereo geometry calibration for constructing ultra-high resolution mosaics and multi-viewpoint 3D captures[1]. These methods will be developed to exploit the continuity of these images for tracking, geometric recovery, and compression.

Moreover the contribution of SHIELD is to study and implement efficient camera auto-calibration, thresholding and blob detection and tracking techniques. Since the computationally most expensive part of video surveillance system is a background and foreground discrimination[2], we plan to implement state-of-the-art algorithm using the FPGA-based UTIA computational platform which is very well suited for such a task.

Personal wearable node for security, privacy and dependability

Regardless of the different perspectives for the future Internet the computing world will be pervasive, ubiquitous and wearable. Computers are becoming available anytime and anywhere in many different forms. They are distributed ubiquitously, pervasively and unobtrusively throughout the every-day environments in forms of small or large, visible or invisible, attached or embedded or blended, simple or complex, and so on. Wired or wireless networks connect these computers locally or globally, coordinated or ad hoc, continuously or intermittently[3]. Pervasive computing adds to mobile computing smart space, invisibility, localized scalability and uneven conditioning[4].

Ashok and Agrawal are giving inside on wearable computing platforms/nodes and technologies[5]. Wearable computing nodes must be small and light enough to fit inside clothing, attach to a belt or other accessory, or be worn directly like a watch or glasses. At the same time, it must be able to accommodate various electronic devices—sensors, cameras, microphones, wireless transceivers, and so on—along with a microprocessor, a battery, memory, and a convenient and intuitive user interface. It must also be able to convey

[1] "Calibrating camera and projector arrays for immersive 3D display", H. Baker, Z. Li and C. Papadas,, Stereoscopic Displays and Applications XX, Electronic Imaging, Woods, Holliman, Merritt, Editors, 2009.
"Exploiting Homologies in Global Calibration of a Multi-imager Array", H. Baker, Z. Li and C. Papadas, The True Vision Capture, Transmission and Display of 3D Video (3DTV-Con), Kos, Greece, 2007.
"Multi-Viewpoint Uncompressed Capture and Mosaicking with a High-Bandwidth PC Camera Array", H. Baker, D.Tanguay and C.Papadas, Omnivis-5, Beijing, 2005.
"Consistent image-based measurement and classification of skin color", M.Harville, H. Baker, N.Bhatti, S.Susstrunk, Proc IEEE Intl Conf Image Processing (ICIP), Italy 2005.
"Motion Tracking on the Spatiotemporal Surface", H. Baker, R. Bolles, Motion Vision Workshop, IEEE Press, Princeton, NJ (91).

[2] Chen, T., Haussecker, H., Bovyrin, A., Belenov, R., Rodyushkin, K., Kuranov, A., Eruhimov, V.: Computer Vision Workload Analysis: Case Study of Video Surveillance Systems. Intel Technology Journal. (May 2005).

[3] Jianhua Ma et al., "Ubisafe Computing: Vision and Challenges (I)," ATC 2006, LNCS 4158, pp. 386 – 397, Springer-Verlag Berlin Heidelberg 2006.

[4] http://www.cc.gatech.edu/ccg/paper_of_week/satya-challenges-of-pervasive2001.pdf.

[5] Roy L. Ashok and D. P. Agrawal, "Next-Generation Wearable Networks," IEEE Computer, November 2003, pp.31-39

information even when not in use, such as a new e-mail alert. Unlike intelligent wristwatches, wearable radios, and other similar devices, wear-ware can be reconfigured as required, which greatly widens the scope of applications. Ubiquitous computing systems are used for critical applications, such as healthcare monitoring or controlling vehicles on motorways, etc[1]. Therefore, security dependability and privacy become more important for Ubiquitous Computing Networks (UCNs). These devices are very dependent on wireless communication which is intrinsically broadcast and hence easily monitored. Messages routed via unknown intermediate nodes may be susceptible to confidentiality or modification attacks. Nodes can be bombarded with messages in order to deplete battery power. Security is thus a critical concern in such a potentially hostile environment, particularly for applications involving financial transactions or healthcare monitoring. Wearable Computing Networks (WCNs) are personal, which means travel around different geographical region and countries. Therefore, the concept sharing worldwide wireless sensor network (WWSN) is extremely important for UCNs and/or WCNs. Lew Shu et al made a good review for WWSN[2]. The main goal of P2P overlay is to treat the underlying heterogeneous USNs (Ubiquitous Sensor Networks) as a single unified network, in which users can send queries without considering the details of the network. In a global vision of WWSN will provide public services, which means will not include private sensitive information. However, like other networks today based on IP protocol security mechanisms can be applied for different purpose and applications.

→ Nowadays, wearable and ubiquitous computing are emerging for embedding different kinds of sensory devices on the user's body or on various items in the environment, we are able to develop various kinds of models for the activity of the persons or items. This development work requires means to collect, store and label the data wirelessly and in a non-obtrusive way[3]. SHIELD framework on UCN & WCN or (UWC) networks (UWCNs) is addressing many key issues regarding the network itself, the node and SPD issues. UWC which may contain various communication protocol modules such as WLAN, Bluetooth, ZigBee, Wibro, and CDMA can be a solution in this era to support the ubiquitous wireless network environment. In ubiquitous wireless environments, UWCs with multiple communication modules can control each communication module as a coordinator and communicate with other devices containing Beyond WLAN and Zig-Bee modules in the surrounding networks. We will also investigate generating cryptographic keys using the context available. The underlying technology is based on the Smart-Its context sensing, computation and communications platform.

Rugged High Performance Computing Node

The Rugged High Performance Computing (HPC) Node represents a ruggedized platform that provides SPD features in an embedded HPC on the field, wherever is required, without the limitations of a classical HPC solution in terms of working conditions, energy consumption, dimensions, etc. The use of an embedded HPC presents many advantages: high elaboration capabilities, system SPD, robustness and redundancy on the field, near-sensor processing, reduced network load, simplicity of deployment and reduced installation costs. Currently available solutions for on-site data processing are limited, in terms of scalability, computing power, SPD, storage and flexibility of use and often rely on PPC or DSP architectures, taking little advantage of code reuse from different market sectors. Available solutions that can be

[1] Dan Chalmers et al., Ubiquitous Computing: Experience, Design and Services," http://www-dse.doc.ic.ac.uk/Projects/UbiNet/GC/Manifesto/manifesto.pdf

[2] Lei Shu et al., "Sharing Worldwide Sensor Network," http://lei.shu.deri.googlepages.com/swdmnss2008CameraReady.pdf

[3] S. Pirttikangas et al., "Experiences on Data Collection Tools for Wearable and Ubiquitous Computing," International Symposium on Applications and Internet, IEEE Computer Society, 2008, pp.149-152.

compared with an HPC rugged node can be classified in three main categories: single board computers for military applications, dual Nehalem systems and high performance ES. Furthermore, classical HPC solutions cannot be simply scaled down to fit ES requirements because of architectural and technological reasons, system requirements in terms of environmental condition, costs, etc... Products of the present generation are often derived from custom equipment and solutions, leveraging on past experience, and seldom allowing a cross disciplinary approach to embedded computing. It is an inherently prudent and safe choice, however it almost never allows a seamless reuse of computing platforms, and even more rarely code can be reused without porting and adaptation of several layers of the SW stack. For many ES market like military and avionics SPD capabilities in HPC Nodes is one of the most important aspects. Generally the common way to achieve a high SPD capabilities, in particular dependability, is to apply the concept of HW redundancy. The trade off of HW redundancy is that system's cost rising up drastically.

→A different approach can be applied to HPC ES using FPGA that are intrinsically redundant. The concept of runtime reconfiguration is applicable to FPGAs and represents the capability to modify or change the functionality configuration of the device during normal operation or fault, though either hardware or software changes. That capability can be specialized in different way in order to reduce component count, power consumption, reusing, fault tolerance, etc. increasing the global SPD capabilities of the system.

Asymmetric cryptography for low cost nodes

Algorithms and protocols for asymmetric cryptography, usually used with powerful hardware, must be adapted to limited devices, both in terms of computing capability and energy constraints.

→The technology to be improved during the SHIELD project shall provide an optimized hardware implementation for an elliptic curve cryptography[1] based on public-key authentication algorithm.

So far all implementations available on the market rely on symmetric crypto primitives and thus must operate as master-key systems, sharing a master secret over all nodes enabled for verification of the authenticity of other nodes in the system. If one component (e.g. a stolen reader) gets compromised and the master key revealed, the whole system is broken. With the use of asymmetric cryptography, the background system or the reader device may verify the authenticity of the node without knowledge of the node's secret – thus compromising such a reader does not do any harm to the overall embedded system. Furthermore since every low

[1] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-key cryptography for RFID-tags. Printed handout of Workshop on RFID Security — RFIDSec 06, July 2006.
Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-key cryptography for RFID-tags. In Fourth IEEE International Workshop on Pervasive Computing and Communication Security — PerSec 2007, pages 217–222. IEEE, 2007.
Michael Braun, Erwin Hess, and Bernd Meyer. Using elliptic curves on RFID tags. International Journal of Computer Science and Network Security, 2:1–9, 2008.
Markus Dichtl and Jovan Goli´c. High-speed true random number generation with logic gates only. In P. Paillier and I. Verbauwhede, editors, Cryptographic Hardware and Embedded Systems — CHES 2007, volume 4727 of Lecture Notes in Computer Science, pages 45–62. Springer-Verlag, 2007.
Franz F¨urbass and Johannes Wolkerstorfer. ECC processor with small footprint for RFID applications. In IEEE International Symposium on Circuits and Systems — ISCAS07, 2007.
Jovan Goli´c. New methods for digital generation and postprocessing of random data. IEEE Trans. Computers, 55(10):1217–1229, October 2006.
Daniel Hein. Elliptic-curve cryptography suitable for RFID systems. Master's thesis, IAIK, Technical University of Graz, 2008. http://www.iaik.tugraz.at/teaching/11_diplomarbeiten/archive/hein.htm.

cost node would have its own secret, revealing one key does not immediately compromise the whole system, but only the very one entity.

→In the run of the SHIELD project a secure authentication protocol based on ECC will be implemented in a low cost hardware-node as well as in an ES software solution and integrated to prototypes in various scenarios. Thus strong asymmetric cryptography shall find its way to low cost nodes in embedded systems, which has for a long time been doubted to be feasible at all.
In addition the implementation will be secured against side-channel attacks (SCA) such as simple power analysis (SPA) differential power analysis (DPA) as well as their electro-magnetic counterparts SEMA and DEMA and fault attacks (DFA). Thus the low cost node shall reach a security level which makes it prepared for future ES certifications.

Reputation-based schemes for secure routing and intrusion detection system

Reputation-based systems are a new paradigm and are being used for enhancing security in different areas. These systems are lightweight, easy to use and are capable of facing a wide variety of attacks. Among these mechanisms, CORE[1], CONFIDANT[2] and OCEAN[3] gain a special mention.
Reputation based systems are used for enhancing security in ad hoc networks as they model cooperation between the nodes which is inspired from social behavior. Such systems are used to decide whom to trust and to encourage trustworthy behavior. Resnick and Zeckhauser[4] identify three goals for reputation systems:

- To provide information to distinguish between a trustworthy principal and an untrustworthy principal.
- To encourage principals to act in a trustworthy manner
- To discourage untrustworthy principals from participating in the service the reputation mechanism is present to protect.

Watchdog and Path-rater[5] are some essential components of any typical reputation based IDS. Watchdog performs the activity of monitoring its neighborhood and based on these observations, Path-rater ranks the available path in route cache. Misbehavior detection and reputation-based intrusion detection may be either distributed or local. Here, fully distributed means that information regarding one's reputation change is immediately propagated in the whole network. In the latter case, called local reputation based systems, nodes are fully dependent on their personal opinion about other nodes' reputation and behavior.

→SHIELD will go beyond the state-of-the-art in this technology by adapting it to a mobile ad-hoc environment. In such a network, it may be difficult for the reputation upgrading process to cope up with the node mobility and it might not be appropriate to depend solely

[1] P. Michiardi, R. Molva, Core: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", Institut EurecomResearch Report RR-02-062 - December (2001)

[2] Sonja Buchegger and Jean-Yves Le Boudec, Performance Analysis of the confidant Protocol: Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks. Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, June(2002)

[3] Sorav Bansal and Mary Baker, Observation based cooperation enforcement in ad hoc networks" Technical Report, Stanford University, arXiv:cs.NI/0307012 v2 6 Jul (2003).

[4] P. Resnick and R. Zeckhauser. Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system" In M. R. Baye, editor, The Economics of the Internet and E-Commerce, volume 11 of Advances in Applied Microeconomics. Amsterdam, Elsevier Science, (2002).

[5] Sonja Buchegger, Cedric Tissieres, Jean-Yves Le Boudec, A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks How Much Can Watchdogs Really Do?," Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'04), pp. 102-111, (2004).

upon personal observation. Using secondhand information can significantly accelerate the detection and subsequent isolation of malicious nodes in MANETS[1].

Anonymity and Location-privacy techniques

Continued advances in mobile networks and positioning technologies have created a strong market push for location-based applications. Examples include location-aware emergency response, location-based advertisement, and location-based entertainment. An important challenge in wide deployment of location-based services (LBSs) is the privacy-aware management of location information, providing safeguards for location privacy of mobile clients against vulnerabilities for abuse[2]. The studies a new attack on the anonymity of location data is given here[3]. Location-based services offer valuable applications to mobile users. To receive these services, users must disclose their location to service providers. This raises privacy concerns. Location records, when analyzed, can reveal sensitive facts about an individual, such as business connections, political affiliations or medical conditions. Misuse of location data can lead to damaged reputation, harassment, mugging, as well as attacks on an individual's home, friends or relatives.

Location privacy based on k-anonymity addresses this threat by cloaking the person's location such that there are at least k−1 other people within the cloaked area. It is proposed a distributed approach that integrates nicely with existing infrastructures for location-based services[4]. As Global Positioning System (GPS) receivers become a common feature in cell phones, personal digital assistants, and automobiles, there is a growing interest in tracking larger user populations, rather than individual users. Unfortunately, anonymous location samples do not fully solve the privacy problem[5].

The Privacy Grid framework offers three unique capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment[6].

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks which researchers identify as target area of interest for solving the problems[7]. For traffic monitoring system privacy, anonymity and location concerns are given here[8].

[1] S. Buchegger and J.-Y. Le Boudec, The effect of rumor spreading in reputation systems for mobile ad-hoc networks" Proc. WiOpt'03(Modeling and Optimization in Mobile Ad Hoc and Wireless Networks), (2003).

[2] Gedik, B.; Ling Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," Mobile Computing, IEEE Transactions, Volume 7, Issue 1, Jan. 2008 Page(s):1 – 18.

[3] Philippe Golle and Kurt Partridge, "On the Anonymity of Home/Work Location Pairs,"

[4] Ge Zhong and Urs Hengartner, "Toward a Distributed k-Anonymity Protocol for Location Privacy," http://www.cs.uwaterloo.ca/~uhengart/publications/wpes08.pdf

[5] Marco Gruteser and Baik Hoh, "On the Anonymity of Periodic Location Samples," http://www.winlab.rutgers.edu/~gruteser/papers/gruteser_anonymityperiodic.pdf

[6] Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang, "Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid," WWW 2008 / Refereed Track: Mobility April 21-25, 2008 • Beijing, China.

[7] Marco Gruteser and Dirk Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," http://systems.cs.colorado.edu/Papers/Generated/2003anonymousLbs.pdf
Li Xiong, "Report on International Workshop on Privacy and Anonymity in the Information Society (PAIS 2008),"

[8] Baik Hoh, Marco Gruteser," Enhancing Privacy Preservation of Anonymous Location Sampling Techniques in Traffic Monitoring Systems," Securecomm and Workshops, 2006, Publication Date: Aug. 28 2006-Sept. 1 2006, On page(s): 1-3.

→It is demonstrated[1] that existing approaches may fail to provide spatial anonymity for some distributions of user locations and describe a novel technique which solves this problem. *(ii)* Prive, a decentralized architecture for preserving the anonymity
of users issuing spatial queries to LBS. Mobile users self-organize into an overlay network with good fault tolerance and load balancing properties. Prive avoids the bottleneck caused by centralized techniques both in terms of anonymization and location updates. Moreover, the system state is distributed in numerous users, rendering Prive resilient to attacks. Extensive experimental studies suggest that Prive is applicable to real-life scenarios with large populations of mobile users.
In the application field of Health previous research results above will be explore in a unique space of SHIELD System of Systems where different kind of networks (in first place UWN) will be investigated to enhanced anonymity and location-privacy on the level that is required by SHIELD scenarios and user requirements.

Reputation-based Secure Resource Management Procedures

WS-Attestation is a recent mechanism developed by IBM[2] that enables TPM remote controlling by means of web services.

→In order to improve this technology, SHIELD project will design an abstract layer that will consider device's security as a service, so that SHIELD project could control the security of one resource and transactions among resources. This will control also traceability and dependence among resources. This remote control of TPM – reputation based- can identify malicious use, corruption and perform a secure flow control of the job.

Waveform-agile and reliable transmission methodologies

Software defined radio (SDR), from its definition: "Radio in which some or all of the physical layer functions are software defined", allows implementing reliably most of the physical layer function blocks.
Taking our survey from the top of the OSI model, SDR can cooperate with an application software-implemented security, and thus cooperate with security at higher OSI levels. Interoperability with hardware security components is also offering itself, namely with cryptographic key exchange/storage hardware components, pseudo-random number generators etc. Possible benefits at this point are in flexibility to join different security procedures over a range of different communication standards, and in easy integration with hardware security components.
SDR can offer some security functionality also at the physical OSI layer. Various spectrum spreading techniques or channel number (frequency) varying techniques can be easily implemented, where a particular communication standard allows.
Since many software defined radios are realized in conjunction with common personal computers, interconnection with common PC applications providing security/privacy tasks is possible.

→SHIELD will improve the state-of-the-art by developing waveform-agile implementations on SDR platform interconnected with personal computer. Joint and cooperating implementations of security procedures over several communication standards are expected to be accomplished and evaluated.

[1] Gabriel Ghinita et al., "Priv´e: Anonymous Location-Based Queries in Distributed Mobile Systems, WWW 2007 Pervasive Web and Mobility May 8-12, 2007. Banff, Alberta, Canada, pp. 371-380.
[2] White Paper: WS-Attestation: Enabling Trusted Computing on Web Services

Distributed self-management and self-coordination schemes for unmanaged and hybrid networks

The Future Internet is envisioned to leap towards a radical transformation from how we know it today (a mere communication highway) into a vast **hybrid network** seamlessly integrating physical (mobile or static) systems to power, control or operate virtually any device, appliance or system/infrastructure. Manipulation of the physical world occurs locally but control and observability are enabled safely and securely across a (virtual) network. It is this emerging 'hybrid network' that we refer to as an 'eNetwork'. An eNetwork integrates computing, communication and storage capabilities with the monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time. The development of industrial informatics along the five years since the 1st INDIN Conference[1] was marked by most tumultuous transformations in the information and communication technologies (ICT) domain, which are radically and rapidly changing our world[2].

An interesting overview on self-management and related projects from EC is presented here[3]. Autonomous and Autonomic Computing are presented as an interesting fusion for the future networks[4]. Further on, Greenwood paper discusses an approach to seamless hybrid connectivity bridging infrastructure-centric and ad-hoc networks to autonomically maximize the potential for sustained connectivity for terminal device users and their services[5]. Kai et al paper presents a decentralized approach for the autonomic management of a group of collaborating base stations to provide efficient and effective wireless network access in highly dynamic environments. It provides a management platform that supports many different management functions based on common mechanisms for information exchange, transactional semantics and security[6].

Hybrid wireless networks may integrate both Intra and Inter technology cases and the mobile node itself may support heterogeneous technologies switching between them in an on-demand fashion. There are several motivations for considering such hybrid networks design. Firstly, the required hardware already exists, where wireless access points are becoming ubiquitous and all laptops and many PDAs sold today are pre-installed with Wi-Fi. Also, some cellphone manufacturers started offering smart phones that integrate Inter wireless technologies, with a focus on GSM and Wi-Fi.

→Agent and peer-to-peer based decentralized self-management is a developing technology that can change the future of energy markets. Energy markets contain vast numbers of devices that produce and consume electricity. These devices are divided over many management domains, each with their own local service requirements. They operate in a complex and ever

[1] http://www2.enel.ucalgary.ca/INDIN03/

[2] Mihaela Ulieru et al, "Engineering Industrial Ecosystems in a Networked World," http://www.indin2007.org/downloads/keynotes/ulieru.pdf

[3] FAbrizio Sestini, "Self-Management in SAC and FIRE," 2008, ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/future-networks/event-20080930-self-management-sac-fire_en.pdf

[4] D. Greenwood Realizing Tangible Business Value from the Fusion of Autonomous and Autonomic Technologies http://www.iaria.org/conferences2007/filesICAS07/Keynote_Greenwood.pdf

[5] D. Greenwood et al., "Hybrid Seamless Mobility Supporting Pervasive Service Collaboration," http://www.whitestein.com/library/WhitesteinTechnologies_Paper_UBICOMM2008.pdf

[6] Kai Zimmermann, Sebastian Felis, Stefan Schmid, "Autonomic Wireless Network Management," https://fit.nokia.com/lars/papers/WAC2005.pdf

changing physical environment, and must serve the needs of a highly autonomous user group[1].

Complex, intelligent, distributed systems in dynamic environments need to adapt continually, and thus need to be designed to this purpose. As central management of such systems is often not an option decentralized self-management is required. Therefore, distributed energy resource self management is a challenge for SHIELD framework on hybrid networks.

Rammig presented[2] a vision of establishing self-coordination as the dominant paradigm of operation of future embedded computing environments. This vision is looked at from three different points of view. First of all techniques to model self-coordinating distributed systems in an adequate manner and algorithmic techniques for such systems are discussed. Then the principle of self-coordination is applied to build proper system structure.

Secure service discovery, composition and delivery protocols

Services among distributed networks must be discovered, composed and delivered in a secure way. These procedures are well defined and consolidated in trusted environment, but with no or limited attention to security issues. Specifically for web services, OASIS[3] (Organization for the Advancement of Structured Information Standards) is working on and progressively releasing a set of standards for protocols to be adopted with the aim to introduce security to web-services. Those protocols are commonly referred as WS-Security or WS-* specifications. Currently the following draft specifications are associated with WS-Security:

- WS-Secure Conversation
- WS-Federation
- WS-Authorization
- WS-Policy

→SHIELD will implement (and if possible) refine these specification to release a very first implementation of some of these mechanism; among them, the most interesting issues is the definition of WS-Security Policy. WS-Security Policy is a standard that regulate a security assertion model, a security binding abstraction and policy considerations.

Policy-based SPD management

Policies permit the declarative specification of security strategies separately from the implementation code of I-ES nodes. The use of interpreted policies allows to change the security behavior of a node without recoding or shutting down the node

In a policy based approach the common characteristics of SDP contexts are structured information, hierarchically organized with enough generality to be adopted in similar environments.

A semantic approach can be used to represent both the policies and the methods to be used to evaluate policy decisions.

Dynamic policy management is the key to achieve higher levels of security, privacy and dependability.

→In this aspect, SHIELD will implement the technologies to provide the ES networks with the ability to adapt the policies at runtime to changes in the environment to react to ongoing attacks. These technologies will be developed starting from the concepts and technologies

[1] Frances Brazier, Elth Ogston, Martijn Warnier, “The Future of Energy Markets and the Challenge of Decentralized Self-Management,”

[2] Franz J. Rammig,” Engineering Self-Coordinating Real-Time Systems,” ISORC’07, 7-9 May 2007 Page(s):21 – 28

[3] http://www.oasis-open.org

developed in the SERENITY and MASTER projects (both dealing with dynamic policy management), and adapting them to the particularities of Embedded systems. The objective is that the provided policy management framework is not simply an adaptation of an existing one, but, on the contrary, designed for the particularities of the ESs.

Semantic representation of the SPD knowledge domain

Semantic technologies are useful to address the interoperability among different (SPD) technologies. A semantic ontology can describe the SPD modules capabilities and interfaces, can represent the metrics and all the exchanged information between the node, network, middleware and overlay layer; semantic ontology can be used also to represent profiles and policies according to interoperable and self describing formats. This is only an example of the possible use of the current state-of-the-art semantic technologies.

→SHIELD will improve this current technology by developing a “lightweight” common semantic languages derived by standard ones (OWL) in order to be easily processed in the Embedded System world, where the processing unit are limited in power and resources.

Secure Resource Management Procedures (at middleware level)

The main key points to manage middleware resources are: the knowledge of their availability, a policy to assign them, a secure model to identify and authorize the requests, an account system to track the resource usage.

→Most of those features can be addressed by protocols like Diameter[1]. Diameter protocol and its extensions are already strongly adopted in many IP systems[2] in order to support Strong Security, Accounting and Resource Management. SHIELD will adopt the same model in the context of secure resource management procedures to be performed at the middleware level of embedded systems networks.

Secure Offline Authentication with mobile devices

Algorithms and protocols for asymmetric cryptography usually need powerful hardware to compute the key generation, encryption, decryption or signature verification algorithms and reasonable storage space to store the private keys, public keys and certificates.

→The technology to be developed during the SHIELD project shall provide an optimized hardware implementation for an elliptic curve cryptography based public-key authentication algorithm. Elliptic curve cryptography is a cryptographic algorithm based on the algebraic structure of elliptic curves over finite fields. It allows much shorter key lengths to reach the same security level as earlier public-key systems, such as the RSA algorithm. This fact is very useful at mobile devices to overcome the storage space constraints.

The great advantage of public key cryptography compared to symmetric cryptosystems is the offline capability at signature verification. As soon as the corresponding public key certificate is loaded the mobile device can verify digital signatures without the need of connectivity to any host.

[1] P. Calhoun and others (September 2003) RFC 3588, “Diameter Base Protocol”, IETF (http://tools.ietf.org/html/rfc3588)

[2] For example the 3rd Generation Partnership Project (3GPP) in defining the Cx, Dh, Dx, Rf, Ro, and Sh interfaces of the IP Multimedia Subsystem (IMS), http://www.3gpp.org.

Mobile devices have become a pervasive part of our everyday live and will become even more important in the coming years. But why not use these devices for interactions between the virtual and the user's world? To make this vision true security concerns need to be addressed carefully.

→In the run of the SHIELD project a secure asymmetric authentication protocol based on elliptic curve cryptography running on mobile devices which have known disadvantages in computing capability, storage space, energy constraints and unstable online connection will be implemented to eliminate those security concerns for the future.

2.2.3 - Relevant work and potential improvements in European research projects

In call ***ARTEMIS-2008-1*** no projects has been funded for the sub programme 6 that could specifically provide a holistic approach to Security, Dependability and Privacy in Embedded Systems. For that reason SHIELD represent itself the very first milestone towards such harmonization.

Moreover, other projects have been funded in other ARTEMIS sub-programmes that involve some unresolved SPD aspects as well as some concept that SHIELD would like to address.

CESAR

CESAR aims at bringing significant and conclusive innovations in the two most improvable systems engineering disciplines:

- Requirements engineering, in particular through formalization of multi viewpoint, multi criteria and multi level requirements,
- Component based engineering applied to design space exploration, comprising multi-view, multi-criteria and multi level architecture trade-offs.

CESAR intends to provide industrial companies with a breakthrough in system development by deploying a customizable systems engineering 'Reference Technology Platform' (RTP) making it possible to integrate or interoperate existing or emerging available technologies. This would be a significant step forward in terms of industrial performance improvement that will help to establish de-facto standards and contribute to the standardization effort from a European perspective.

SHIELD perfectly fits this view, since it also aim at deploying a "Reference **SPD** Platform" making it possible to integrate or interoperate existing or emerging available **SPD** technologies. Moreover SHIELD will overcome this "reference design" by "implementing" the proposed platform in significant industrial application scenarios.

CHARTER

CHARTER is trying to ease, accelerate, and cost-reduce the certification of critical embedded systems by melding real-time Java, Model Driven Development, rule-based compilation, and formal verification. This approach, Quality-Embedded Development (QED), will push software certification to a new level and thereby significantly contribute to the safety and security of the upcoming age of an embedded software society.

SHIELD will extend this idea not only to software certification, but to the whole SPD chain: the benefits of the SHIELD architecture in terms of cost-reduction of certification have been already illustrated.

EMMON

Improving sustainability of urban life requires that monitoring of huge geographical extensions is performed in real time. The EMMON project aims to allow such monitoring using Wireless Sensor Network (WSN) devices – small, communicating and cooperative nodes with sensors. In order to achieve this ambition, EMMON will perform technological research at the level of devices, in new, efficient, and low power consumption communication protocols, embedded software with better overall energy efficiency, secure, fault-tolerant and reliable middleware for large scale monitoring and remote command and control operational systems for end-users.

SHIELD will improve this vision by performing technological improvements not only for nodes dependability, but also for critical SPD oriented basic functionalities that are important in (but not limited to) monitoring applications.

SMART

There are certain specific and very important, for numerous application domains, features of WSNs such as high-security levels, low power consumption, video-capabilities, auto-configuration and self-organization, that are not efficiently addressed by today's offerings; SMART aims at providing an infrastructure that will support all those features efficiently and inexpensively. This innovative infrastructure will be based on both an off-the-shelf reconfigurable device and on a specially designed and implemented Reconfigurable Application-Specific Instruction-set Processor (RASIP). Even though, the reconfigurable hardware resources are often considered, for certain processing tasks, more power hungry than the ultra-low-power microcontrollers, it has been proved that they allow for extremely more performant and power-efficient processing when implementing encryption/decryption/authentication algorithms as well as data/video/image compression tasks. The SMART system will also take advantage of the partial real-time reconfiguration feature of the reconfigurable devices and will be able to alter their processing tasks according to the environment the sensor network operates in.

SHIELD, thanks also to the experience of HAI, who is member of the SMART consortium, will overcome the idea of this project by addressing single SPD basic functionalities instead of producing ex-novo a secure node. This will improve the state-of-the-art giving flexibility, in this case, at node level, allowing the same performance in different application scenarios.

Also in ***FP7*** research, particular effort has been put in Security topics, both with general and specific calls[1]; we have identified some potential starting point that SHIELD will improve with its outcome and approach.

IMSK

The aim of the Integrated Mobile Security Kit project is to combine technologies for area surveillance, checkpoint control, also CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security.

[1] Towards a more secure society and increased industrial competitiveness, May 2009, European Commission

SHIELD will extend the objective of this project by “embedding” the composability concept into any Embedded Systems, not only the ones dedicated to a specific application. Thanks to the outcome of SHIELD, in terms of basic functionalities and specifications, each device can be composed to provide a valuable platform also (but not limited to) critical applications.

ECRYPT II

European Network of Excellence for Cryptology II, a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7). It falls under the action line *Secure, dependable and trusted infrastructures*. ECRYPT II started on 1 August 2008 and its objective is to continue intensifying the collaboration of European researchers in information security. It is organized in three labs: (i) Symmetric techniques virtual lab (SymLab); (ii) Multi-party and asymmetric algorithms virtual lab virtual lab (MAYA); (iii) Secure and efficient implementations virtual lab (VAMPIRE). In particular the main objectives of these labs are the optimization of cryptography or other security primitives and the adaptation to new quantum computing, while the development of lightweight cryptography (suitable to a low-powered environment) is only the secondary objective, still open.

SHIELD will go beyond the state of the art of this project by deeply investigating and producing the lightweight cryptographic algorithms and techniques for devices with low power and computational resources; SHIELD consortium believes that, rather then quantum computing, embedded computing will be of capital importance in the next years, so this objective should be perceived with major effort.

Section 3 - S&T approach and work plan

3.1 - Quality and effectiveness of the S&T methodology and associated work plan

3.1.1 - Overall strategy of the Work Plan

The project work plan lasts 12 months. Activities will be compliant with deliverables and milestones lists. Some phases (see figure and table below) have been identified corresponding to critical steps in the development of SHIELD framework.

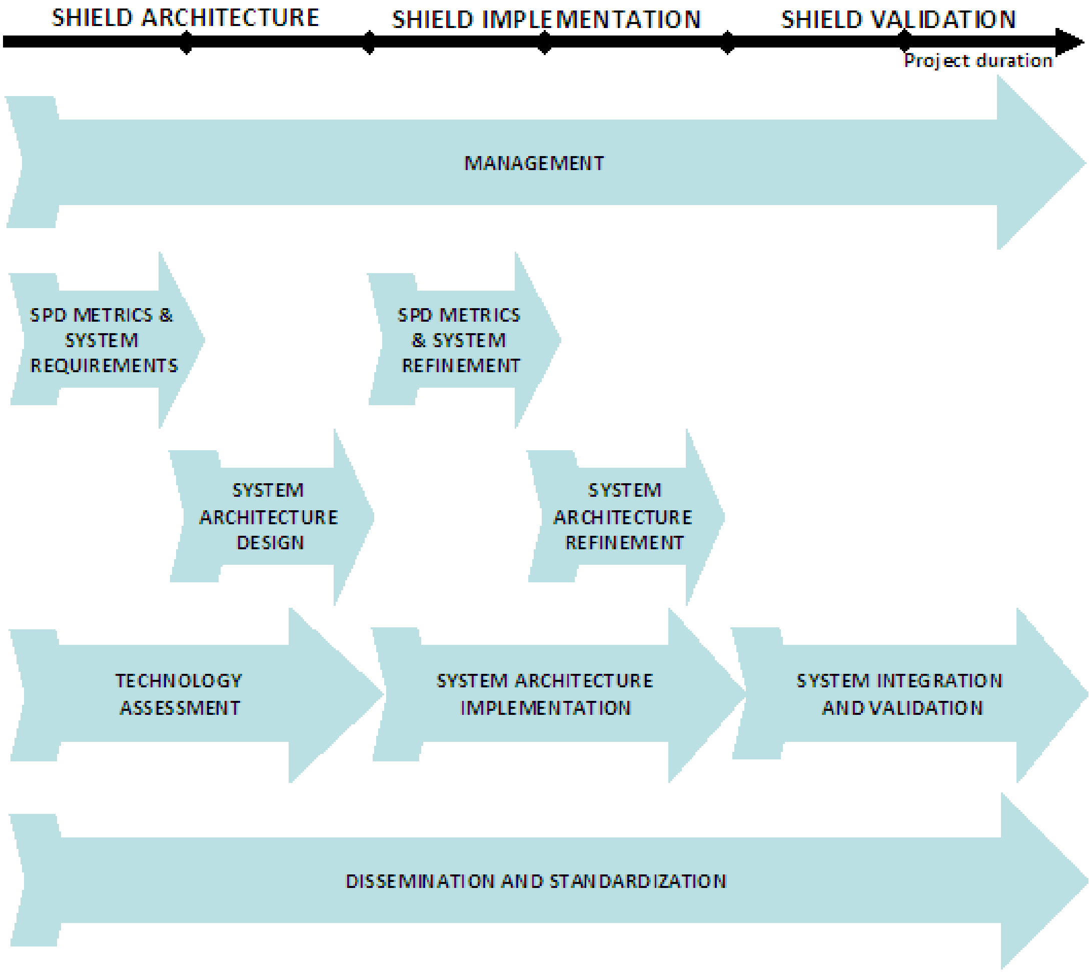

SHIELD ARCHITECTURE
SHIELD IMPLEMENTATION
SHIELD VALIDATION
Project duration
MANAGEMENT
SPD METRICS & SYSTEM REQUIREMENTS
SPD METRICS & SYSTEM REFINEMENT
SYSTEM ARCHITECTURE DESIGN
SYSTEM ARCHITECTURE REFINEMENT
TECHNOLOGY ASSESSMENT
SYSTEM ARCHITECTURE IMPLEMENTATION
SYSTEM INTEGRATION AND VALIDATION
DISSEMINATION AND STANDARDIZATION

Figure 3.1 – SHIELD Phases

Phase	Related activities
Technologies assessment	**Classification of technologies** pertaining to the SHIELD objectives will be performed **taking into account current standardization activities, as well as outputs from the most important industrial past and ongoing (and finished) private and public research projects**. Note that the **partners involved in SHIELD have participated to most of the main European research projects** with results in the scope of SHIELD and are involved in several related industrial projects; so, first of all, they will analyze and exploit the good results already achieved, thus avoiding wasting resources in replicating activities.

Phase	Related activities
SPD metrics and Requirements Definition	**Generic SPD metrics as well as the high level requirements, not peculiar to a specific application context, will be defined** to classify and validate SHIELD functionalities in current and future market spreading perspective
System Architecture Design	System architecture will be defined including the identification of all the functionalities and of their SPD requirements. In spite of these application scenario, it is important to underline that **the aim of the project is not to produce a working system for a narrow or specific domain**, **but to produce an innovative, modular, composable, expandable and high-dependable architectural framework** and concrete tools capable of improving the overall SPD level in any ARTEMIS sub-programmes context, with minimum engineering effort.
System Architecture implementation	The various functionalities will be designed and implemented. The **SPD performance of the various functionalities will be separately tested**, **aiming at validating,** through the set of defined metrics**, the compliance of the achieved SPD performance with the SPD requirements**.
SPD Metrics and Requirements Refinement	**SPD metrics will be refined as well as the requirements** taking into account the scenario. Particular attention will be devoted to this phase in order to **understand which performance indicators and peculiar requirements are the most suitable for the selected application domain**.
Architecture tailored Refinement	The **general system architecture will be personalized and tailored on the selected application scenario**. According to continuous evolution in ESs research and development activities (e.g. other ARTEMIS projects outcomes), a refined **enhanced SHIELD implementation will be designed.**
System Integration and Validation	The **system integration** phase **will lead to the final pilot prototype**. **Extensive trials, basing on defined SPD metrics, will be performed to test the selected Value Added Service**. Therefore, pilot prototype and field trial set-ups, including prototypes, performances will **prove SHIELD's platform advanced security, privacy and dependability functionalities**.
Dissemination and Exploitation	Activities will ensure the **impact of the project outputs on the outside world**. **Liaisons with other Artemis projects will guarantee project results in line with the overall JU expectations**. **A pilot demonstrator**-will be setup at the end of the project, **in order to show the composability of different SPD technologies in an integrated SPD chain**.
Management	Activities will ensure that project objectives will be effectively and efficiently met. Moreover, **a check** has been foreseen in order to guarantee that the SHIELD project will always be **in line with industrial and market trends**.

pSHIELD has been organized in 7 work packages, each one divided into Tasks. Here is listed the complete work breakdown structure.

WP no.	Work package title	Leader	Person-months
WP1	**Project Management**	**SESM**	62,5
Task 1.1	Project management	SESM	
Task 1.2	Liaisons	SESM	
WP2	**SPD Metric, requirements and system design**	**THYIA**	76
Task 2.1	Multi-technology requirements & specification	ASTS	
Task 2.2	Multi-technology SPD metrics	Tecnalia	
Task 2.3	Multi-technology architectural design	HAI	
WP3	**SPD Node**	**SESM**	151,8
Task 3.1	Nano, micro/personal node	THYIA	
Task 3.2	Power node	ETH	
Task 3.3	Dependable self-x and cryptographic technologies	AS	
WP4	**SPD Network**	**SCOM**	61
Task 4.1	Smart SPD driven transmission	SCOM	
Task 4.2	Trusted and dependable Connectivity	MGEP	
WP5	**SPD Middleware & Overlay**	**ED**	116
Task 5.1	SPD driven Semantics	TRS	
Task 5.2	Core SPD services	THYIA	
Task 5.3	Policy-based management	ED	
Task 5.5	Overlay monitoring and reacting system by security agents	ED	
WP6	**Platform integration, validation & demonstration**	**HAI**	134,5
Task 6.1	Multi-Technology System Integration	HAI	
Task 6.2	Multi-Technology Validation & Verification	ED	
Task 6.3	Lifecycle SPD Support	ATHENA	
Task 6.4	Multi-Tecnology Demonstration	ASTS	
WP7	**Knowledge exchange and industrial validation**	**CWIN**	27,2
Task 7.1	Dissemination	SESM	
Task 7.7	Exploitation	CWIN	
	TOTAL		629

It is important noting that the SHIELD breakdown structure reflects the System Architecture described in Section 2. In particular, WP3, deals with the design and development of SHIELD SPD modules at node level, WP4 deals with the design and development of SHIELD SPD modules at network level and WP5 takes care of middleware layer SPD modules and the overlay system created by the security agents. WP2 focuses on the identification of the overall SHIELD system requirements and specification, its design and the definition of the SPD metrics. WP6 integrates, validates and verifies the solutions developed in WP3, WP4 and WP5 using the metrics and the specifications provided by WP2. WP6 is also in charge of validating the SHIELD framework by means of significant application scenarios. The project WBS is depicted below.

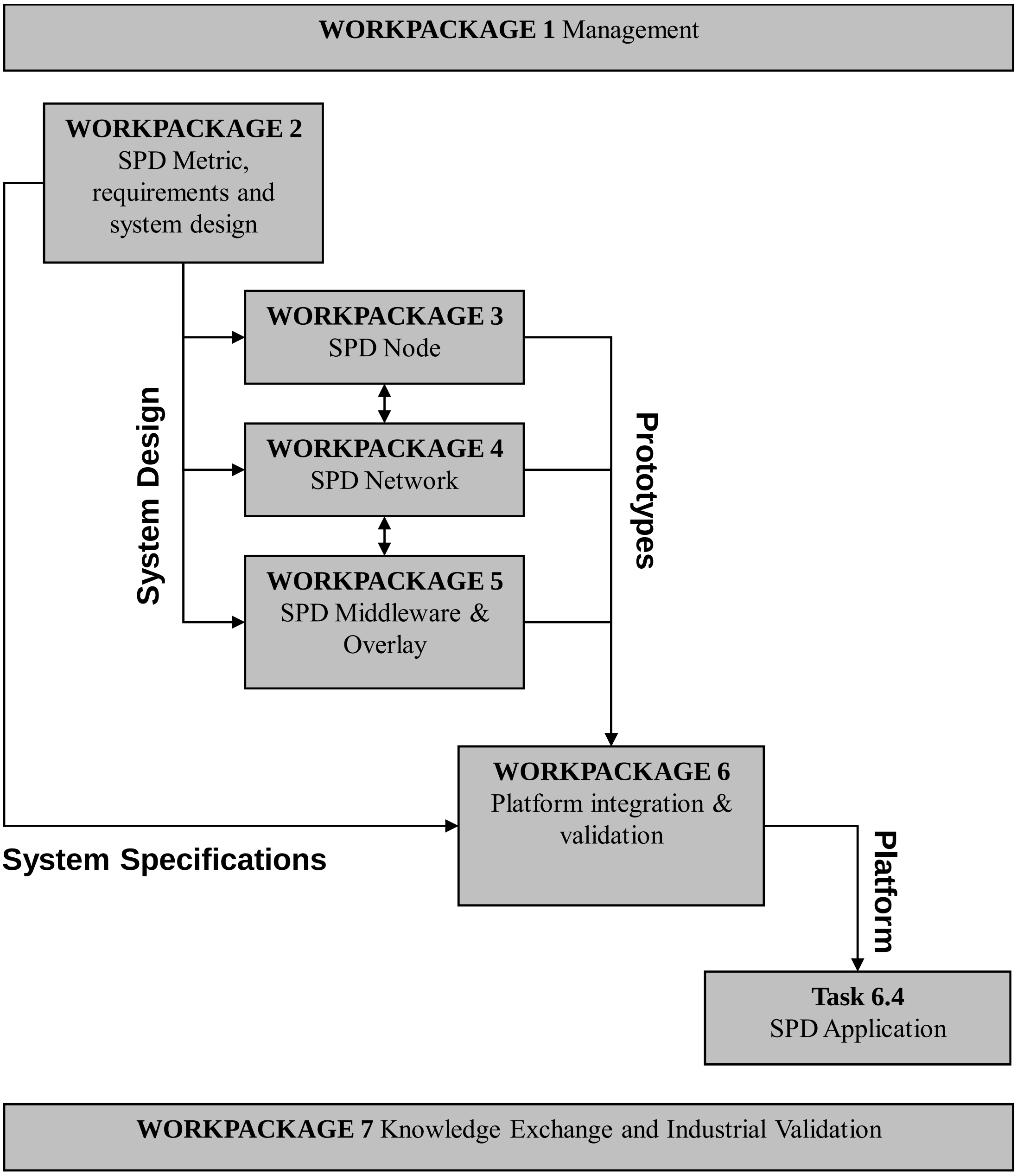
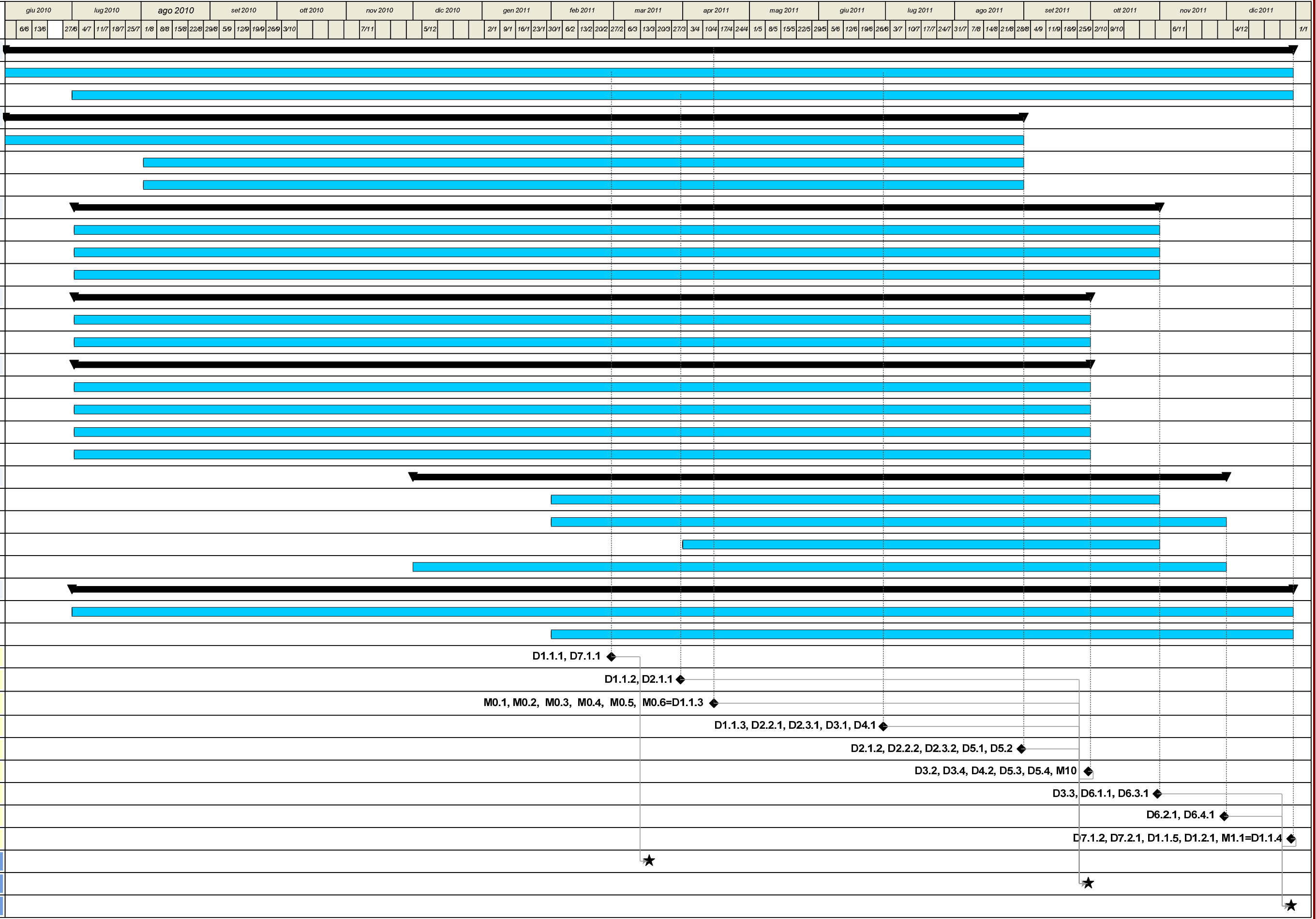


Figure 3.2 – SHIELD Work Breakdown Structure

3.2 - Timing of work packages and their components

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



3.3 - Work package list/overview

Work package no[1]	Work package title	Lead partic. no.[2]	Lead partic. short name	Person-months[3]	Start month[4]	End month
WP1	Project Management	12	MAS	62,5	0	19
WP2	Scenarios, requirements and system design	20	THYIA	76	0	15
WP3	SPD Node	1	SESM	151,8	1	17
WP4	SPD Network	15	SCOM	61	1	16
WP5	SPD Middleware & Overlay	7	ED	116	1	16
WP6	Platform integration, validation & demonstration	10	HAI	134,5	6	18
WP7	Knowledge exchange and industrial validation	6	CWIN	27,2	1	19
	TOTAL			629		

[1] Workpackage number: WP 1 – WP n.

[2] Number of the participant leading the work in this work package.

[3] The total number of person-months allocated to each work package.

[4] Measured in months from the project start date (month 1).

3.4 - Deliverables list

Del. no.[1]	Deliverable name	WP	Nature[2]	Dissem. level[3]	Deliv.[4] month
D1.1.1	Collaborative tools and document repository	1	O	PP internal	9
D7.1.1	Web Site	7	O	PU public	9
D1.1.2	Quality Control Guidelines	1	R	PP	10
D2.1.1	System Requirements and Specifications	2	R	PU	10
D1.1.3	Management Plan	1	R	PP	13
D2.2.1	Preliminary SPD Metrics Specifications	2	R	PP	13
D2.3.1	Preliminary System Architecture Design	2	R	PP	13
D3.1	SPD node technologies prototype	3	P,O	PP	15
D4.1	SPD network technologies prototype	4	P,O	PP	13
D5.1	pSHIELD semantic models	5	R	PP	15
D5.2	SPD middleware and overlay functionalities prototype	5	P,O	PP	15
D2.1.2	System Requirements and Specifications – Next Realize	2	R	PU	15
D2.2.2	SPD Metrics Specifications	2	R	PU	15
D2.3.2	System Architecture Design	2	R	PU	15
D3.2	SPD nano, micro/personal node technologies prototype report	3	R	PU	16
D3.3	SPD power node technologies prototype report	3	R	PU	17
D3.4	SPD self-x and cryptographic technologies prototype report	3	R	PU	16
D4.2	SPD network technologies prototype report	4	R	PU	16
D5.3	pSHIELD semantic models report	5	R	PU	16
D5.4	SPD middleware and overlay functionality report	5	R	PU	16
D6.1.1	Platform integration report	6	R	PU	17
D1.1.5	Quality Control Report	1	R	PU	19
D1.2.1	Liaisons Report	1	R	PU	19
D6.2.1	Platform validation and verification	6	R	PU	18
D6.3.1	Lifecycle and SPD Support Report	6	R	PU	17

[1] Deliverable numbers in order of delivery dates. Please use the numbering convention <WP number>.<number of deliverable within that WP>. For example, deliverable 4.2 would be the second deliverable from work package 4.

[2] Please indicate the nature of the deliverable using one of the following codes:
R = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

[3] Please indicate the dissemination level using one of the following codes:
PU = Public
PP = Restricted to other programme participants (including the JU).
RE = Restricted to a group specified by the consortium (including the JU).
CO = Confidential, only for members of the consortium (including the JU).

[4] Measured in months from the project start date (month 1).

Del. no. [1]	Deliverable name	WP	Nature[2]	Dissem. level[3]	Deliv.[4] month
D6.4.1	pSHIELD demonstrator	6	R,P,O	PU	19
D7.1.2	Dissemination Report	7	R	PU	19
D7.2.1	Exploitation Plan	7	R	PU	19

Milestones deliverables:

M0.1 Project Periodic Report – Management Report (M10)
M1.0 Project Periodic Report – Management Report (M15) /supplementary review in Sept. 2011
M1.1 Project Final Report – Management Report (M19) /final review in February - March 2012

3.5 - Work package descriptions

Work package number	**WP1**	**Start date or starting event:**		**Month 0**				
Work package title	**Project Management**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	36	1	3	0	3	0	3	2
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	2	1	~~1~~	1	0,5	4	2	1
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	2						

Objectives

The aim of this work package is to provide the internal project management and the overall coordination of activities, financial and technical planning and control. It ensures that the project objectives are met and represents the contact point of the project to the ARTEMIS JU and the external world. It also addresses any issues concerning access rights, including cases where partners join or leave the project during its duration. It is assisted in its tasks by other bodies established as part of the management structure.

Description of work (WP Leader: MAS)

Task 1.1: Project management (Leader: MAS - Partners: AS, ASTS, CS, ED, Tecnalia, ETH, HAI, ~~ISD,~~ MAS, MGEP, SCOM, SESM, THYIA, TRS, UNIROMA1)

The management structure used for the project is described in section 5.1. The construction and roles of the PA and TMC are defined in the Consortium Agreement. They will supervise work package and task progress and content and timely availability of project deliverables to the project coordinator and the PA. Project coordination will execute the routines for the internal project management and overall coordination of activities. It will ensure that the overall project contractual requirements are met in accordance with the time plan and budget. It will also supervise the process of handling internal disputes, dealing with non-performing partners and the entering and leaving of partners. It will also address any issues concerning access rights and IPRs.

The work to be performed includes the following specific tasks:

- Overall financial and technical planning;
- Controlling project scheduling and achievements;
- Reporting of progress and resource expenditure;

- Organization of the meetings of the PA, TMC, plenary, and review meetings;
- Liaison with other projects (at a technical level, liaison will also be performed by WP leaders and individual partners);
- Handling the cost claim procedures and maintaining the financial budget status of each partner;
- Maintaining the technical description of the work and the Consortium Agreement;
- Approving and validating the visible outputs, such as deliverables, presentation material, papers, etc., thus adding a level of quality assurance to the project;
- Managing intellectual properties and patent requests;
- Supervising the website and e-mail lists;
- Contact point to the ARTEMIS JU including supervision of deliverable creation and in-time forwarding;
- Chairing processes to handle IPR on project results.

This task is mainly devoted to management. All participants are included according to the described management structure.

Task 1.2: Liaisons (Leader: SESM - Partners: ASTS, CS, SCOM)

In an early stage of the project the partner involved in this task will search for other EC FP7 and Artemis funded projects, concerning topics related to SHIELD. Then, a strong relationship will be solicited and established to share and improve the results of the single project and of the whole Artemis technology platform. This will permit a useful exchange of knowledge among consortia and an improved, coordinated and synergetic continuation of the standardization processes.

The SHIELD identified technologies and solutions will represent a reference guideline for the design and development of ESs where SPD capabilities are required. In particular, the SHIELD results will be used for the cross fertilization among projects and will be available for possible reuse to provide SPD features to the ESs that might be designed and developed in other projects.

Deliverables

Public

~~D1.1.4 Annual Report (M12)~~

D1.1.5 Quality Control Report (M19)

D1.2.1 Liason Report (M19)

Internal

D1.1.1 Collaborative tools and document repository (M9)

D1.1.2 Quality Control Guidelines (M10)

D1.1.3 Management Plan (M13)

Milestones

M1 Project collaborative working environment (M9)

Work package number	**WP2**	**Start date or starting event:**		**Month 0**				
Work package title	**SPD metrics, requirements and system design**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	9	0	14	3	3	4	8	2
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	12	9	~~0~~	0	0	1	11	0
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	0						

Objectives

The objectives of WP2 are:

- 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;
- The definition of proper SPD metrics to assess the achieved SPD level of each layer, as well as of the overall system;
- The definition of SHIELD system architecture. Identification of the SPD layers functionalities, their intra and inter layer interfaces and relationships

Description of work (WP Leader: THYIA)

Task 2.1 Multi-technology requirements & specification (Task Leader: ASTS - Partners: SESM, CS, CWIN, ED, ETH, THYIA)

This task will identify the requirements and describe the specifications of the overall SHIELD system. For each SPD technology, for each layer, a formal set of high level, architectural, interface and performance requirements will be identified. This task will be influenced by the application scenario. This scenario will be taken as a reference for defining the SPD requirements of each architectural layer (even though the conceived architecture will be able to support any ES scenario). Requirements and specification will be also influenced by the liaisons activated in WP1.

An iterative approach will be adopted. A preliminary set of requirements and specification will be provided at the early beginning of the project. The preliminary outcome of this task will be used by WP3, WP4 and WP5 to develop potential prototypes and by WP6 to validate them. The requirements and specification will be refined on the basis of the results of the validation phase and on the detailed description of the application scenarios from Task 6.4.

The partner involved in this task are representative of SPD industries deeply involved in the technical work packages (WP3, WP4 and WP5) and end user involved in the demonstration of real SPD applications (Task 6.4).

Task 2.2 Multi-technology SPD metrics (Task Leader: Tecnalia - Partners: ASTS, ATHENA, CS, CWIN, ED, Tecnalia, ETH, THYIA)

The main result of this task will be the identification of SPD metrics. As a matter of fact, for the SPD needs, metrics are required for the measurement of security, dependability, reliability, trust and reputation, availability, privacy, anonymity and traceability, for all the levels (node, network communication, middleware, applications). The proposed metrics will be also based on the scenario identified in Task 6.4.
Task 2.2 aims at developing the basis for system interoperation on all levels (node, network and middleware). In order to pursue such aim, another result of this task shall be metrics and standards for the interoperation of nodes and systems, which shall be part of the future standardization for such systems. As also influence on legislative issues might be possible, special reports may extend the task deliveries in case of detection of such issues.

A further result of this task will be the formal description of SPD requirements and specifications. In this respect, they will be derived from the inputs of all the technical work packages (WP3, WP4 and WP5) and, since a significant part of these requirements may overlap or conflict with each other due to their multiple origins, an efficient coordination will be fundamental. The final result will be a coherent and clear description of the SPD metrics specifications, acceptable by all partners. Within the project, this task builds the basis for all subsequent steps by providing some standard metrics for the integration and test of the specific components/subsystems which are implemented for demonstration purposes.

As for Task 2.1, this task will provide a preliminary description of SPD metrics to influence the prototype development in WP3, WP4, WP5, to start the SPD lifecycle activities in WP6 and to provide support to the validation phase. After the integration of the preliminary prototypes a refinement of the SPD metrics will be done accounting the application scenario.

Task 2.3 Multi-technology architectural design (Task Leader: HAI - Partners: SESM, ATHENA, CS, CWIN, ED, ETH, SCOM, THYIA)

R&D for embedded security, intended as a system issue that must be solved at all abstraction levels (protocols, algorithms, architecture), will lead, in the framework of this task, to a coherent, composable and modular architecture for a flexible distribution of SPD information and functionalities between different ESs while supporting security and dependability characteristics.

This task aims, at the one hand, to explore the minimum set of interdependencies between applications and architectures in an efficient way and to systematically classify those with respect to SPD. On the other hand, it aims to produce a composable architecture which will include most critical elements, thus covering most of the SPD requirements for all the applications. This approach is expected to produce a multi-layered architecture, where each layer consists of several hardware and software SPD modules (components), since it is imperative to take into account the need for composable security, privacy and dependability.

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.

Deliverables

Public

D2.1.1 System requirements and specifications – Realize 2 (M10)

D2.2.2 SPD Metrics specifications (M15)

D2.3.2 System architecture design (M15)

D2.1.2 System requirements and specifications – Realize 3 (M15)

Internal

D2.2.1 Preliminary SPD metrics specifications (M13)

D2.3.1 Preliminary system architecture design (M13)

Milestones

M2	System requirements and specification (M10)
M3	Preliminary SPD metrics and system architecture design and network prototype (M13)
M4	SPD metrics, system architecture design and preliminary SPD prototypes (M15)

Work package number	**WP3**	**Start date or starting event:**			**Month 1**			
Work package title	**SPD Node**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	29	20	0	4	18	7	0	0
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	42	0	~~8~~	2,8	0	0	21	0
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	0						

Objectives

This WP is dedicated to:

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

Description of work (WP Leader: SESM)

In the following section the technologies examined in the pSHIELD project are described. However, since pSHIELD is a pilot project, these technologies could not be fully addressed, but they will be addressed with different effort according to the reduced budget. Moreover the participation with reduced effort (less than 2mm) for some partners has been foreseen to perform, for some technologies, only a technological scouting.

The WP aims at providing SPD intrinsic capabilities at node layer through the creation of an Intelligent ES HW/SW Platform consisting of three different kinds of Intelligent ES Nodes: nano node, micro/personal node and power node. These three node types (which can be considered three node levels of increasing complexity) will represent the basic components of the lower part of the SPD Pervasive System, and will cover the possible requirements of several market areas: from field data acquisition, to transportation, to personal space, to home environment, to public infrastructures, etc.

Moreover, the selected application scenario, described in detail in WP6, will drive the identification of the Intelligent ES nodes that needs to be developed and the identification of the selected devices to be used in their pilot implementation. As well, the sharing and exchange of proper design specifications and requirements previously defined in WP2 will permit the development of SHIELD framework first level (the node level).

The activities will start from SPD simple nodes creation, the nano nodes, filling the lacks of intrinsic SPD capabilities of this device level considering current state of the art. These intrinsic SPD features and capabilities are mandatory in contexts with high SPD requirements in order to satisfy the SPD more complex requirements of the higher node levels (i.e. micro/personal and power nodes).

The effectiveness of the results will be guaranteed by an iterative process of refinement and enrichment. Such a strategy will be based both on the bidirectional exchange of specifications and feedbacks between these levels and the other tasks of the WP3 and on the contribution coming from research and development activities performed in WP2 and WP4 which are strictly interconnected and interdependent with WP3.

More in detail, WP3 Tasks will follow the specifications, requirements and architectural guidelines identified and described in Tasks 2.2 and 2.3. The design and development of the Intelligent ES Nodes and of the whole HW/SW Platform, in fact, will rely on a set of technologies improvement and composability in the overall SHIELD framework, as specified in WP2.

Each task will contribute to improve and enable the composability mechanisms of the whole node-specific set of SPD technologies. Nonetheless each task will affect and give specific attention to the development of specific technologies, as detailed in the following.

Task 3.1 Nano, Micro/Personal node (Task Leader: THYIA - Partners: AS, CS, CWIN, ~~ISD,~~ MAS)

Nano nodes represent the leaves of the pervasive system and typically consist of small devices with limited resources both in terms of hardware and software. Their simplicity and limitations don’t represent a guarantee in terms of SPD and, considering their role and massive distribution in the environment, they could become an interesting target for attacks, hacking, etc. A good representative of this class of ES is Wireless Sensor Network: wireless sensor nodes will be considered as the reference point for prototype development. Starting from the experience matured on existing devices, this task will propose a new class of nano node that will provide the enhancement the following technologies:

- Intrinsically secure ES firmware. Security issues in firmware have never been explored as well as the techniques to make it intrinsically secure. Since the node is the basic component of the SHIELD architecture, particular care will be devoted to the secure boot of the nano node and integrity protection of the ES firmware based on hardware “hooks” and secure key installation at manufacturing or at deployment (depending on usage scenario). In particular, novel methods and tools will be investigated, taking into account nano node hardware constraints as well as nano node performance limitations. Secure firmware upgrade mechanisms will also be designed and verified;

- Power supply protection of multiple sources. It is to maintain operation even if external power supply is removed (i.e. blackout / malicious or not). The research which will be performed under the SHIELD project will combine both countermeasures in case of failure, together with protection circuits of the power supply units. Under the first topic, concepts such as microgenerators, supercapacitors, remote powering and secondary power sources will be investigated, while under the second topic, the research will focus on the selection of different operative modes, being able to plug or unplug critical and non-critical sections of the nodes, or disconnect any damage sub-system which fails or works in a suspicious mode (minimizing the risk of leakages). This part of the work will be of close interaction with the other architecture tasks (WP2), because it will be required to know how the system works, and characterize the degree of importance of any of the sub-systems on the architecture

The micro/personal node class consists of devices richer than the nano nodes in terms of hardware and software resources, network access capabilities, mobility, interfaces, sensing capabilities etc.. Starting from the requirements and architecture output from WP2, SICS will work with the design of trusted boot and software upgrade for micro/personal nodes based on TCG technologies. In particular we will make detailed design proposal evaluating usage of the TCG mobile phone profile and the Mobile Trusted Module (MTM). We envision the final design using either a standard TCG TPM module or the MTM as core root-of-trust in the system. In particular we will focus on secure boot and secure software upgrade methods with the goal of having interoperability with the nano node secure firmware upgrade principles to as large extent as possible.

A prototype will be developed accordingly with the requirements and specification provided by task 2.1. Proper interfaces (defined in task 2.3) will allow the nano and micro/personal node interoperation with the rest of SHIELD platform.

Task 3.2 Power node (Task Leader: ETH - Partners: SESM, AS, CWIN)

This Task will focus on devices that maintain the characteristic of an ES though offering high performance in terms of computing power. This class of nodes represents, in the pervasive system, the first level of massive data elaboration, with the peculiarity that the computing power is provided directly on the field. The Task will focus on the following technologies:

- Rugged High Performance Computing Node. This node will represent a ruggedized platform that provides a HPC ES on the field, wherever is required, without the limitations of a classical HPC solution in terms of working conditions, energy consumption, dimensions, etc. The node will be developed starting from the experience matured in the HPC field and will be designed following the requirements of an ES. One self contained board will take care of storage, networking, memory and processing, all performed by devices soldered on board, without piggyback modules or plug-in devices or moving parts: this robustness helps greatly in system integration and certification. Computing power will reach a maximum of 100GFlops per node that will also provide easy adaptability and configurability, thanks to a high speed, high density FPGA which allows a maximum total of 700Gops. A high amount of high speed memory will be available on board, enhancing robustness, density and posing loose constraints on compactness of OS and code. The core will be based on X86 architecture, offering the compatibility with an enormous amount of code. Solid state storage will enhance performance, thanks to its lower access time and to its higher reliability (no moving parts). Networking and connections are made easy by the available interfaces: Gigabit Ethernet, Infiniband, XAUI (RapidIO). Power consumption can easily be modulated and adapted to the constraints an ES and depending on the installation site (150W-400W). This node will be provided with intrinsically dependable capabilities, an aspect very important in ES markets like military and avionics. Generally the common way to achieve a high dependability is to apply the concept of HW redundancy. The trade off of HW redundancy is that system's cost rising up drastically. A different approach is proposed in T3.4 and can be applied with the use of FPGAs that are intrinsically redundant. Runtime reconfiguration is the capability to modify or change the functionality configuration of the device during normal operation or fault, though either hardware or software changes. That capability can be specialized in different way in order to reduce component count, power consumption, reusing, fault tolerance, etc.. A new approach for FPGA runtime reconfiguration that is capable to increase the nodes dependability will be developed for this node;

- Embedded Camera Array auto-calibration and auto-configuration techniques for Panoramic Automated Site Monitoring in 3D. Coherent surveillance of complex extended sites is hindered by current image capture techniques which rely upon separate and distributed cameras for scene observation. The task of mentally registering different perspectives while assessing observed activities falls upon the already-overworked analyst. Better would be an integrated viewing system that could present a coherent continuous viewpoint for review, free of jumps and dislocations. Panning, zooming and automated tracking would enable greatly increased effectiveness in monitoring activity. a camera system will be developed to provide this all-seeing integrated view, while delivering high quality range data coupled to the video;

- Real alternatives for low power ES nodes being able to provide SPD features. The HW and SW implementation will take into account the size and power constrains of these kind of devices, while keeping as much as possible their performances and functionality.

The main outcome of task 3.2 will be prototypes of the described technologies, matching with WP2 requirements, specification and interface design.

The activities related to the design and development of the enhanced power node hardware prototype, requested by the new objectives of the pilot project, will be performed by Eurotech. If required , these activities could be carried out in ETHLab laboratories (ETHLab, Eurotech Research Center) which will be freely place at disposal for the project.

Task 3.3 Dependable self-x and cryptographic technologies (Task Leader: AS - Partners: CS, ATHENA, THYIA)

This task will provide horizontal SPD technologies that will be adopted in task 3.1 and 3.2 at different levels, depending on the complexity of the node and considering its HW/SW capabilities, its requirements and its usage. The research will rely mainly on the following technologies:

- Automatic access control, denial-of-services, self-configuration and self-recovery as mechanisms in charge of preventing non authorized/malicious people to access the physical resources of the node. The development of this technology relies also on security, privacy and dependability features at network level (see WP4), because ES nodes could be reached by the network. According to this statement, particular attention will be devoted to integration activities (see WP6) of this technology in the overall framework aiming at ensuring the highest level of QoS against possible vulnerabilities. This technology represent a key feature for empowering the performances of ESs in all the proposed scenarios, allowing to handle malicious attacks in a shared node environment where the possible attacker is an insider who already has the necessary credentials and wants to degrade service availability of part of the node network for his own purposes (for instance shared face recognition devices installed on cruise lines gates);

- Self-reconfigurability and self-adaptation of sensing and processing tasks, is proposed in order to guarantee robustness and dependability of the information collected from the ES node. It represents a key feature at SHIELD’s node layer and will also affect the performance of the overall framework, influencing SPD capabilities at network and middleware level (see WP4 and WP5). Self-reconfigurability can be used to increase the function density of a processing node, to make a node more secure against side-channel attacks through measurement of EM radiation, and to implement self-healing properties. As well, self-recovery can be implemented through reallocation of functional blocks that will replace and mark faulty resources, through device re-programming in the case of programmable devices (self-reconfigurability), or through degradation of service. Self-reconfigurability and Self-recovery will be provided to the nodes adopting field-programmable gate arrays (FPGAs), programmable processor with a reconfigurable datapath and a simple reprogrammable microcontroller. Although some of these techniques have already been published in the literature, to this date they have not been used in marketed products. Despite of this statement, SHIELD partners plan to design, develop and exploit such innovative technology in the selected application scenario both as a relevant test-field for their effectiveness and as first prototype in the perspective of a future market spreading;

- Hardware and Software crypto technologies. Particular effort will be spent on the code optimization (time and memory) and fine-tuning to improve the characteristics of the node while maintaining the high level of security of the component. Another aspect will consist also in reducing the requests of the SW resources, taking into account also the hardware constrains and sensor architecture. One of the topic that will be investigated will be the study and design of embedded operating systems and firmwares with lower resources requirements (e.g. by using a memory management better adapted to the security/integrity requirements that could be put on certain memory location without generating a too important overhead).

Choosing the right cryptographic technology or technologies to address information security for the three different ES Nodes, will be made by a combination of research and testing different approaches and technologies in order to choose the best for the specific problem.

Once the research and test phases are over, the chosen approach will be prototyped, thus allowing integration into the respective demonstration environments.

During the research phase, the requirements and system design guidelines issued in WP2 will be used to address the specific problem of choosing a framework to supply cryptographic features for the system.

First of all, it will be necessary to choose the Asymmetric Cryptographic paradigm (PGP, PKI, SPKI, etc.) to accomplish the system security requirements, based on a risk analysis of those requirements, and also on system requirements.

Several approaches will be analyzed and a cost benefit analysis will be issued.

After choosing the best paradigm to use, it will be necessary to choose the right Cryptographic Algorithm to use. In this area it will be necessary to establish a compromise between the strength of the algorithm (determined by the security risk), the computational power available to process cryptographic tasks and other security requirements.

In order to choose the best algorithms, a complementary study will be performed to test the respective algorithms on the specific hardware of each node, allowing for the presentation of a cost benefit analysis to support the decision.

After choosing the Asymmetric Cryptographic paradigm and the algorithms to use, a system framework will be defined to implement the chosen approach. In this area we will perform the necessary studies, followed by tests of available open source technologies, that could be reused to develop the demonstration system. Since specifying a commercial framework is not possible in this phase, costs are not considered.

Prototypes of such technologies will be developed, following the composability criteria of the SHIELD architecture design delivered by WP2.

Deliverables

Public

D3.2 SPD nano, micro/personal node technologies prototype report (M16)

D3.3 SPD power node technologies prototype report (M17)

D3.4 SPD self-x and cryptographic technologies prototype report (M16)

Internal

D3.1 SPD node technologies prototypes (M15)

Milestones

M4 SPD Metrics, system architecture design and preliminary SPD prototypes (M15)

M5 SPD prototypes (M16)

M6 SPD prototypes and pSHIELD Platform Integration (M17)

Work package number	**WP4**	**Start date or starting event:**		**Month 1**				
Work package title	**SPD Network**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	0	0	0	2	12	0	0	1
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	0	0	~~0~~	0	8	18	8	0
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	12	0						

Objectives

The objectives of WP4 are:

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

Description of work (WP Leader: SCOM)

In the following section the technologies examined in the pSHIELD project are described. However, since pSHIELD is a pilot project, these technologies could not be fully addressed, but they will be addressed with different effort according to the reduced budget. Moreover the participation with reduced effort (less than 2mm) for some partners has been foreseen to perform, for some technologies, only a technological scouting.

This WP will follow an approach similar to the WP3, focusing on the transmission (communication) level.

Task 4.1 Smart SPD driven transmission (Task Leader: SCOM - Partners: THYIA, UNIGE)

The design and development of the Smart Transmission Layer in SHIELD will rely on waveform-agile implementations on Software Defined Radio (SDR) platform interconnected with personal computer. Joint and cooperating implementations of security procedures over several communication standards are expected to be accomplished and improve the state-of-the-art. As well, expected benefits at this point are in flexibility to join different security procedures over a range of different communication standards, and in easy integration with hardware security components.

SDR can cooperate with an application software-implemented security, and thus cooperate with security at higher OSI levels. For instance, interoperability with hardware security components is also offering itself, namely with cryptographic key exchange/storage hardware components, pseudo-random number generators etc.

Since many Software Defined Radios are realized in conjunction with common personal computers, interconnection with common PC applications providing security/privacy tasks is possible.

In SHIELD, SDR will offer some smart communications functionalities, also at the physical OSI layer, as various spectrum spreading techniques or channel number (frequency) varying techniques.

More specifically the metrics identified in Task 2.2 will be used for the measurement of security, dependability, reliability, trust and reputation, availability, privacy, anonymity and traceability to evaluate the communication between SPD nodes on a data link and network interconnection level.

Ad-hoc algorithms will be implemented in order to enhance security, privacy and dependability features using the basic SPD modules of the SDR.

Output models, developed coherently with already available SDR modules and the related pSHIELD architecture layers, will allow demonstrating SPD capabilities of the pSHIELD network against malicious intentional attacks.

At network level the development of SHIELD SPD-based new technology can support existing wireless standards by allowing a complete interoperability and by increasing trustworthiness and improving the spectrum utilization through environment awareness, self-reasoning, self-healing and learning capabilities. For instance, risk management applications in case of fault and/or lack of reliability of communication systems can be associated with situations where a node can be used both for intelligent communications and efficient dynamic spectrum management aiming at managing human driven actions and for collection and recognition of information from underlying platform levels.

Task 4.2 Trusted and dependable Connectivity (Task Leader: MGEP - Partners: ATHENA, CS, Tecnalia, THYIA, UNIGE)

Main activities will concern 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.

SHIELD framework will take advantage of physical interoperation for providing reliable and efficient communications even in critical channel conditions by using adaptive and flexible algorithms for automatic and dynamic system parameter configuration such as adaptive modulation and coding, transmission technique, carrier frequency, etc. as well as multiple antenna techniques. Therefore, the proposed framework will make a step change in spectrum efficient radio access enabling smart usage of licensed, unlicensed or unused frequency bands to generate added value in terms of cost and energy reduction by means of a distributed approach. For instance, adaptive modulation and coding enables robust and spectral-efficient transmission over time-varying channels. Basing on channel measurements, provided by the physical layer, it is possible to dynamically adapt the modulation, coding and data rate in order to meet the required QoS level. In particular, it is necessary to continuously observe the radio channel especially if heterogeneous communication standards are employed in the considered frequency band in order to avoid harmful interference among users.

Some other activities will concern 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. For that purpose specific intrusion detection systems will be studied and designed.

Other activities will concern 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, integrity and authenticity of transmitted data, and relying on the existence of accessible key distribution centre and certification authorities.

How data reliability mechanisms (including confidentiality, integrity, and authenticity) can be shared between different wireless network technologies will be investigated. The SPD metrics developed in WP2 will be the basis for evaluations of the achieved levels of reliability.

Deliverables

Public

D4.2 SPD network technologies prototypes report (M16)

Internal

D4.1 SPD network technologies prototype (M13)

Milestones

M3 Preliminary SPD metrics and system architecture design and network prototype (M13)

M5 SPD prototypes (M16)

Work package number	**WP5**		**Start date or starting event:**		**Month 1**			
Work package title	**SPD Middleware & Overlay**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	0	0	0	4	20	7	37	1
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	0	0	~~0~~	0	0	0	11	14
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	22						

Objectives

The objectives of WP5 are:

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

Description of work (WP Leader: ED)

In the following section the technologies examined in the pSHIELD project are described. However, since pSHIELD is a pilot project, these technologies could not be fully addressed, but they will be addressed with different effort according to the reduced budget. Moreover the participation with reduced effort (less than 2mm) for some partners has been foreseen to perform, for some technologies, only a technological scouting.

Task 5.1 SPD driven Semantics (Task Leader: TRS - Partners: UNIROMA1, ED, THYIA, TRS, CWIN)

In this task semantic technologies will be developed to address the interoperability among different SPD technologies. A semantic ontology will be defined to describe the SPD modules capabilities and interfaces, to describe the metrics and the relevant information exchanged between the node, network, middleware and overlay layer.

The semantic methodologies and technologies will be developed in order to address the interoperability issues among different SPD technologies. A methodology for the ontology building process will be settled, then a suitable meta-model and an OWL-like semantic language will be identified. This framework will lay a groundwork to build, as a second step, an ontology of the SPD modules, capabilities and interfaces, that thanks to a semantic-aware model of all the exchanged information and control flows between the node, network, middleware and overlay layer, will allow an effective way to represent and reason about all the relevant entities by means of a common (shared) and consistent schema.

The outcome of this task will be a lightweight common semantic languages derived by standard ones (i.e. OWL) in order to be easily processed in the embedded system world where the processing unit are limited in power and resources. The semantic ontology will be part of the prototypes delivered by WP5.

Task 5.2 Core SPD services (Task Leader: THYIA - Partners: CS, ED, UNIROMA1)

This task will design and develop the core SPD services provides by the SHIELD middleware:

- service management functionalities such as secure service discovery and delivery, service compositions
- context awareness features to refine and extend the existing middleware implementations

The interaction between SPD-middleware and ES nodes will be bidirectional (see Figure 2.2). The SPD-middleware will use data received by ES nodes and will provide information to the upper layers of the system. In both cases information passing through the middleware should be represented in a proper way (e.g. using semantic metadata) in order to enhance security and introduce context-aware features for providing advanced service discovery and management functionalities to the applications.

A complete model will be defined for developing a context-aware security and discovery middleware, based on semantic metadata (e.g. profiles and policies), used to describe the context of an application, its relevant security requirements and the needed context-dependent adaptation strategies. A prototype of this model will be implemented to offer a wide range of mechanisms for discovering, collecting and managing relevant context information, and for securely accessing the resources. A key feature common to the developed infrastructure is the exploitation of ontology based, semantic technologies to represent context information.

Since security support in middleware architecture is still largely unexplored in both academic and industrial research activities, this task will investigate how to extend the firstly emerging models to accomplish security management solutions for middleware including context awareness features.

The design and development of the SPD Middleware core services will be accomplished according to the specifications, requirements and architectural guidelines depicted in Tasks 2.1 and 2.3. In order to build the target functionalities a modular approach will be followed by partition the features of the middleware in abstract SPD modules. Each module will be a collection of conceptually similar functions that provide services to other modules or to other layers. The SPD modules will be characterized to be dynamically composable. This task will also define and implement specific interfaces (based on the design results of task 2.3) for accessing middleware capabilities from outside systems.

Task 5.3 Policy-based management (Task Leader: ED - Partners: CS, CWIN, Tecnalia)

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

- Use of policies. Policies permit the declarative specification of security strategies separately from the implementation code of ES nodes. The use of interpreted policies allows to change the security behavior of a node without recoding or shutting down the node;
- Design and development of an authorization based PAP (Policy Administration Point) for the Policy Enforcement Point and Policy Decision Point.
- Design and development of a configuration module for lowering policies to devices level.
- Design and development of algorithms and tools to enrich the smart capabilities of the middleware and increase its autonomy;

The outcome of task 5.3 will be integrated in the WP5 prototypes.

Task 5.4 Overlay monitoring and reacting system by security agents (Task Leader: ED - Partners: ATHENA, CS, THYIA, UNIROMA1)

This task aims to design and implement an overlay layer based on a system of reacting security agents. The outcome of this task will be a software implementation of a security agent prototype ready to be integrated and interwork with the rest of SHIELD architecture.

The security agent will be designed to *interpret* and *elaborate* the SPD information generated by the SHIELD multi-layer framework. So the Security Agent produces high-level SPD information which is aggregated and eventually shared and distributed with other Security Agents acting with different scopes to the SHIELD systems. The high-level SPD information will be assessed with the metrics defined in task 2.2, in order to assess the SPD level of the single layer as well as of the overall system.

The security agent will be designed and developed to build autonomously an overlay network composed by different security agents that monitor SPD among groups of embedded system peers, networks, applications and services. Each security agent will interprets the information shared in the SPD system in order to discover imminent threats and mounting attacks. All security events of interest will be correlated with the underlying criticality rating the targeted asset. This will results in accurate prioritization and enables fast response to the threats, targeting most critical assets.

The security agent reacting system will be a combination of network scanning, passive network monitoring, and integration with existing data provided by the layers. It allows the security agent to organize the network assets into categories. This feature will permit to assign ad-hoc security policies for monitoring each application or service component.

A multi-agent approach which combines intelligent, adaptive, autonomous and cooperative capabilities of the agents will be developed. Teams of security agents will cooperate to monitor over time the SPD level on the whole service chain. Therefore, in order to guarantee security and dependability in inter-agent communication, new semantically enriched communication protocols and distributed algorithms capable of dynamically identifying potential dangerous activities, will be defined and validated. The benefits brought by semantic technologies developed in Task 5.1 will be also adopted to exploit the security agent capability and adapt security needs and associated policies to possible unforeseen situations.

The main outcome of this task will be the development of a software prototype implementing monitoring features.

Deliverables

Public

D5.3 pSHIELD semantic models report (M16)

D5.4 SPD middleware and overlay functionalities report (M16)

Internal

D5.1 pSHIELD semantic models (M15)

D5.2 SPD middleware and overlay functionalities prototype (M5)

Milestones

M4 SPD Metrics, system architecture design and preliminary SPD prototypes (M15)

Work package number	**WP6**	**Start date or starting event:**		**Month 6**				
Work package title	**Platform integration, validation & demonstration**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	9	0	29	5	9	6	13	1
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	4	20	~~6~~	4,5	0	1	25	0
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	0						

Objectives

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

Description of work (WP Leader: HAI)

Task 6.1 Multi-Technology System Integration (Task Leader: HAI - Partners: ASTS, THYIA, CS, CWIN, HAI, MAS, SCOM, ATHENA)

This task aims at integrating components and prototypes developed in WP3, WP4 and WP5 and at providing validation & verification based on the requirements and scenario specified in WP2. The integration process will follow an iterative approach.

A vertical testbed covering various layers of SHIELD will be the integration result, targeting to the demonstration of the interoperability of the various SHIELD SPD modules and addressing all SPD concerns. In particular, the testbed resulting from the integration of the implementations performed in WP3, WP4 and WP5, will be tested in the application scenario defined in Task 6.4 and validated against the SPD metrics and requirements defined in Task 2.2.

Task 6.2 Multi-Technology Validation & Verification (Task Leader: ED - Partners: SESM, ASTS, ATHENA, CS, ED,~~ISD,~~THYIA)

The activities of this task require initially an assessment of the interface conformance following a specified validation procedure. This is followed by experimenting attacks in the selected scenarios, as well as situation of communication overheads impacting on communication efficiency.

Validation of the integrated prototype features is a challenging research task due to the heterogeneous environments in which the different modules (components) have been developed. In particular, each interaction between components requires extensive validation to ensure security is not compromised. The validation methodology will include security quality modeling and security validation via software architecture evaluation. Software architecture has a great influence on the system final quality, as it can inhibit or enable product's quality attributes; so, software architecture evaluation allows early validation of quality attribute fulfillment. The validation methodology will also address embedded system families where different members of the family may require different levels of security. The trade-off analysis among security and other parameters (e.g. complexity, Quality of Service, etc.) will also be addressed.

Finally, a targeted field trial validation will be considered, since they could provide a fundamental mean for validating all the SHIELD SPD features and concepts. In particular, field trial results could be analyzed even taking into account the feedbacks received from potential end-users in real scenarios.

Task 6.3 Lifecycle SPD Support (Task Leader: ATHENA - Partners: SESM, ASTS, ATHENA, CS)

This task aims at guaranteeing the proposed architecture to be future-proof, to support the installation, download and upgrade cycle and to address the security and integrity issues involved. To address these issues, this task will start from the early system phases and related processes, as discussed for example in the ISO/IEC 12207 standard about the software life cycle processes.

Embedded systems usually lack resources for applying all the security features; therefore a compromise between security and cost must be reached. Therefore, developers should be able to choose which security features they need for each specific function in order to optimize resource consumption and protect truly important messages while not wasting resources in those that are not sensitive.

Additionally, security-aware code generators can be discussed to extend current code generation and verification tools with awareness of architectural, security, and/or co-design concepts. The end goal is to describe code generators that can guarantee given security properties.

For the development of the proposed framework, specific tools will be described to analyze the security implications of the upgrades. These tools will determine how particular vulnerabilities and/or classes of attack are covered/exposed by the application of a given software/firmware upgrade.

Task 6.4 Multi-technology Demonstration (Task Leader: ASTS - Partners: ATHENA, CS, CWIN, ETH, THYIA)

In this task a pilot demonstrator will be developed to validate the proposed architecture in and industrial relevant application scenario: m*onitoring of freight trains transporting hazardous material*

The goal of this Shield use-case is to demonstrate how information from sensors in ad-hoc environments will require actions depending on the constellations.

Thanks to an agreement made in the scope of the pSHIELD project, Telenor Objects will provide, through the Norwegian cluster, its technological knowledge/tools for the realization of the demonstrator.

Telenor Objects connects objects and devices with software applications through a new infrastructure called Object Service Enablement Functions (OSEF). Reducing complexity, development effort and maintenance costs for applications are the underlying drivers for the OSEF functions. The largest innovation potential lies in allowing sensor information to be shared in a safe manner across any application and allowing any device to connect to any application - which means that new applications can be created on the basis of installed devices.

Though the platform is generally applicable, Telenor Objects suggests using intelligent management of hazardous waste as the use-case for SHIELD. Hazardous material may consist of toxic, reactive, explosive and ignitable substances. When hazardous material is mismanaged it has the potential to pollute the environment and threaten human health.

Handling of hazardous material includes identification, labeling, packaging, storage, transportation and disposal. The envisaged use case will concentrate on the labeling, storage and transportation. Furthermore, it will include the integration of distributed smart-sensors in order to monitor car integrity and warn about possible leaking of hazardous material. As witnessed by the results of risk assessment and accidents happened in recent past, this is an important problem to be addressed in the context of critical infrastructure protection and railway security.

Among the hazardous materials carried by freight trains there are wastes from industrial and laboratory use. The cooperation partner of Telenor Objects is one of the leading European waste handlers, and has currently different systems for labelling of waste, including bar-code and RFID. Currently many of the waste handling procedures are supervised actions, where advises are given based on experienced personnel. Together with Telenor Objects the company is undergoing a chance of procedures, where most of the information is provided online and dependent on the material being handled. Examples of this advanced handling are transportation and storage issues, where an online inventory of all material is provided, including positions on the lorry, reactivity towards other waste and environmental conditions as heat or water.

The processes are highly variable, starting from the logistics of planning the material collection, transportation issues like co-location, and environmental conditions. Hazardous material handling also includes a continuous online measuring, monitoring and documentation system. In Shield focus will be on access to the services provided through the sensors. One application might be the run-time information for drivers of hazardous waste on where and how material has to be placed in order to avoid collocation of reactive components.

In this specific use case, the following requirement has to be fulfilled:

- Secure handling of the critical information of the hazardous material;
- Secure and dependable monitoring of the hazardous material.

Deliverables

Public

D6.1.1 Platform integration report (M17)

D6.2.1 Platform validation and verification (M18)

D6.3.1 Lifecycle and SPD Support Report (M17)

D6.4.1 pSHIELD demonstrator (M19)

Milestones

M6 SPD prototypes and pSHIELD Platform Integration (M17)

M7 pSHIELD Integrated platform validation and verification (M18)

M8 Final Demo (M19)

Work package number	**WP7**		**Start date or starting event:**		**Month 1**			
Work package title	**Knowledge exchange and industrial validation**							
Participant no.	1	2	3	4	5	6	7	8
Participant short name	SESM	AS	ASTS	ATHENA	CS	CWIN	ED	Tecnalia
Person-months per participant	6	0	4	1	3	2	2	1
Participant no.	9	10	~~11~~	12	14	15	20	21
Participant short name	ETH	HAI	~~ISD~~	MAS	MGEP	SCOM	THYIA	TRS
Person-months per participant	0	0	~~0~~	0,7	0,5	1	6	0
Participant no.	22	23						
Participant short name	UNIGE	UNIROMA1						
Person-months per participant	0	0						

Objectives

The objectives of WP7 are:

- Industrial Dissemination
- Industrial Exploitation of results.

The standardization and industrial dissemination and exploitation activities play an essential role, from an ARTEMIS perspective, in the validation of research results in the industrial sector. Therefore, such activities shall be considered as integral part of the project both in terms of industrial research and experimental development.

Description of work (WP Leader CWIN)

Task 7.1 Dissemination (Task Leader: SESM - Partners: ASTS, ATHENA, CS, CWIN, Tecnalia, MAS, MGEP, THYIA)

This task aims at disseminating the project results and at influencing new standards. Detailed dissemination and standardization strategies have been reported in sections 4.2 and 4.3. Dissemination activities will consist in the publication of all important results in well-known conferences and journals. The research issues of the project will be promoted through the organization of special sessions in conferences and workshops on the research topics of the project. The universities will contribute to the dissemination of knowledge by producing scientific publications, by organizing and participating to dissemination events (international conferences and workshops) and by organizing an international journal special issue on the main research SHIELD topics.

Task 7.2 Exploitation (Task Leader: CWIN - Partners: ASTS, CS, CWIN, ED, SCOM, THYIA)

The target of this task is to promote and facilitate the exploitation of the achieved results.

The exploitation is expected to be in many business segments such as Transportation, Automation and Manufacturing Industry, Health, etc.. One driving force for the exploitation will be the convincing proof-of-concept prototypes and demonstrators that will be developed in SHIELD. Another one will be the exploitation strategies that will be devised for the projects results that could be submitted for standardization.

Deliverables

Public

D7.1.1 Web Site (M9)

D7.1.2 Dissemination Report (M19)

D7.2.1 Exploitation Plan (M19)

Milestones

M1 Project collaborative working environment (M9)

3.6 - Efforts for the full duration of the project

Partic. No.	Partic. short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	Total
1	SESM	36	9	29	0	0	9	6	89
2	AS	1	0	20	0	0	0	0	21
3	ASTS	3	14	0	0	0	29	4	50
4	ATHENA	0	3	4	2	4	5	1	19
5	CS	3	3	18	12	20	9	3	68
6	CWIN	0	4	7	0	7	6	2	26
7	ED	3	8	0	0	37	13	2	63
8	Tecnalia	2	2	0	1	1	3	1	10
9	ETH	2	12	42	0	0	4	0	60
10	HAI	1	9	0	0	0	20	0	30
~~11~~	~~ISD~~	~~1~~	~~0~~	~~8~~	~~0~~	~~0~~	~~6~~	~~0~~	~~15~~
12	MAS	1	0	2,8	0	0	4,5	0,7	9
14	MGEP	0,5	0	0	8	0	0	0,5	9
15	SCOM	4	1	0	18	0	1	1	25
20	THYIA	2	11	21	8	11	25	6	84
21	TRS	1	0	0	0	14	0	0	15
22	UNIGE	0	0	0	12	0	0	0	12
23	UNIROMA1	2	0	0	0	22	0	0	24
Total		62,5	76	151,8	61	116	134,5	27,2	629

3.7 - List of milestones and planning of reviews

Milestones are control points where decisions are needed with regard to the next stage of the project. For example, a milestone may occur when a major result has been achieved, if its successful attainment is a requirement for the next phase of work. Another example would be a point when the consortium must decide which of several technologies to adopt for further development.

Milestone number	Milestone name	Work package(s) involved	Expected date [1]	Means of verification[2]
M1	**Project collaborative working environment**	WP1, WP7	9	D1.1.1, D7.1.1
M2	**System requirements and specification**	WP2	10	D2.1.1
M3	**Preliminary SPD metrics and system architecture design and network prototype**	WP2, WP4	13	D2.2.1, D2.3.1, D4.1
M4	**SPD Metrics, system architecture design and preliminary SPD prototypes**	WP2, WP3, WP5	15	D2.2.2, D2.3.2, D3.1, D5.1, D5.2
M5	**SPD prototypes**	WP3, WP4	16	D3.1, D3.4, D4.2
M6	**SPD prototypes and pSHIELD Platform Integration**	WP3, WP6	17	D3.3, D6.1.1, D6.3.1
M7	**pSHIELD Integrated platform validation and verification**	WP6	18	D6.2.1
M8	**Final demo**	WP6	19	D6.4.1

[1] Measured in months from the project start date (month 1).

[2] Show how you will confirm that the milestone has been attained. Refer to indicators if appropriate. For example: a laboratory prototype completed and running flawlessly; software released and validated by a user group; field survey complete and data quality validated.

3.8 - Known risks and contingency plan

The known risks in SHIELD are related to the dimension of the project and the challenging objectives it want to achieve. These risks relate to the following main areas:

1. Research and technological risks;
2. Economic and exploitation risks;
3. Organizational risks;
4. Methodological risks;
5. Investment related risks.

These risks are described below, and the consequences and contingency actions are explained.

3.8.1.1 Research and technological risks

Due to the high number of SPD technologies that will be developed and integrated in the SHIELD system, for the sake of simplicity, instead of listing all the risks associated to each technology, two macro-risks have been identified.

Risk 1. A technology development at node, network or middleware layer delays

Probability: [Medium]. As described in section 2.2, SHIELD aims to enhance more than 20 SPD technologies at all levels of an ES. It is possible that one or more of challenging technologies can require more effort to be enhanced to match the specifications. However as shown in section 5.3 for each technology at least two partners are involved in its development and approx the 2/3 of the consortium is always involved in R&D activities. So in the case one of the technologies is delaying the other partners can provide technical assistance or some more effort.

Gravity: [Medium/High]. The delay of one or more technologies can cause a delay in the delivery of a prototype and thus the entire project can be delayed.

Contingency plan. If a critical delay occurs in one or more of the SPD technologies, two main countermeasures can be taken. First of all the technology can be used at the state of the art, without enhancement, and adapted to be composable with the rest of the architecture. Secondly, taking advantage from the composability feature of the SHIELD system, it can be replaced by other available SPD solutions (even if with less performance).

Risk 2. The composability concept fails

Probability: [Low/Medium]. As described in section 2.1, the leading SHIELD concept is to demonstrate the composability of heterogeneous SPD technologies. It can occur the case that this innovative concept once deployed produced less benefit than the effort it requires to operate, even if the current research literature seems to demonstrate the contrary[1]. Moreover the SHIELD workplan has been organized to check continuously (through integration, validation and verification processes) the achievements of the project milestones and results.

Gravity: [Medium]. If the static and dynamic composability concept fails, the added value brought by the project is limited to the evolution of the single SPD technologies in ESs and to the simplification of (re-)certification processes.

[1] "*A top-down, multi-abstraction layer approach for embedded security design reduces the risk of security flaws, letting designers maximize security while limiting area, energy, and computation costs.*". Source: D. D. Hwang, P. Schaumont, K. Tiri and I. Verbauwhede, "Securing Embedded Systems", published by the IEEE computer society, IEEE security & privacy, 2006.

Contingency plan. To mitigate the effects of this risk, as soon as one of the checks fails (during the integration, the validation or the verification processes) less strict requirements and specifications and a more efficient system design can be studied, to improve the SHIELD performances with the minimum effort.

3.8.1.2 Standardization and exploitation risks

Risk 3. Products appear on the market before the project work is completed

Probability: Low. The key players in this market are embedded system manufacturers, integrators and their suppliers, of which several major ones are in the consortium. Whilst partners are aware of ongoing work on small-scale single-technology, proprietary solutions, they are aware that especially from 2001 the SPD topics have become a worldwide priority. However, they have no knowledge of a similar activity to SHIELD that takes such holistic approach to SPD, where a composable convergent over-layer can guarantee efficiency, reliability, adaptability, resiliency over different networked ES technologies.

Gravity: Medium/High. If a product will appear on the market before the project work is completed then this would be a serious situation that might impact to the project.

Contingency plan. If a seemingly competing product came to the market during the project's lifetime, it would have to be examined carefully. It is highly unlikely that all the types of technological advances proposed by SHIELD with respect to the standard integrated SPD solution would be covered, or that all the features and functions of SHIELD could be included in any product that could emerge within the next couple of years. Rather than closing the project, a realistic contingency plan would be to work together with the manufacturer to enhance their product with SHIELD aspects that they do not have.

Risk 4. Standards emerge that prevent the deployment of the results, or lead towards a different solution to that being developed in the project

Probability: Low. The key players in standardization groups are present in the SHIELD consortium. They are aware of the work in relevant standards organizations (refer to section 4.3).

Gravity: High. If standards did emerge that prevented the deployment of the results, or led towards a different solution to that being developed in the project then this would be a serious situation that might impact heavily to the project.

Contingency plan. If a standard emerged to handle ES SPD in all layers in a different manner, it might still be feasible to adapt the SHIELD infrastructure to the new standard. The SHIELD components are very modular and composable, and the necessary adaptations may be largely a case of modifying the external interfaces.

3.8.1.3 Organizational risks

Risk 5. Withdrawal of a key partner

Probability: High. In a project with 32 partners lasting 3 years, the chances are high that at least one partner will have to leave the project due to an event such as major internal re-organization or takeover. Alternatively, a partner may find itself unable to complete its allocated responsibilities, due to the transfer of key personnel within, or outside, the company, financial problems, etc. In both cases it will be necessary to find a replacement partner.
Key partners are considered those with management roles (Coordinator, WP leaders), and those that provide node or network technologies not provided by other partner.

Gravity: Medium. Thanks to the good balance of the project consortium, a complete collapse of the project is highly unlikely, even if a key partner withdraws. Monitoring procedures will be put in place to detect early any under-achieving partner and the project will encourage open and honest reporting of problems, so that solutions can be found as soon as possible.

Contingency plan. The Consortium Agreement regulates the penalties that such a defaulting partner would have to pay, and this money can then be used to enable the work to be done by another partner. The consortium comprises major companies, who have expertise in several areas relevant to SHIELD, and a transfer of resources to an existing partner would be the first choice for a replacement. Given the overwhelming interest expressed to be part of this consortium, if no replacement could be found internally, it is expected to be simple to find an external replacement organization to take over the work at relatively short notice.

Risk 6 Since WP6 builds on all other work packages, the main risk identified is the delaying of components delivery.

Probability: Medium. Because of the number and variety of components to be integrated onto the platform, there is a chance of not being able to produce working demonstrations of all expected features coping with the challenging scenarios addressed in WP7. SHIELD has continuous verification mechanism that helps to identify potential delays and to react in time.

Gravity: Medium.

Contingency plan. Measures can be taken to minimize the risks if there's some foreseen delay; for example some components can be replaced with older versions or components already developed in other projects, so that a single delay should not compromise the final demonstration.

3.8.1.4 Methodological risks

These relate primarily to the need to merge research results from different organizations, with a potentially large degree of difference in methods, terminology, and outputs.

Risk 7 The consortium fails to deliver proper models and tools

Probability: Medium. The complexity and innovation of SHIELD conceptual framework and related tools can lead to unforeseen design deadlocks.

Gravity: Medium. This methodological risk causes problems to system development.

Contingency plan. Contingency plans of the consortium foresee that in such a case the parameterization and configuration of the field test will be solely based on the extensive experience of the project partners in development of SPD systems and technologies. Drawbacks of this measure are that the evaluation of progress beyond the state-of-the-art cannot be executed at the quality intended and in a reproducible manner.

Risk 8 The consortium fails to deliver prototypes according to the specifications and requirements

Probability: Medium. To enable composability of SPD functionalities, SHIELD requirements and specifications should be applied strictly. It is possible that one or more prototypes fails to respect the specifications is medium.

Gravity: Medium. This methodological risk causes problems to the platform integration and the field tests.

Contingency plan. In this situation, a minimal combination of industrial partner existing products would provide a substitution for the prototype. Yet the results of such a substitution would not be able to provide all the functionalities of the project prototype. Therefore, the gravity of this risk is rated medium.

3.8.1.5 Investment related risks

Risk 9 Low or negative investment return

Probability: Medium. This is a sensitive issue for all participants since all investments need to be related to a return plan. Participants believe that potential benefits identified during the project definition phase are sufficient to guarantee valuable returns. However, the outcome of the project may be subject to re-definitions or deviations thus altering the initial expectations of the respective partners with respect to resources necessary to accomplish a certain task and wide-scale applicability of results.

Gravity: High.

Contingency plan. To enhance the possibility that investments bring a positive outcome to the project, acceptance preparation activities will be conducted starting from the beginning of the project.

Risk Description	Probability	Impact	Contingency Plan
Technology development delay	Medium - Partner experience and project monitoring	Prototype delivery delay	Adapt state of the art technologies
Composability fails	Low/Medium – continuous project monitoring	Project results less effective than expectation	Review the system specifications, more efficient design
Product appears on the market	Low – the European SPD industry is in the project	SHIELD impact will be lower than expectation	Enhance the state of the art product to come with newer one
Conflicting standards	Low – the partners are involved in the major standardization groups	SHIELD impact on the standards would be very low	Adapt the SHIELD architecture to that standard
Partner withdrawal	Medium – project has 31 partners, but high degree of complementarily	Project might suffer small delay or under-performing results	The resources are re-allocated to commit other partners
Component delivery delay	Medium – WP6 depends on WP3, WP4 and WP5	Integration phase delays	Replace the missing components with older version
Model or tool delivery fails	Medium – WP3-WP6 depends on the result of WP2	Development phase delays	Rely to the partners experience in developing SPD systems
Prototype fails to be delivered	Medium – WP3-WP5 are delivering some SPD prototypes	The composability validation can fail	Reduce the composable SPD functionalities to the minimum set
Low or Negative investment return	Medium – project benefits and partner marketing experience are indisputable . But runtime project redefinition can alter the initial expectations	Low or negative outcome can reduce the exploitation of the project results	The acceptance preparation activities will be conducted starting from the beginning of the project.

Table 3.1 - Risk assumptions and contingency plans

Section 4 - Market innovation and market impact

pSHIELD has been conceived as first phase 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. These market innovations and impacts are reported below.

4.1 - Impact

The **current technological situation** for the ES solutions in the area of security, privacy and dependability are ad-hoc designed, implemented and deployed for each specific system pursuing sub-optimized performances and incompatibility at an higher costs while the growing number and quality of treats are emphasizing 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 proposed technical solutions.

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

By proposing to realize embedded SPD via standardized design methods mainly based on a *frameworks of composable technologies* to be settled on the specific industrial solution, a *set of on new SPD metrics* allowing fast, standard validations and certification as well as *methods and mechanism to easily design and keep SPD level compliant for all the system's lifetime*, the SHIELD project aims to **drastically improve SPD quality of ES** addressing the above mentioned industrial requirements.

Due to heterogeneity and wideness of the overall embedded systems market is a very hard task to express the **market dimension** but it is easy to imagine how relevant and huge the market of SPD ES could be: following in this chapter, some examples, mainly related to the four application scenarios proposed in SHIELD, will be highlighted in order to show the overall market potential of the SHIELD solutions and to figure out the **expected impacts** in the pilot scenarios.

To obtain these valuable goals the project will completely fit in ARTEMISIA Subprogram Six as well as in the overall ARTEMISIA Target, as explained in the following subparagraphs.

4.1.1 - Contribution to the expected impacts listed in the work programme under the relevant sub-programme

SHIELD will contribute to reach the target of the Sub programme 6. The relevance to such Sub-Programme has been already described in section 1. Following it is presented how SHIELD will effectively contribute to reach the main impacts expected by such workprogramme (as indicated in the official Annual Work Programme 2009):

1) ***"Enhancing security, privacy and dependability to increase people's confidence in applications, systems, devices and infrastructures"***

Security, privacy and integrity have been the subject of intensive ICT research in the areas of general purpose computing, networking and cryptography. However, in actual embedded systems, SPD solutions are extremely tailored on the specific system features. The European

Commission (EC) has been addressing the problems of SPD already for IST in the FP6[1] but that still those efforts did not succeed to arrive in embedded systems (actually the word embedded does not appear in the whole report...) and that's why ARTEMIS addresses the topic and why SHIELD is so necessary. Moreover, the growing number of breaches[2,3,4,5] in information security has created compelling challenges towards secure electronic systems that will be emphasized by the augmented complexity of the future ES. The impossibility to use well defined metrics and standardized parameters for SPD does not allow the provision of a quick and reliable evaluation of the effectiveness guaranteed by the ad-hoc solution nor a precise rating between alternative solutions to the same SPD problem.

SHIELD aims to enhance security, privacy and dependability, thus increasing people's confidence in applications, systems, devices and infrastructures that were considered vulnerable or untrustworthy in the past. The feeling and knowledge of complete protection from faults, frauds, break, will reduce the fear or reluctance in using new features or services, enabling industrial actors and service providers to offer them with minimal additional cost to the customer.

The weakness in SPD and their perception from citizens, currently avoid the possibility to use advanced technological systems in applications strongly sensible to privacy issues. In those contests, security and dependability are fundamental properties considered mandatory, not just a strategic advantage, but an enabler of the application. The pervasiveness, the level of ubiquity and the fusion with the environment, with personal space and every-day life, expose pervasive systems to several SPD issues that strongly require that future systems must be intrinsically secure. SHIELD will study these issues and will define suitable solutions to satisfy SPD requirements of future markets and increase people's confidence and acceptance of pervasive systems. The impact will be guaranteed by SHIELD approach that will ensure SPD capabilities in all the layers of a pervasive system, starting from the device level to the application layer.

The "feeling and knowledge of complete protection from crime and violent "supporter riots", as foreseen in the ARTEMISIA AWP for the subprogram six, could not be achieved without addressing SPD – like SHIELD intend to do – with an holistic approach covering systems and their lifecycle process (design, development, testing, deployment, maintenance, etc.) at the same time. Moreover if we want to increase confidence, we will have to connect this with a strong dissemination strategy as detailed in next section 4.2.

Reaching the above target will also contribute to achieve the second relevant impact listed in the Workprogramme:

2) *Enabling industrial actors and service providers to offer new features or services with minimal additional cost to the customer.*

SHIELD will contribute to reaching such impact also providing industrial actors with a reference framework for developing "SPD compliant" applications: a must for the implementation of future SPD features in the Embedded System area, will be represented by

[1] see ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402464encfull.pdf

[2] Oyster card crack - http://www.v3.co.uk/vnunet/news/2219828/london-oyster-cracked, the original presentations at http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html, while a more scientific: http://eprint.iacr.org/2008/166

[3] keeloq crack - http://www.wired.com/threatlevel/2007/08/researchers-cra/
or http://hackedgadgets.com/2007/09/08/keeloq-remote-vehicle-entry-system-cracked/

[4] Dutch passport readout - http://www.rfid-SHIELD.com/newsItem.php?id=0000000018&p=11. also those things make people unsecure even if there was no cryptography "broken" only the sequential numbering scheme exploited.

[5] iPhone SMS bug
http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html

the availability of a common approach to SPD embedded features based on a standardized way to integrate and make interoperable different and enhanced SPD technologies. This new approach will tackle all the development process of new ES, from the design up to the certification phase, in order to produce a tangible reduction in the development costs as well as a faster time-to-market deployment of commercial ES products. Furthermore the increased security leads to increased trustworthiness and better protection of company interests on the future user side, thereby protecting the vital interests of the European industry against misuse, fraud and theft of products as well as the vital interests of the customers regarding privacy of data and service quality. This aspect will have, as consequences, more secure and dependable products offered in the final market at a minimal additional cost. Another example will be Selex Communication (SCOM). Taking advantage from SHIELD framework, the TETRA[1] technology developed by SCOM could make a step over in terms of intrinsic security according to a modular and compliant development strategy where integration and interoperability with other SHIELD technologies will be addressed. Moreover, such an approach will allow SHIELD-oriented TETRA technology to broaden market perspectives and applications towards the development of innovative, secure, dependable and privacy-oriented transmission/communication modules.

The innovative SHIELD approach specifically target the main outcomes expected by the Sub priority 6, namely:

3) ***Definition of a common conceptual framework to address the requirements for security, privacy and dependability, with a particular focus on compositional design and development. Research should take into account the interplay between system properties such as safety, reliability, availability, maintainability, security, and survivability, and should work with certification and qualification authorities to establish new approaches to certification and qualification required to accommodate the new technology.***

As previously asserted the researches in SHIELD will concentrate mainly in achieving a common framework for SPD accounting new composability mechanisms. In this respect SHIELD fully address these topics in WP2 (Task 2.1 and Task 2.3) where the requirements, specification and design of SHIELD conceptual framework is delivered.

The Liaison Task foreseen in WP1 will exactly take in account development in other ARTEMISIA and FP7 area relevant to safety, seamless connectivity and sustainability of future ES, while the methods and tools developed in the project in order to support all the lifecycle quality of SPD keep in account the maintainability of the new systems both from the effectiveness of their performances and from the aspect of their total cost of ownership (TCO). It is very important for embedded system products to be based on platforms that can be evolvable throughout their whole life cycle. The SHIELD project will contribute to the development of robust and secure solutions for evolvable embedded platforms, allowing easy support and maintenance throughout their lifecycle.

Moreover Task 2.2 aims to define common SPD metrics in order to facilitate the certification and qualification procedures while the involvement of the partners with certification authorities and the intent to obtained standardized procedures and methods, in particular for certification purposes, will guarantee the commitment with qualification bodies. For instance, techniques and methods developed by the SHIELD consortium can be used in the Common Criteria (CC, ISO/IES 15408) evaluation and certification process (CEM, ISO/IES 18045). SHIELD consortium will, furthermore, provide contributions from the project results to (1)

[1] For more details, see http://www.tetraworldcongress.com/profiles.cfm?logo=188

XML and WS-based security standards from W3C and OASIS (e.g. WS-Security and XML-Security) and (2) to the standards of TCG – Trusted Computing Group.

Additionally the valuable SHIELD results will be presented to the most relevant national certification authorities. For example:

- Italy: ED has strict contacts with the Organismo di Certificazione della Sicurezza Informatica (OCSI - http://www.ocsi.isticom.it/);
- Greece: HAI is in contact with the National Intelligence Service (EYP - http://www.nis.gr/);
- Spain: AS has contacts with the Spanish Association for Standardisation and Certification (AENOR - http://www.aenor.es/) related to the ISO/IEC 27001;

4) Instantiation of this framework with architectures, components, methods, interfaces and communications, tools and tool chains, to enable the design, development, analysis, validation, and deployment, as well as certification (or qualification).

SHIELD realizes an instantiation of the framework with components, methods, algorithms, procedures and interfaces in the following work packages:

- WP3 – SPD technologies at node level;
- WP4 – SPD technologies at network level;
- WP5 – SPD technologies at middleware and overlay level.

Furthermore WP6 (Task 6.3 – lifecycle SPD support) develops proper tools to manage the whole SPD lifecycle (design, development, analysis, validation and deployment) based on the metrics defined by WP2 (Task 2.2 – multi-technology SPD metrics).

5) Test beds and field trial set-ups, including prototypes, in order to prove the advanced security, privacy and dependability concepts

Task 6.4 (application) set-up a pilot demonstrator integrating the technologies prototypes developed by WP3, WP4 and WP5.

WP6 validates and verify the advanced SPD concepts thanks to the SPD metrics defined in WP2 and to the SPD lifecycle tools developed by Task 6.3.

4.1.2 - Contribution to the general ARTEMIS targets

SHIELD will contribute in achieving the general ARTEMIS main targets, in particular:

ARTEMIS Target #1: *Reduce the cost of the system design from 2005 levels by 15% by 2013.*

All the SHIELD configurations will be based on secure and manageable/self-manageable architecture foundation. Combining design tools for security with other COTS tools will result in tool-set for creation of application code, capable to build security, privacy and dependability into embedded systems. This new approach could have great impact in the engineering process of the new embedded systems.

The possible application of the new SHIELD based architecture in embedded systems can offer innovative solutions to ES manufacturers for protecting their equipment at the node level. This should motivate further development of safe embedded computer distributed systems. For instance, the proposed secure sensor network node is a basic element for implementation of networks for distributed data collection and processing: such sensor networks are substantial for data collection in power management and environmental control systems and the possibility to implement them using SHIELD framework will greatly contribute to their development and deployment.

ARTEMIS Target #2: *Achieve 15% reduction in development cycles - especially in sectors requiring qualification or certification - by 2013*

As previously asserted, the availability of a common framework easily arranged and configured to support a new set of SPD features using the composability mechanisms available in SHIELD both statically (at design time) and dynamically (at run time) will greatly contribute to easier the development of new SPD solutions when using as base another SHIELD-compliant solution already developed and validated. This approach will reduce in sensible way the time-to market of new products and systems solutions, thus reducing the development costs and making easier all the development process.

As a consequence of the holistic approach but, even more, as fruit of the conceptual targets on which SHIELD is based, including certificability, a qualified and easier SPD-certification process and some relevant tools to achieve it (metrics *in primis*) are expected to be reached as one of the major project goal. A valuable part of the development for SPD compliant ES is constituted by certification costs, time and complexity. Tackle appropriately with such development aspects will contribute to this important ARTEMIS target.

ARTEMIS Target #3: *manage a complexity increase of 25% with 10% effort reduction by 2013*

The future ES will be requested to properly work in a higher complex configuration, by building dynamically communications links and cooperative actions in scenarios moving from managed and trusted scenarios to completely unmanaged and un-trusted ones. The objective of SHIELD is to allow that this happen in an easier way for the designer by continuing to provide SPD features both in managed and unmanaged situation as well as in trusted and untrusted situations. A key role to obtain this results will be performed by the composability of SPD technologies which will be settled up, via the logical composability-mechanisms performed in the framework, to behave in a different way in static and in dynamic conditions.

ARTEMIS Target #4: *reduce the effort and time required for re-validation and recertification after change by 15% by 2013.*

The possibility to guarantee required SPD level by using integrated metrics will enable, using the SHIELD complaint tool-set, to decrease development and verification time and will contribute to reduce the certification process expenses. Build-in protocol verification and configuration mechanisms in the integrated tool set will provide the possibility to know ahead of time that the embedded system under development will work as desired when deployed.

SHIELD project will contribute to provide early validation methodology focusing on SPD aspects and taking into account the variability of embedded system families addressing important topics of the Artemis Strategic Research Agenda inside the ‘Design Methods and Tools’ area of research:

- methods and tools for simulation,
- automatic validation and testing,
- verification and validation methods and tools for developing product lines of embedded systems.

Moreover, the provision of early validation techniques adapted to SPD will further contribute to increase quality of final products and decrease time-to-market and costs.

The project is aimed at pursue Formal Security Requirements Specifications: developers will be able to map SHIELD SPD requirements to CC security functional and assurance requirements, while evaluators will be able to use checklists issued by SHIELD to verify security claims, and the automated tools developed by the SHIELD consortium will produce the necessary evidence for these claims. In this respect SHIELD focuses on one of the most challenging problem in embedded software development: the elimination of programming bugs and originated vulnerabilities that are an important subset of the otherwise much more complex Common Criteria.

ARTEMIS Target #5: *achieve cross-sectoral reusability of Embedded Systems devices developed using the ARTEMIS JU results (for example, interoperable hardware and software components for automotive, aerospace and manufacturing …).*

SHIELD aims at the development of an architectural framework supporting modularity offline - at design time - as well as online or dynamical reconfiguration under detection of different intrusions. The selected approach should ensure reusability of this architecture and related tools for a variety of applications, requiring different level of SPD. Each applications could stress particular aspect of SPD by using the SHIELD framework specialized with opportune SHIELD compliant SPD technologies. This approach will allow the different industries to stress particular cost-benefit aspects by starting from the same platform. For instance, if aerospace industry will take the advantage of highly dependable and certified architecture configurations, the other industries might trade that dependability for power-efficiency or another important cost.

SHIELD will moreover contribute in the development of seamless mobile environments at the architectural level by supporting entities "on the move" to be able to maintain a disruption-free connection by means of secure and dependable embedded systems communications.

4.1.3 - Contribution to industrial competitiveness and sustainability

SHIELD will contribute to industrial competitiveness at two main levels:

a) Contributing to the growth of the overall ES market in Europe
b) Contributing to the partners specific competitiveness

4.1.3.1 Contributing to the growth of the ES market in Europe

The embedded system market requires a built-in approach where SPD functionalities are natively addressed from the design through the entire system life-cycle in contrast with an SPD add-on approach today in use. In particular the industry needs an approach to SPD which will provide key improvement, such as:

- Faster design and flexible, standardized development of SPD solutions independent from possible increase of system complexity;
- Flexible way to reuse tested solutions already validated in other systems and/or applications;
- Fixed method and reference parameter to evaluate the level of SPD achieved at each stage of the development process;
- Standardised and easy certification procedures, reusable by certification bodies in order to assess the compliancy of different ES under certification.

Embedded systems in the future will be increasingly used to capture, store, manipulate, and access data of sensitive nature in more complex arrangement, and will be entrusted with more critical roles. This perspective raise several unique and challenging SPD issues to be explored highlighting the composable and modular aspects of the solution.

SHIELD aims to be a reference model for all the security, privacy and dependability aspects involving embedded networked system. In fact the provided architecture will pursue the design and development of a multi-layer/multi-technology framework able to guarantee the composability of SPD functionalities at all levels: ES nodes and networks layers, middleware-layer, service and application layers.

In order to estimate how the proposed advanced approach could impact on the ES production, starting from some relevant market researches (for reference see the note below in this page[1,2,3,4]) the SHIELD consortium has identified three impacts-parameters (grade of reusability, development cost reduction and time-to-market reduction) and promoted an internal survey to foreseen how they will be influenced by the projects result. The survey assessment could be presented in synthesis as follows: considering the advantages in design process originated by the reusing of the common functionalities among ES parts and taking in account similar experiences in software engineering[4], we can estimate a time-to-market reduction up to 40% adopting the SHIELD framework compared with the use of traditional methods, tools and supports to implement the same SPD solution. We can also estimate an improvement of about 35% in reusability factor in SDP systems adopting the SHIELD framework related to traditional approaches. The project, in fact, will propose a common SPD conceptual framework that will impact design methodologies for services involving technologies providing advanced SPD features. The adoption of SHIELD methods gives advantages also in the deployment of such technologies on multiple applications solutions. The project aims at reduce up to 25% the design cost for each new ES maintaining at the same time advanced state of the art SPD quality.

The overall impacts expected through SHIELD, in fact, are the following:

- The project with its research and industrial contributions in the field of SPD aims at ***leveraging the design/development*** of innovative application scenarios that require effective SPD solutions at all layers, such as pervasive e-health, mobile enterprise, homeland security or video-surveillance.
- SHIELD will introduce the concept of ***embedded SPD*** as a characterization of ES resulting from the aggregation of features addressing complex requirements for embedded SPD systems in various fields such as railway, health, cruise liners and industrial control sensors (flowmeters); such concept will support the evolution of ES with an impact similar to the one that the evolution of embedded systems itself had on the design and usage of Real Time Operating Systems.
- The current implementation of SPD in ES is obtained in hardware by using heterogeneous Systems on Chip, Networks on Chip and FPGAs, and in software by multi-site and multi vendor pieces of software. The system resources (often restricted in ES) are shared among those elements and even if the single components can have a predictable behaviour their interaction can introduce unpredictability due the complexity of the integrated system.

[1] “Semiconductor Trends and Opportunities for Europe”, March 2009.
http://www.semi.org/cms/groups/public/documents/web_content/ctr_029000.pdf

[2] “*ESIA 2008 Competitiveness report*”, EECA, 2008.
http://www.eeca.eu/data/File/ESIA_Broch_CompReport_Total.pdf

[3] "*Study of Worldwide Trends and R&D Programmes in Embedded Systems in View of Maximising the Impact of a Technology Platform in the Area*", study by FAST & tech. University Munich for the EC. November 2005.
ftp://ftp.cordis.europa.eu/pub/ist/docs/embedded/final-study-181105_en.pdf

[4] From the META Group series: IT Performance Engineering & Measurement Strategies: "Our research shows reused code averages 25% of the defects found in new code, and reusable components enable the final product to be delivered 40% faster". Source, META Group - Reuse Productivity by Donn Di Nunno, September 2000.

To deal with this problem the project will offer a set of already collaborating and high-performing SPD technologies that will be highly interoperable by adopting new approaches to system composition for both hardware and software elements.

In this way, the project will contribute to ***decrease unpredictability*** for single or multi-technology trusted platforms and thus is expected a strong usage of SHIELD approach in all business segments where embedded secure devices are used, e.g., semiconductor, transportation, health, telecom, consumer electronics, industry, etc

All the above mentioned impacts will have effect on a huge market cause they will contribute on growing sectors of the market as well as on new market niches promoted by the cost-effective availability of SHIELD products itself. Some examples of those growing and new market will be defined in the following while the expected market improvement for them will be highlighted in the next paragraph.

Since the overall embedded systems market is a very heterogeneous we will hereafter provide some examples, especially in connection to the application scenarios chosen by SHIELD to validate the project results, could be given in order to show the overall market potential of the SHIELD solutions after implementation in the pilot scenarios:

pSHIELD realizes only a little impact in Railway scenario while some others industrial relevant scenarios will be addressed by the fully operational SHIELD framework.

Example 1 –The Railway Scenario

The total annual world market for the rail supply industry in 2007 is estimated at more than EUR 120 billion , with an expected annual growth of between 2.0 % and 2.5 % over the next nine years. In 2016, the total world market will have reached a volume of EUR 154 billion.

The growth in 2006 and 2007 has been very high. The world market volume increased by approximately EUR 19 billion, i. e. with a nominal growth rate of 9 % and a real growth rate of 6 % p.a.

In particular the security railway segment is a rapidly increasing quote as security demand has become a mandatory requirement in any new tender. Referring to SHIELD objectives and scope of work, both vital and no-vital railway systems must fulfill security requirements, that are more and more strict. As a consequence rail security market that in 2008 has been over 500M€ is expected to almost double in 2016.

Example 2 –The Healthcare Scenario

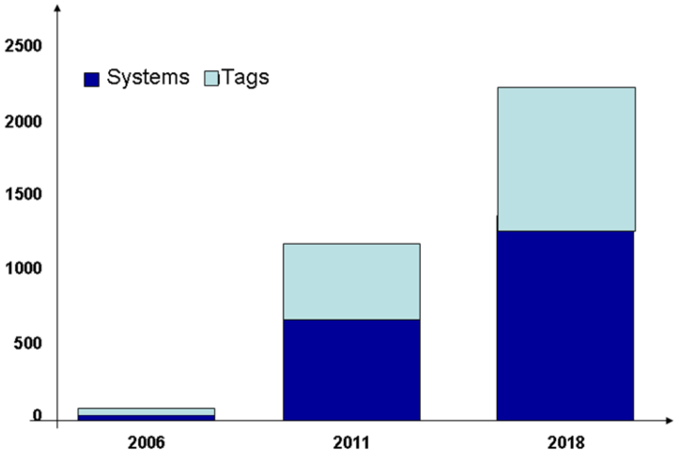


Figure 4.1 – RFID systems and RFID tags markets (source: Market Analysts Supply, 2009)

The market for RFID tags and RFID systems in healthcare will rise rapidly from $90 million in 2006 to $2.1 billion in 2016. This growth is related to real time location systems and to tagging of drugs. Trade with counterfeiting and piracy of products evolves constantly secure RFID tags offer additional possibilities to solve this problem. The novel approach for authentication allows additional mobile and privacy scenarios those opening new opportunities.

Example 3 – Access control market, related to the maritime/cruising scenario

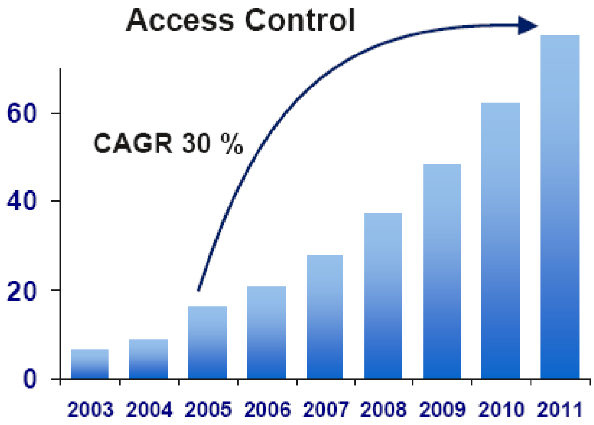


Figure 4.2 - Access Control Chipcard market (source: Frost & Sullivan, 2007)

From the semiconductor industry's point of view the access control market was reported to show a compound annual growth rate (CAGR) of 30% from 2005 to 2011. Of course the global financial crisis also stroke this market, but after recovering from the crisis this market is expected to behave similar as before. In addition the novel approach to be implemented in the SHIELD project, based on asymmetric cryptography for authentication shall even strengthen the market and open new opportunities, as explained in the scenario description.

Example 4 –The Flowmeter Scenario

This industrial sector could be considered have no great possibility to grow if addressed with traditional products:

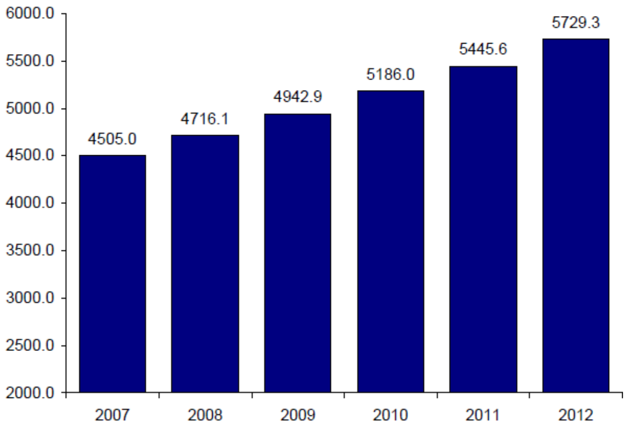


Figure 4.3 – Total Shipment of All Flowmeter worldwide (Millions of dollars). Compound Annual Growth Rate (CGAR) = 4,9%

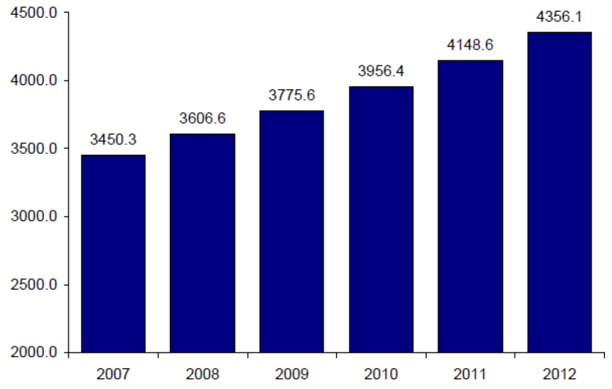


Figure 4.4 - Total Shipment of All Flowmeter worldwide (Thousands of Units). CGAR = 4,8%.

As we can see, in fact, the Compound Annual Growth Rate (CGAR) is 4,9 (4,8%) for shipments of all flowmeters worldwide from 2007 to 2012. The CAGR is almost the same in spite of global financial crisis. It means that the market of flowmeters is very steady.

4.1.3.2 Contributing to the partners specific competitiveness

The specific exploitation plan of partners is presented in section 4.2. Following, an immediate look on the potentialities (in terms of partners' competitiveness) could be obtained by figuring the overall cost reduction or the improvement in the market share in developing new solution, SHIELD based, in the pilot application scenarios:

Railway market impact - reduction of costs
As mentioned in the exploitation plan, Ansaldo STS aims at exploiting SHIELD results in its wide worldwide market sized 1 Billion Euro last year. Security system demand is more and more increasing every year and responding to such a demand is often mandatory to acquire a complete integrated system, especially in the metro sector. Results of SHIELD should increase the Ansaldo STS competitiveness thanks to the following expected impacts:

- at least 20% cost reduction of security system development;
- at least 20% time-to-market reduction for security system;
- Strong increasing of security requirements fulfilment;
- Notable increasing of ability to provide complete/integrated railway systems thanks to new secure system architectures.

The predicted amount of rail security sales for Ansaldo STS is about 25M€ per year. Since rail security is a recent business area for Ansaldo STS, this amount has been evaluated in rather conservative assumptions; in fact, the rail market share is much higher and there are not so many competitors, especially in rail security. Of this value, about 2,5M€ (one tenth) will be development costs, since Ansaldo STS mostly integrates devices supplied externally.

The investment in SHIELD will be about 1M€, with an expected gain in cost reduction of about the 20%, that is 500K€ per year (expected to increase after 2009 due to the market growth). Therefore, the investment is expected to be repaid between the 2nd and the 3rd year after the end of the SHIELD project.

The analysis reported above does not account for other factors which could positively affect the estimations, including the competitive advantage due to the higher system dependability and the lower time to market of novel solutions, as well as the suitability of SHIELD to other types of ES developed by Ansaldo STS.

4.1.4 - Support to the emergence of new markets and applications

European markets trends represent valid indicators in order to understand the latent power of SHIELD innovative approach to the design of SPD-based ESs. European industrial leaders in the field of ESs, which are represented in large part within the SHIELD consortium, will assure a proper development and exploitation of SHIELD platform aiming at both increasing the level of high tech products exports (hopefully over 20% as share of total manufacturing exports) and leading the R&D activities in ESs field towards the challenge of doubling public and private investments in the next 10 years.

The horizontal presence of SPD at all levels is expected to foster the access to huge markets, where large scale applications will become a concrete possibility. From the industrial perspective, the main assumption that drives SHIELD activities is that intelligent functions embedded in components and devices will be the key factor in empowering next generation industrial processes and markets in Europe. As a consequence, the design of an innovative SPD-based framework where new functionalities and improved quality of existing solutions co-exist with the capability of delivering such architecture in a competitive cost-effective time frame, will impact on European competitiveness in a large range of domains as automotive, defense, health, industry and energy.

Considering the health care scenario, as example, where currently SPD applications are restricted only to home or to the medical ambulatory and that could be extended to any environment through an SPD pervasive system, the annual estimated growth rate is 21.3%, which highlights the market opportunities in security systems. A report by Business Communications Company Inc. estimates the global Internet security market to be about $27.7 billion in 2005 and expected to rise at an average annual growth rate (AAGR) of 16.0%, reaching $58 billion by 2010. Furthermore, SPD features will ensure a great impact in defense market, where the most adopted approach is to provide SPD through the closure of the systems rather than SPD enabled technologies and solutions.

Another key factor, for the European industrial competitiveness, is represented by the increasing value of the share of embedded electronics components in the value of the final products (in domains as Telecommunication Systems and Health/Medical Equipment these values are reaching respectively 37% and 33%). Therefore, the value added by SHIELD embedded components (i.e. hardware and software) which will be able to overcome challenges as cost, reliability and interoperability as well as security, privacy and dependability is expected to be some orders of magnitude higher than the cost of the embedded devices themselves.

Finally, the necessity to maintain and ensure SPD for the future, will potentially originate a new business like:

- Business promoted by a network of SPD certification laboratories that will be born from the SHIELD effort to promote SPD metrics and certification process based on its framework
- Businesses that will provide updated solutions to follow and anticipate the evolution of future menaces and attacks.

In the medium/long term perspective, SHIELD will significantly open new possibility for new products and applications also by influencing European R&D activities in ES security, privacy and dependability fields, as far as SHIELD achieved results will influence and at the same time benefit from other projects in which consortium partners' are taking part as SAFAR, MERASA and Enduring Prosperity. As well, with respect to first ARTEMIS call funded project, a possible interaction can be founded with CHESS project which seeks industrial-quality research solutions to problems of property-preserving component assembly in real-time and dependable embedded systems. Concerning these objectives, SHIELD “built in” platform can be easily exploited in order to enhance security, privacy and dependability features.

Moreover, the adoption of SHIELD holistic approach, entailing a seamless SPD enhancement at any layer of the Secure Service Chain (SSC) could contribute to FP7 COSINE2 project objectives in terms of alignment of national research strategies and optimal tuning of RTD policies to the new European Embedded Systems Research environment both at institutional and market level. In fact, SHIELD’s interoperable platform enhancement of SPD services in a large range of application domains will be able to influence development strategies driving ESs designers towards the creation of intrinsically SPD-based solutions exploiting SHIELD modules.

Finally, the project outcomes will positively impact also the definition of new standards for communication and cooperation in user-centric applications for embedded systems. These results will be targeted by fostering collaboration with standardization bodies like OMG or OASIS (e. g. OMG Data Distribution Service specification, etc.).

4.2 - Dissemination and exploitation

SHIELD partners have a strong interest in disseminating and exploiting project results. For this reason they have already planned an effective and realistic industrial and academic dissemination and exploitation plan.

This project will give opportunity to industries and SMEs to acquire know-how and the possibility to exploit results to introduce *new commercial products*, identify new possible application scenarios of SPD technologies, contribute to regulatory bodies with an *effective services and technology architecture* proposal. Moreover, they are interested in *contributing to standards* as described in Section 4.3.
Next sections provide a complete overview of the SHIELD consortium plans in terms of *exploitation, dissemination* and *patents*.

4.2.1 - Dissemination plan

SHIELD *pays a special attention to dissemination activities*, confirmed by the will to contribute in embedded SPD technology and middleware services diffusion, especially within the research test-beds scenario. The dissemination activities will therefore combine complementary actions that altogether should constitute an efficient relay of information towards the market and decision making entities (governments, standardization fora), research and technical community and end users; the wish is also to place the project in the overall European strategies aimed at taking benefit from increasing diffusion of wireless technologies as a concrete alternative to the wired ones. The activities will therefore cover:

Communication actions: production of brochures and setting up of a web portal, developed for providing also a centralized access to the services, contact names, and project's documentation has been foreseen. The web portal will represent a key feature of project dissemination activities involving also the diffusion of studied and developed SPD metrics. Therefore, the aim of SHIELD project is to become a point of reference both at technological and validation level through the dissemination of innovative techniques for the assessment of ESs based applications as well as through the presentation of obtained SPD modules performance.

Publications: project results will be disseminated by paper submissions to major European and worldwide journals and reviews. The SHIELD consortium has already identified some related conferences and journals that could be exploited for this purpose. Here we list the main conferences and journals, but for a more complete list and more details, please refer to Annex C at the end of the document.

Main Conferences

- International Conference on Dependability (DEPEND);
- International Cryptology Conference (CRYPTO);
- Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT);
- International Conference on Software Engineering (ICSE) and the associated workshops (e.g. Workshop on Software Engineering for Secure Systems, Workshop on Software Quality, Workshop on Modeling in Software Engineering);
- International Conference on Software Engineering and Knowledge Engineering;
- International Conference on Software Engineering and Data Engineering (SEDE);
- CeBit, RFID-World, Hannover Trade Fair, RFID-Summit Vienna, DATE, ECRTS, and IWCMC.

Main Journals

- IEEE Transactions on Software Engineering;
- ACM Transactions on Software Engineering Methodology;
- International Journal of Software Engineering & Knowledge Engineering;
- IEEE Software

Participation in standard and industrial fora working groups: SHIELD consortium will therefore establish strong liaisons with research and decision making groups, as it will be described in Section 4.3.

Moreover, SHIELD proposal will have great impact on already running cooperation activities among partners. Actually, Finmeccanica Mind@Share Community and Finmeccanica Network of Excellence, at national level, represent an effective mean of cooperation and joint technology development among SHIELD Italian partners. SHIELD goal will be to reinforce and enlarge such working groups involving new stakeholders, also coming from other member states and in particular from SHIELD's partners member states, to the aim of empowering the spreading of knowledge and good practices in the field of secure, dependable and privacy-oriented ESs.

4.2.2 - Exploitation plan

The exploitation plan focuses on the promotion of the SHIELD framework, highlight the advantages of using it in different SPD emerging applications as well as in enhanced SPD needs coming from the applications already addressed in the project.

SHIELD will give opportunity to industries and SMEs to acquire know-how and the possibility to exploit results in order to reach the following (but not limited to) main objectives:

- Consolidate the competences
- Identify new possible application scenarios of SPD technology
- Introduce new commercial products
- Contribute to regulatory bodies with an effective services and technology architecture proposal

The current section describes, at partner level, the exploitation plan, both for academia and industries.

4.2.2.1 Sample individual industrial exploitation plans

SESM - FINMECCANICA: will exploit the SHIELD project results applying the new approaches FPGAs Run Time Reconfiguration developed during the project to COTS and embedded system. This will allow improving the products and services offered by SESM in the market of aeroportual communications.

Acorde Seguridad: the developed knowledge will enable the creation of a new family of devices in the company portfolio, leading to the opening of a new production line and a research team to further improve the concepts developed within the SHIELD project, as well as a new commercial line. Public dissemination will be mainly done via website, via conference and publications, as well as technical symposia, and covers different aspects of information transfer. Most important is the visibility of the project and the transmission of the results towards the industrial community (system integrators), as well as for national and local administrations as potential end-users. Protection of the knowledge will be granted through the appropriate patents, what will enable the ulterior presentation in fairs, and public demonstrations though our group's network of commercial delegates all over the world.

Ansaldo STS: The results provided by the application of the SHIELD platform to the railway security system will have an impact not only on the quality of the system developed, but also on the design and development costs.
Concerning the increase in system quality, SHIELD will likely improve the advantage of the security system in terms of resiliency, availability and scalability with respect to competing products, and this should have a positive marketing impact.
Concerning the reduction in development costs, SHIELD will significantly reduce the time to market since it enables design modularity with possible reusability of components and it also allows for a quicker verification / assessment of the overall system.
Furthermore, due to the generality of system architecture, the results can be applied to other dependability critical systems (e.g. those used for railway supervision and management) developed by our company.
From the business point of view, Ansaldo STS aims at exploiting SHIELD results in its wide worldwide market sized 1 Billion Euro last year. Security system demand is more and more increasing every year and responding to such a demand is often mandatory to acquire a complete integrated system, especially in the metro sector.
According to the SHIELD plan, first basic results and implementation perspectives should be valuable from the end of 2010 in order to achieve at the end 2011 new architectures and development approaches able to reinforce Ansaldo STS, in terms of client requirement compliance, costs and time-to- market reduction.
A dissemination action will be also carried out inside our company in order show achievable benefits to departments in charge of adopting new development and product platforms.

Elsag Datamat: the results of the SHIELD project will be used to enhance the Elsag Datamat innovation activities with the purpose of developing prototypes and products to be proposed on national and international markets. Furthermore Elsag Datamat intends to tighten new cooperation and alliance with the European partners involved in the project, to develop both new joint projects and business-oriented activities.
The main fields of application of the project results will be in the areas of secure and dependable service middleware and information aggregation solutions for Embedded Systems distributed over IP network infrastructures.

Fundación Tecnalia Research & Organisation: Tecnalia will use the knowledge and results generated in SHIELD to mature their technologies and generate avant-garde service packages and training courses, especially centered on TPM-based solutions, the SPD Metric-based solutions, and Secure Embedded and Services Management-based solutions. For this purpose, Tecnalia works close to the market to identify current needs and to anticipate future needs in the constantly changing sector of Information and Communication Technologies. Though collaboration and co-operation with its members and with leading European companies, Tecnalia develops innovative products and services that ease the transfer of technology and contribute to improve industry competitiveness. Product and services developments put the emphasis on the validation of the approaches by performing experimental trials that ensure its effectiveness. The result is a portfolio of packages products and services including consultancy packages, start-up services, collaborative R&D projects, classroom-based training courses, internet-based training courses, publications (state-of-art survey, models, and methods), etc. Tecnalia will make use of its normal commercial channels to exploit SHIELD project results. That is, mainly "Tecnalia Consultancy Services Dpt.", Tecnalia@net (A commercial Network) and Tecnalia@centers (A Network of Excellence Centers). In addition, the commercial force at Tecnalia, integrated by 4-5 commercials, will support project results exploitation.

Tecnalia@net is Tecnalia's Commercial Network, comprising 35 partners who market and sell Tecnalia products and services in 50 countries worldwide. The network generates 800,000 Euros income for Tecnalia, or 15 percent of Tecnalia's total revenue (data for 2003). Tecnalia@net is formed by companies who agree to include Tecnalia products and services in their product portfolio, and the collaboration is based on service marketing or product distribution agreements. Tecnalia@net allows for a multiplier effect that enables Tecnalia technology to reach not only Europe, but a much broader scope of countries worldwide.

Tecnalia@Center is the Network of Centers for Software Engineering Excellence that comprises a series of technology centers that are similar to Tecnalia in their goals, objectives, activities and legal status; each center is directed towards supporting the software industry in a certain region. The Tecnalia@Center network complements Tecnalia's existing technological capabilities, and enables us to launch initiatives at a global level.

Expected Impact: Tecnalia yearly performs over 50 consultancy services varying from software development maturity assessments to in company technologies introduction, with an impact on over 600 professionals within more than 70 different companies yearly. The average income from these activities is of around 3M euro per year. Among these companies around the 60% are small organizations, therefore Tecnalia estimates that the results of SHIELD will be made available to over 25 SMEs per year as well as to the 52 partners of Tecnalia@net which have at the same time a medium of 10 companies contacted each year, from which 80% are SMEs. The following table summarizes the expected Impact of SHIELD results through Tecnalia dissemination and exploitation (in cumulative numbers).

TECNALIA	Year 1	Year 2	Year 3
Nº of companies to be contacted	35	70	110
Nº of companies to be consulted	10	20	35
Professionals with capable of exploitation SHIELD results	150	400	900
SMEs using SHIELD results	10	40	60
Expected Economical income for Tecnalia from SHIELD results	100 K€	300 K€	500 K€
Nº of published international papers	3	6	10
Nº of new contracts of qualified researches at Tecnalia due to SHIELD	2	5	8

Eurotech: Eurotech will promote project results following SHIELD dissemination plan and participating to dissemination activities related both to academic and industrial contexts. The main target of these activities is to increase and deepen the knowledge and experience on SPD pervasive systems in Europe. This target will be achieved participating to scientific workshops and conferences, publications on scientific journals and professional magazines, publication of tutorials and whitepapers for professionals related to SHIELD results and through communications and promotional activities on the media. Dissemination will include also the establishment of relationship and synergies with existing and new networks of excellence and with clusters/groups focusing on SHIELD topics, both in Europe and world-wide. SHIELD project represents an opportunity to increase Eurotech Group presence in pervasive, wearable and nanocomputer markets, with a particular attention to all the application contexts requiring a high level of SPD. SHIELD results will foster the identification of guidelines that will suggest and drive the evolution of Eurotech Group products in markets with SPD requirements: the project represents an investment for the future in terms of research and know-now. Eurotech R&D center ETH Lab is directly interested in the exploitation of technologies, approaches and solutions identified and developed in the project with respect to four main areas: Intelligent ES Nodes, Smart Transmissions, Secure Middleware and Information Aggregation. The exploitation activities in these fields will put in clear evidence the SPD capabilities of the new products and will have an import social impact, accelerating the public acceptance of pervasive system in everyday life. Finally, SHIELD's results will be used by ETH Lab in further research activities referring to the mentioned areas of scientific interest.

Hellenic Aerospace Industry: HAI has made a strategic decision to extend its activities in the security area and, in particular, border/coastal surveillance and infrastructure security. Currently HAI is actively working in this area and is involved in several related research projects. The SHIELD project is important to HAI as it pursues security, privacy and dependability challenges in embedded systems. HAI expects that such embedded systems will be part of the security solution products and services it will develop in the near future. Furthermore, the holistic approach adopted by SHIELD is expected to contribute to HAI's expertise in pursuing its business goals as security systems integrator and service provider. HAI's exploitation plans will be updated periodically, adapting to the SHIELD findings and market changes. Currently HAI has particular interest in exploiting the technologies developed by SHIELD in the areas of ad-hoc networks, sensor networks, services over dynamic networks, systems integration and lifecycle support.

~~*Integrated Systems Development:* for what concerns exploitation of the results, the business models to be followed are the collaboration with the key players in certain application domains for the development of innovative products or licensing of the technology.~~

MAS: Movation was founded by the seven IT and telecom companies in Norway to foster open innovation in mobile areas. Exploitation of the results achieved in Shield is going to take place through (i) the direct contacts with the CTO/CEO of the inner circle members of Movation, (ii) in conjunction with the companies which Movation is supporting and (iii) through MobileMonday Norway. Movation has an inner circle of companies such as Telenor and Opera Software. The inner circle members, typically CTO or CEO meet about twice a year to discuss technologies and strategies, suggestions for new companies and cross-boarder issues. Telenor Objects, one of the participants in these meetings, is working to harmonise the telecom platform for devices and sensors. Thus we envisage that Shield results will contribute to these discussions. During the last two years Movation has been involved in about 70 companies with evaluation, advise or active participation. These SMEs are often at the forefront of a specific technology, but are not up-to-date when it comes to the latest developments in Research. During Shield Movation will extract relevant aspect and will bring it into one of the companies.

One of the companies Movation works with is the Norwegian Rail Authority (JBV), looking for an advanced system for integrated operations of the railways on the Norwegian Network. Such an integrated operation includes an online support system for all activities on the tracks.

Selex Communications: Selex-Communications will be involved in the exploitation of technologies and solutions for the specific research and technology development (RTD) areas of which it is responsible or directly involved: Intelligent ES Nodes and Smart Transmissions. The exploitation activities will represent a solid approach to promote the use of SHIELD technologies and solutions in the new products for the SPD communication markets of the future. The results of the project will also foster the identification of new customers and markets, both in terms of characteristics and quantification. SHIELD results will be used within Selex-Communications further research activities.

THYIA: aims at exploring embedded technology and 3D integration approach for smart sensor (e.g., smart dust, smart video surveillance applications) that are key technologies for deploying a large number of sensor over a geographically distributed urban or out of urban areas where performance vs. cost a critical for such kind of deployment. Taking the benefits of embedded design and 3D integration the future exploitation in many Railways, Health and other security applications will become potentially feasible. Especially, the business interest for exploitation lies in short range intelligent devices, and different miniature sensor technologies. The following table is giving the potential Thyia's drivers for 3D integration and motivation behind why 3D embedded system design and integration is important for achieving strategic goals for SHIELD.
The main interest of Thyia in the exploitation plan lies in RFID, PDA, specific sensor platform, smart cameras, and other devices that will be delivered in the market after the termination of the project.

Miniaturization	Case for 3D	Caveats
Miniturisation	Stacked memories. "Smart dust" sensors.	For many cases, stacking and wirebonding is sufficient
Power Consumption	In certain cases, a 3D architecture might have substantially lower power over a 2D	Limited domain. In many cases, it does not
Memory Bandwidth	Logic on memory can dramatically improve memory bandwidth	While memory bandwidth can be improved dramatically, memory size can only be improved linearly
Mixed Technology (Heterogeneous) Integration	Tightly integrated mixed technology (e.g. GaAs on silicon, or analog on digital) can bring many system advantages	Though might justify 3D integration, this driver might not justify vertical vias., except for the case of imaging arrays

Table 4.1 - Thyia's potential drivers for embedded devices and 3D integration with emphasis on SPD design

Tecnologie nelle Reti e nei Sistemi T.R.S. S.p.a.: will take advantages from the research results on data distribution systems. New services and products will be delivered deploying DDS software in COTS and embedded systems.

4.2.2.2 Sample individual academic exploitation plans

ATHENA/Industrial Systems Institute: will publish any important results in well-known conferences and journals (see Section 4.2.1). In addition, the research issues of the project will be promoted through the organization of special sessions in conferences and workshops on the research topics (areas) of the project. An important event where such results and topics will be addressed is the Workshop on Embedded System Security (WESS), which is a part of IEEE/ACM Embedded System Week (ESWEEK).

Mondragon Goi Eskola Politeknikoa: results will be used in the context of teaching activities at the University (at computer science and telecommunication engineering degrees and postgraduate lectures). This teaching material will also be offered as industry courses. Mondragon University acts as a R&D supplier for (it is in fact a subsidiary of) Mondragon Corporation Cooperativa, one the 10 main industrial groups in Spain. In this scope, Mondragon University plans to develop advanced courses and seminars to train personnel from local companies during the first two years after the project and also the dissemination of the results by means of publications.

Università di Genova: will publish obtained results in referred International conferences and journals focusing particularly on the study and development of innovative SPD metrics as well as on the study and development of innovative algorithms for secure resource management at transmission level through environment awareness, self-reasoning, self-healing and learning capabilities. Moreover, the University of Genoa ISIP40 group, who will take part in the project, will take advantage from obtained results and performed research in terms of teaching activities, involving students in master thesis strictly related to SHIELD developed solutions. Finally, relevant effort will be devoted to the creation of the SHIELD Manual, particularly concerning the SPD metrics description and to the institution of specific seminars concerning part of SHIELD technologies which will be held each year at University campus.

Università di Roma: intends to exploit the results of this project for didactic and teaching purposes. In particular, many master degree theses are expected to profit from the documentation and the background coming from the SHIELD project. Moreover, project results will be exploited to upgrade and update the programs of several courses and to hold thematic seminars on these matters both at universities and in the companies. In particular, participation to this project will allow new generation engineers to acquire know-how on telecommunication and informatics and more specifically on secure resource management over heterogeneous embedded systems networks. This project will give the chance to reinforce the already existing cooperation and to create new links with the universities, manufactures and operators involved in the project with the target to stimulate these companies towards advanced research topics. Finally, dissemination will be also assured by extensive publications especially on the major international reviews and conferences and by the participation to the main events organized by the European Union as well as by other institutions.

4.2.3 - Patents incentive plan

Due to the innovative aspects of SHIELD project, it is expected that partners will generate Intellectual Property that has to be protected through patents, yet made available for other partners for their own work in the project, and exploited outside of the project by appropriate licensing. Furthermore, due to SHIELD project's concerning with security in embedded systems, patent generation could be a prestigious goal within project objectives. Some partners of the consortium bring in SHIELD a strong expertise in patents production: this is the case, for example, of Infineon Germany~~ or Integrated Systems Development~~. As detailed in section 5.2, the consortium members account skilled people in standardization activities. For example:

- ~~ISD - Mr Constantin Papadas (he has been awarded 9 US and Japanese patents);~~
- UNIROMA1 - Prof Francesco Delli Priscoli (he holds 4 patents).

4.3 - Contribution to standards and regulations

Since the project is a pilot, it could not provide results available to promote standardization activities.

The research challenges raised by the SHIELD project will match the goals of most of the standardization bodies and industrial fora involved on embedded systems and security design. In this context a leading role is expected to be played by the industrial partners of the consortium, since they just participate the most relevant standardization bodies (*ISO, ETSI, MORFEO, ITU, CENELEC,…*) and industrial fora (*NFC Forum, Trusted Computing Group, ADAS, OMG, …*). However, the fundamental cooperation of the more research-focused partners in this standardization activity will improve the capability to produce valuable feedbacks and brand-new solutions to those issues that the SHIELD project is expected to raise in the current standards.

Some partners of the SHIELD consortium have a strong experience in standardization activities and can guide the whole consortium to relevant impact on standardization bodies and industrial fora. For example

- THYIA - Dr. Gordna Mijic in the last 8 years actively participated in the standardization activities for UMTS and UWB as well as other latest technologies development at ETSI, 3GPP and ITU

In the following we describe the contributions to standards which may arise from the project.

4.3.1 - Contribution in standardization bodies and industrial fora

Strong and consistent interactions with relevant organizations may be established with the following standardization bodies and industrial fora, in which one or more partners play a very significant role:

- ***ISO/IEC 27000***, the series of standards that have been specifically reserved for information security matters.

➢ Partner’s Role: Member (Tecnalia)

→ SHIELD could naturally bring to the development of new standards for security or the harmonization of the existing ones.

- ***IEEE International Conference on Composition-Based Software Systems (ICCBSS)***, a premier international forum for researchers, educators, industrial practitioners and students to present and discuss the most recent innovations, trends, experiences and concerns in Composition-Based Software Systems development.

➢ Partner’s Role: Member of the Steering Committee

→ SHIELD could bring new ideas and specifications for (Commercial off-the-shelf) COTS-bases Software Systems

- ***European Telecommunications Standards Institute (ETSI)***, which produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

➢ Partner’s Role: Contributor (THYIA)

→ SHIELD could contribute with some security solution for mobile and radio technologies

- ***Object Management Group (OMG™)***, an international, open membership, not-for-profit computer industry consortium. OMG Task Forces develop enterprise integration standards for a wide range of technologies, and an even wider range of industries. OMG's modeling standards enable powerful visual design, execution and maintenance of software and other processes. OMG's middleware standards and profiles are based on the Common Object Request Broker Architecture (CORBA®) and support a wide variety of industries. All of our specifications may be downloaded without charge from our website.

➢ Partner's Role: Contributing Member (highest level) (SESM)

→ Dissemination of SHIELD activities and studies; Standardization of embedded systems (software) interfaces or services in a number of different domains (Real Time embedded systems, Data Distribution Systems etc.)

4.3.2 - Interaction with other relevant standardization bodies and industrial fora

Possible interactions with relevant organizations may be established with the following standardization bodies and industrial fora, to which one or more partners of the SHIELD consortium belong to and actively participate:

- ***ADAS Air Ground Data-link User Focus Group (DUG),*** a non-permanent task force acting as an operational/technical body for the ODT (Operational Requirements and Data Processing Team), on data-link matters. The DUG shall coordinate the harmonization of European data-link operational requirements for services in support of SESAR's operational concept through the development of data-link European OSED.

→ SHIELD could contribute on security issues in data-link

- ***European Organization for Civil Aviation Equipment (EUROCAE)***, a non profit making organization which was formed at Lucerne (Switzerland) in 1963 to provide a European forum for resolving technical problems with electronic equipment for air transport. EUROCAE deals exclusively with Aviation standardization (Airborne and Ground Systems and Equipments) and related documents as required for use in the regulation of aviation equipment and systems.

→ SHIELD could provide useful hint and solution for electronic equipment for air transport

- ***EPCglobal Hardware (Action Group and Software Action Group)***, that is leading the development of industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks.

→ There is a potential need to address security issues within EPCglobal more actively; especially the European understanding of privacy and data protection is not properly represented. SHIELD results from WP3 could add security specification to RFID application.

- ***Trusted Computing Group (TCG)***, a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.

→ Given the fact that SHIELD addresses issues dealing with trusted computing building blocks and software interfaces across multiple platforms, contributions to TCG will arise. In particular SHIELD could give a substantial contribution on Trusted Platform Module specification and thus increase the European influence on that worldwide standard.

- ***Near Field Communication Forum***, formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. Formed in 2004, the Forum now has over 150 members. Manufacturers, applications developers, financial service institutions, and more all work together to promote the use of NFC technology in consumer electronics, mobile devices, and PCs.

→ SHIELD could provide useful hint for node short-distance communication protocol

- ***Bluetooth Special Interest Group (SIG)***, a privately held, not-for-profit trade association, founded in September 1998. The main tasks for the Bluetooth SIG are to publish *Bluetooth* specifications, administer the qualification program, protect the *Bluetooth* trademarks and evangelize *Bluetooth* wireless technology. In particular SHIELD partners participate in ***Secure Simple Pairing*** and ***Ultra Low power*** white paper groups.

→ About Secure Simple Pairing, SHIELD could help in the definition of a protocol for pairing wireless devices: this could help in specifying security protocols in the node

→ About Ultra Low Power, SHIELD could help in the design of a lightweight protocol for pairing and protecting privacy and integrity of low power wireless transmission: This could help in defining security in node with constraints in term of power consumption

- ***Object Management Group (OMG)***, an international, not-for-profit computer industry consortium. OMG Task Forces develop enterprise integration standards for a wide range of technologies, and an even wider range of industries. OMG's modeling standards enable powerful visual design, execution and maintenance of software and other processes. OMG's middleware standards and profiles are based on the Common Object Request Broker Architecture (CORBA®) and support a wide variety of industries.

→ SHIELD could contribute to methods and tools development for embedded systems

- ***PoweRline Intelligent Metering Evolution (PRIME)***, a project that was launched by Iberdrola in order to asses the idea, define and test a new, future proof, PLC based, open standard that could meet the future requirements on customer real time interfacing and smart grid evolution.

→ SHIELD could help the definition of a low cost security architecture for protecting power line communication

- ***International Council on Systems Engineering (INCOSE)***, a not-for-profit membership organization founded in 1990, whose mission is to advance the state of the art and practice of systems engineering in industry, academia, and government by promoting interdisciplinary, scaleable approaches to produce technologically appropriate solutions that meet societal needs.

→ SHIELD could bring interesting ideas in security engineering for systems

- ***European Security Research Advisory Board (ESRAB)***, an organization of 50 members including high level strategists, with a responsibility relating to security research, from a broad spectrum of stakeholder groups including public and private users, industry, the European Defence Agency and research establishments.

→ Results from SHIELD should converge ESRAB Standardization Policy

- ***International Telecommunication Union (ITU)***, the leading United Nations agency for information and communication technologies. As the global focal point for governments and the private sector, ITU's role in helping the world communicate spans 3 core sectors: radio communication, standardization and development. ITU also organizes TELECOM events and was the lead organizing agency of the World Summit on the Information Society.

→ SHIELD new security solutions could be discussed, standardized and developed by ITU

- ***European Committee for Electrotechnical Standardization (CENELEC)***, created in 1973 as a result of the merger of two previous European organizations: CENELCOM and CENEL. Nowadays, CENELEC is a non-profit technical organization set up under Belgian law and composed of the National Electrotechnical Committees of 30 European countries. In addition, 8 National Committees from neighboring countries are participating in CENELEC work with an Affiliate status. CENELEC members have been working together in the interests of European harmonization since the 1950s, creating both standards requested by the market and harmonized standards in support of European legislation and which have helped to shape the European Internal Market. CENELEC works with 15,000 technical experts from 30 European countries. Its work directly increases market potential, encourages technological development and guarantees the safety and health of consumers and workers.

→ SHIELD could contribute with some innovative security solutions

- ***Wireless World Research Forum (WWRF)***, a global organization founded in August 2001, including over 140 members from five continents, representing all sectors of the mobile communications industry and the research community. The objective of the forum is to formulate visions on strategic future research directions in the wireless field, among industry and academia, and to generate, identify, and promote research areas and technical trends for mobile and wireless system technologies.

→ SHIELD outcomes could be discussed in this forum and become reference ideas for the mobile communications industry

- ***Deutsches Institut für Normung (DIN)***, the German Institute for Standardization that develops norms and standards as a service to industry, the state and society as a whole. A registered non-profit association, DIN has been based in Berlin since 1917. DIN's primary task is to work closely with its stakeholders to develop consensus-based standards that meet market requirements.

→ SHIELD outcomes could give ideas to new standards

4.3.3 - Integration, interoperation and open source implementation

Artemisia WP has indicated the following organization/initiative as playing a significant role for the Embedded Systems development, so they are a preferential field for SHIELD results:

- "standard development and harmonization, as the basis of any integration and inter-operation"
- "open source reference implementations of standards, in order to facilitate their take-up in the market"

The consortium includes partners that belong to this type of organization/initiative. In particular they are:

- ***Information Security Forum (ISF)***, the world's leading independent authority on information security. By harnessing its world-renowned expertise and the collective knowledge and experience of its members - including 50% of Fortune 100 companies - the ISF delivers practical guidance and solutions to overcome wide-ranging security challenges impacting business information today.

→ SHIELD could bring to open source reference implementations of standards

- ***Morfeo Open-Source Software Community***, that works towards the following goals: Speed up the development of Service Oriented Architectures-related software standards, which are key for both systems integration and the evolution of the network as an ecosystem of proliferating services; create business opportunities in the field and integrate solutions targeting enterprises and the Administration based on standard platforms and applications developed within the community; improve the productivity and assure the quality of open-source software-related developments that can be integrated with the standard software development infrastructure for projects of this type (Gforge); act as a catalyst for R&D&I projects in the software field that naturally integrate a range of scientific and technological agents, helping to boost R&D&I activities and the development of a strong industrial fabric in countries where the consortium members operate.

→ SHIELD could help standards development and certification

4.3.4 - Other standardization activities

Up to now, potential activities among standardization organizations or industrial fora where SHIELD partners can act directly have been described. Other related activities could be suggested among different organizations.
This is the case of SHIELD Results from WP2 - *SPD Metric, requirements and system design*, WP6 - *Platform integration, validation & demonstration*. In fact techniques and methods developed by the SHIELD consortium can be used in the Common Criteria (CC, ISO/IES 15408) evaluation and certification process (CEM, ISO/IES 18045). Developers will be able to map SHIELD security requirements to CC security functional and assurance requirements, while evaluators will be able to use checklists issued by SHIELD to verify security claims, and the automated tools developed by the SHIELD consortium will produce the necessary evidence for these claims. In this respect SHIELD focuses on one of the most challenging security problem in software development: the elimination of programming bugs originated vulnerabilities; an important subset of the otherwise much more complex Common Criteria.
About '*Security Engineering Methological Framework*' and '*Security Software Web-Services*', SHIELD consortium will provide contributions from the project results to the XML and WS-based security standards from W3C and OASIS: WS-Security and XML-Security.

Furthermore, since there are no standards dealing with the issues of Composable Security, a contribution towards the creation of standards for Composable Security it's a direction which SHIELD will look after.

4.4 - Management of intellectual property

Due to the innovative aspects of SHIELD, it is expected that partners will generate Intellectual Property that has to be protected through patents, yet made available for other partners for their own work in the project, and exploited outside of the project by appropriate licensing. The project's handling of Intellectual Property Rights (IPR) will be detailed in the consortium agreement and will be in compliance with Article 23 of the Statutes annexed to Council Regulation 74/2008 of 20 December 2007 on the establishment of the ARTEMIS Joint Undertaking.

An essential SHIELD result is the prototypes implementation of the developed system architecture for multi-layer secure and dependable solutions for embedded systems for heterogeneous application fields (railroad, health, cruise liners, flowmeter). Hardware and software together with the new emerging products will be protected within the consortium and within the individual partners. The generated Intellectual Property will be protected through patents, yet made available for other partners for their own work in the project, and exploited outside of the project by appropriate licensing.

In conformance with the model contract, contractors shall enjoy access rights to the knowledge and to the pre-existing know-how, if that knowledge or pre-existing know-how is needed to carry out their own work under the SHIELD project. Access rights to knowledge shall be granted on a royalty-free basis. Access rights to pre-existing know-how shall be granted on a royalty-free basis, unless otherwise agreed before signature of the consortium agreement. In addition, the participants may conclude any agreement aimed at granting additional or more favourable access rights (including to third parties, e.g., affiliates), or at specifying the requirements applicable to access rights (without restricting them). Such provisions will be included in the consortium agreement. Related to dissemination of knowledge to standardisation all partners involved in the generation of this knowledge must agree to submission, since knowledge in standards must be public. The decision making process in section 5.1 will be applied.

Access to foreground or knowledge generated by the project (including patents) will be granted by any partner for project purposes, royalty free and for other use's either royalty free or under fair and reasonable conditions. The consortium is aware of the services of the Commission's IPR Helpdesk and will set up any agreements after consulting the respective guidelines and model agreements.

Participants will analyse possibilities for protection of knowledge, including patents. In that analysis patents will also be considered. Once any patent has been applied for, the project coordinator will inform the other partners as to who will need to be contacted for licenses (subject to a patent being approved) when considering future commercial exploitation. The Project Manager will also contact the Commission-funded IPR support organisation to ensure that other EU projects and organisations world-wide are aware of the new pending patent.

The main aspects of intellectual property rights management are detailed below:

4.4.1 - Ownership and transfer of ownership of knowledge

Knowledge shall be the property of the contractor carrying out the work leading to that knowledge. Where several contractors have jointly carried out work generating the knowledge and where their respective share of the work cannot be ascertained, they shall have joint ownership of such knowledge.

4.4.2 - Protection of knowledge

Where knowledge is capable of industrial or commercial application, its owner shall provide for its adequate and effective protection, in conformity with relevant legal provisions, including the Model Contract and any Consortium Agreement, and having due regard to the legitimate interests of the contractors concerned. Details of any such protection sought or obtained will be included in the Dissemination Plan.

4.4.3 - Access rights to knowledge

The general principles relating to access rights are the following:

1. Access rights shall be granted to any of the other contractors upon written request. The granting of access rights may be made conditional on the conclusion of specific agreements aimed at ensuring that they are used only for the intended purpose, and of appropriate undertakings as to confidentiality. Contractors may also conclude agreements with the purpose of granting additional or more favorable access rights, including access rights to third parties, in particular to enterprises associated with the contractor(s), or specifying the requirements applicable to access rights, but not restricting the latter.
2. Access rights to pre-existing know-how shall be granted provided that the contractor concerned is free to grant them.

Access rights for execution of the project are the following:

1. Contractors shall enjoy access rights to the knowledge and to the pre-existing know-how, if that knowledge or pre-existing know-how is needed to carry out their own work under that project. Access rights to knowledge shall be granted on a royalty-free basis. Access rights to pre-existing know-how shall be granted on a royalty-free basis, unless otherwise agreed before signature of the contract.
2. Subject to its legitimate interests, the termination of the participation of a contractor shall in no way affect its obligation to grant access rights to the other contractors pursuant to the previous paragraph until the end of the project.

Access rights for use of knowledge are the following:

1. Contractors shall enjoy access rights to knowledge and to the pre-existing know-how, if that knowledge or pre-existing know-how is needed to use their own knowledge. Access rights to knowledge shall be granted on a royalty-free basis, unless otherwise agreed before signature of the contract. Access rights to pre-existing know-how shall be granted under fair and non-discriminatory conditions to be agreed.

In addition, the participants may conclude any agreement aimed at granting additional or more favorable access rights (including to third parties, e.g. affiliates), or at specifying the requirements applicable to access rights (without restricting them). Such provisions will be included in the Consortium Agreement.

	Access rights to pre-existing know-how	**Access rights to knowledge resulting from the project**
For carrying out the project	Yes, if a participant needs them for carrying out his own work under the project	
	Royalty-free unless otherwise agreed before signing the contract	Royalty-free
For use purposes (exploitation + further research)	Yes, if a participant needs them for using his own knowledge	
	On non-discriminatory and reasonable conditions to be agreed	Royalty-free unless otherwise agreed before signing the contract
	Possibility for participants to agree on exclusion of specific pre-existing know-how of a participant from this obligation before this participant signs the contract (or before entry of a new participant)	

Figure 4.5 - The Provisions relating to Access Rights

Once any patent has been applied for, the Project Manager will inform the other partners as to who will need to be contacted for licenses (subject to a patent being approved) when considering future commercial exploitation.

Section 5 - Quality of consortium and management

5.1 - Management structure and procedures

The main target is to deploy an efficient and effective governance procedure for all the activities within the project and set up an effective management structure for the whole project which is suited to the project scope and the number of partners within the consortium.

The organization and all the relevant activities will be inspired to the **industrial qualification** of the project's results. The downstream focus of the R&D activities, in other words, will be the "life motif" guiding the management in every aspect concerning the SHIELD project. To reach such scope a design authority group will be setup with representatives from the main industries of the consortium in order to keep tightly connected the solutions found and the real industrial needs.

This peculiar project management vision leads to follow a couple of concepts: **Formal simplification** and **Focus on impact-relevant aspects**. The simplification of formal duties in the project is essential in order to improve the *efficiency* of all the relevant activities, while major attentions kept on impact-relevant aspects of the project promotes the *efficacy* of the SHIELD results.
The simplification will be obtained by keeping only essential versions of public deliverables (reducing the numbers of periodic reports and making essential the contents in those documents, for instance) and adopting simplified decision processes.
The focus on impacts will be obtained by:

- setting up of a Design Authority (a group of partner representatives of the major industries in the TMC that shall be responsible for the preparation and maintenance of the SHIELD framework design data)
- keeping a continuous control of the quality of the project results
- taking care of both standardization components and technical guidelines in the area
- giving great account to every aspect in the project relevant to:
    - industrial and market impact
    - contingency of manufacturing and business risks ,
    - ARTEMIS target's convergence
    - liaison with other R&D projects (especially the ones already funded by ARTEMIS and the ones that will be funded during the SHIELD development phase).

In order to apply the above described management strategy and to efficiently manage the overall project, a specific WP dedicated to management has been foreseen in the project work plan. Within this WP all the aspects related to technical, administrative and quality management of the project will be included. The successful management of the project and consortium will be also based on the experience, capability and motivation of the Coordinator as well as of the Project Manager.

The responsibility of the administrative project co-ordination will be taken by MAS. MAS will express the Project Manager and will represent the single point of contact with the JU for all matters.

The responsibility of the technical project co-ordination will be taken by SESM, a R&D industrial oriented organization with remarkable expertise in the field of security and dependability applied to the embedded systems.

The overall management of the project will be based on six key points:

- The **Organization Structure**, which will define the project organization and management structure to allow efficient work and decision taking;
- The **Decision Making Structure**, to achieve rapidly common agreement on a peer-to-peer base within the different working groups;
- The **Information Distribution Management**, to manage efficiently the information processing: speed of information exchange is essential during project execution;
- The setup of **Regular Meetings** is crucial to maintain relationships, to promote information and exchange and to make agreements and major decisions;
- The **Quality Control**, to guarantee the procedures correctness and the quality of outcomes.
- The **Risk Management**, to decrease the probability of potential risks and to mitigate their effects.

5.1.1 - Organization Structure

The overall organizational structure proposed for the project is shown in the diagram below. It is aimed at ensuring the fulfillment of project objectives, by allowing a good communication among the participants and the most valuable and cost-effective management of the project.

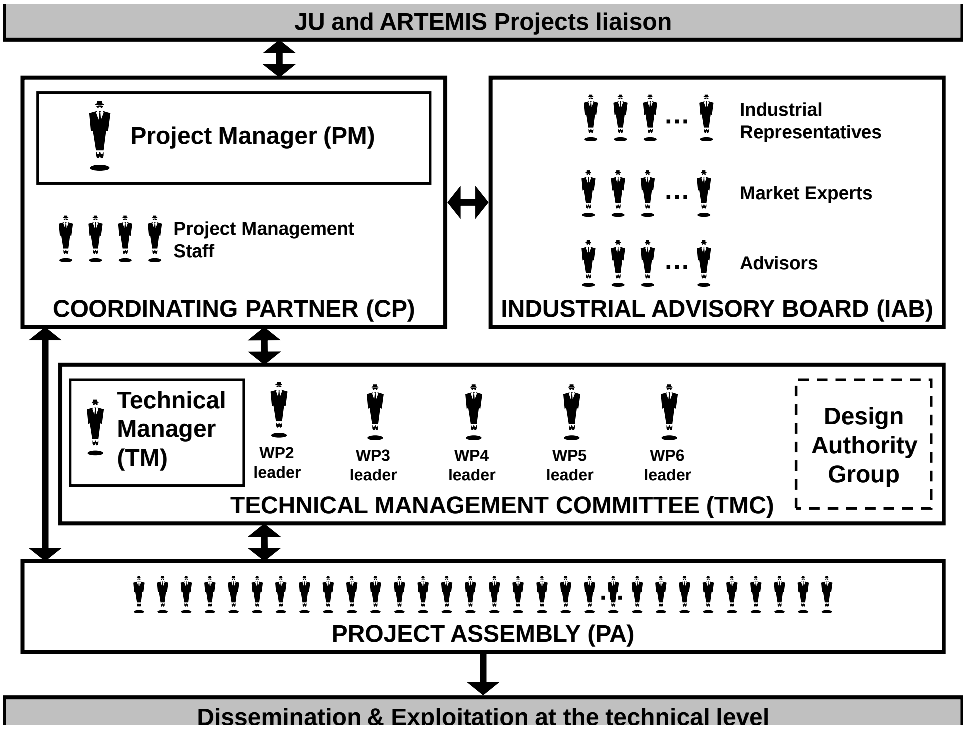

JU and ARTEMIS Projects liaison
Project Manager (PM)
Project Management Staff
COORDINATING PARTNER (CP)
Industrial Representatives
Market Experts
Advisors
INDUSTRIAL ADVISORY BOARD (IAB)
Technical Manager (TM)
WP2 leader
WP3 leader
WP4 leader
WP5 leader
WP6 leader
Design Authority Group
TECHNICAL MANAGEMENT COMMITTEE (TMC)
PROJECT ASSEMBLY (PA)
Dissemination & Exploitation at the technical level

Figure 5.1 - Organization Structure

Management responsibilities exist at the project (Project Manager and Technical Manager), and work-package levels (WP leader and Task leaders).

In more detail, the organizational structure of project foresees the following responsibility levels:

Coordinating Partner (CP)

The Coordinating Partner is the unique point of contact with the ARTEMIS JU for all matters. Specific duties include:

- Organization and chairmanship of the PA meetings and Industrial Advisory Board meeting
- Participating to the Technical Management Committee and calling for the meeting of WP Leaders in case of urgency.
- Supervise the liaison's activities with other ARTEMIS projects at a technical level (liaison will also be performed by the WP leaders and individual partners)
- Adding a level of quality assurance to the project in terms of validating the visible outputs, such as deliverables, presentation material, papers, etc
- Maintaining the Description of Work
- Monitoring the project Website and suggesting improvements

Based on previous experiences in these areas, the Coordinating partner will additionally:

- Collect and collate the Periodic Progress Reports
- Prepare the report due prior to the project Reviews
- Supervise the Cost Claim of each partner and control the handling of Cost Claim procedures maintaining the financial budget status of the whole project.

The Coordinating Partner will nominate the Project Manager.

Project Manager (PM)

The Project Manager, appointed in the person of Mr. Josef Noll (see MAS table in section 5.2 for his relevant Curriculum Vitae) has the overall responsibility for the organization, planning and controlling the project. The PM is a full time managerial role. PM will be assisted by the Project Management Staff in its duties. The PM represents the sole contact person for the project with the ARTEMIS JU and will ensure the punctual delivery of reports and deliverables to the JU. The PM will guarantee the quality of adopted procedures and issued deliverables and is entitled to request additional reports and remedial actions where appropriate. The PM will be also responsible for efficient administration of the project, calling, organizing and chairing the Industrial Advisory Board and Project Assembly meetings and proposing the agenda. The PM will supervise the work of the Technical Manager. The PM will supervise financial and administrative data from the partners, and will prepare the technical and financial data for submission to the JU.

The Project Manager is responsible for:

- the overall technical and administrative co-ordination of the project;
- the control of the project scheduling and achievements;
- the generation of corrective actions, if needed, in conjunction with the Industrial Advisory Board and with the agreement of the Project Assembly;
- the submission to the JU of the deliverables and regular reports of progress;
- being the initial point of contact for liaisons with other JU projects;
- the organization and chairing of the Project Assembly and Industrial Advisory Board meetings;
- risk analysis;
- project level dissemination.

Technical Management Committee (TMC)

A Technical Management Committee (TMC) will be established to support PM in the management of the different technical aspects of the project. The TMC will be in charge to propose the members of the Design Authority Group inside the TMC and is responsible for technical decisions and inter-work-package communication. The TMC debates and approves the design proposals of the Technical Manager. The TMC should ensure that the technical developments and the general progress of the project are in-line with the objectives of the project. The TMC will be composed by technical WP leaders (WP2, WP3, WP4, WP5 and WP6). TMC will be chaired by a Technical Manager (TM). Members of the TMC will be selected at the kick-off meeting.

Technical Manager (TM)

The Technical Manager (TM) is a full time managerial role that has the overall technical responsibility for the project. He provides support to the PM as far as technical management is concerned. TM is in charge to propose design authority. He is responsible for the long-term technical strategy, the choice of techniques, and the quality of results. The TM will monitor compliance of the project progress with the work plan on the basis of progress reports provided by each Work Package Leader. The TM is entitled to request additional information and remedial actions where appropriate. The Technical manager is responsible for the organization and chairing of Technical Management Committee.

Work Package Leader (WPL) and Task Leader (TL)

For each work-package, a Work Package Leader (WPL) is responsible for the technical co-ordination. The responsibility of each WPL is to ensure the activities of the workpackage proceed according to the project work-plan. The WP leader is responsible for the production of the relevant deliverables and may delegate parts of this responsibility to other workpackage participants, in particular to the Task Leaders for the relevant competencies. The Task Leaders will co-ordinate the technical activities inside each task, and refer to the relevant WPL for interactions and information sharing with other Task Leaders inside the WP.

Industrial Advisory *Board (IAB)*

An advisory Board will be established, supporting the PM, to help the project remain focused on the most important topics agreed with the ARTEMIS JU. The board will ensure that the project meets its objectives, whilst also monitoring external developments world-wide, and trends in standardization/specification bodies that come to their attention. The board will be mainly composed by representatives of partners playing a significant role in the industrial market addressed by the project. It could be supported by technical advisors and market experts who will be appointed from time to time.

Project Assembly (PA)

The PA comprises one representative from each partner. It is the only project body that can make decisions on contractual matters, such as the budget, timeline, deliverables, and PM shifts. It will meet periodically, and the meetings will be chaired by the Project Manager.

5.1.2 - Decision Making Mechanism

The **decision making mechanism** of the project will follow the above mentioned structure with respect to relations among Task Leaders, WP Leaders, PM, TM as well as the Assembly and the Industrial Advisory Board foreseen in the organization.

The decision making process is structured in three levels:

- Work package and task leaders are the most important negotiators to reach the common consensus at WP/Task level. Each partner involved in the technical activities of the task will have one vote. Most of the decisions are expected already to be solved on this level.

Decisions will have to be endorsed by a 2/3 majority of positive votes among all the present members. In the case a decision cannot be taken, the problem shall be forwarded to the Work Package Leader for a decision to be taken by the whole work package;

- Decisions not solved on the task or work package level or requiring inter-work-package decisions are handled in the TMC. If consensus cannot be reached at this level the decision should be forwarded to the Project Assembly;
- Finally, the Project Assembly is the ultimate decision making body of the consortium and compromises all partners and is headed by the project manager. A 2/3 majority verdict will be sufficient to carry the decision.

Honoring the peer nature of partners, affected partners will always be invited to place their opinion on all levels of the decision making process. Additionally, specific decisions and corresponding voting procedures may be defined by the consortium agreement.

When a dispute cannot be resolved satisfactorily on the above levels the PM will make all the possible efforts to solve possible conflicts by searching a consensus among the involved partners. If is not possible to reach an agreement the PM, on request of at least one of the contenders, will submit the case to PA calling a PA meeting within 3 months. The Project Assembly, on the basis of possible consultation with the TMC, is the ultimate instance in case of dispute. Quotas and other mechanism to solve the conflicts will be specified in the Consortium Agreement.

The effective execution of the decisions and detailed plans are then demanded to the PM and TMC.

Further details with respect to the decision-making, conflict resolution as well as the management of internal administrative & financial issues will be incorporated in the project's Consortium Agreement.

5.1.3 - Information Distribution Management

Accurate and rapid communication is essential to the effective management of the project.

The Project Manager (PM) is responsible to facilitate and promote internal communications between partners. The PC makes sure that each partner receives all general, technical or management information necessary to carry out the project. The PC controls that this communication strategy is applied by all the partners.

Project internal information comprises multiple information and format such as project planning and control information, technical information and deliverables or software source code. This information is directly exchanged between all relevant partners in the format most appropriate and efficiently used. Project external information consists of deliverables (public or restricted to TIG and other bodies) and contributions to standardisation bodies. If not specified in the list of deliverables (see table 3b in section 3) this information must obtain approval by the PA. In case of TIG communication the TIG Manager is in charge of monitoring if all requests are answered and that documents have the proper depth of contents for the intended audience.
To provide potential interested entities and the public in general an easy to reach point for initial information and contact a web page will be established. This webpage is also the entrance to information restricted to the TIG.

Electronic information exchange will be favored. Given the geographical distribution of the consortium members, electronic communication will be the most regularly used channel for internally sharing both ad hoc and scheduled documents as project planning, technical information, draft versions of deliverables and informal documents.

For day-to-day operations, web based collaboration technology will be made available to facilitate effective information communications. A web based Content Management System (CMS) will be set up at the beginning of the project. Document and correspondence control will be automated to the extent feasible. Daily communication between all participants will be assured using electronic mail and Web based bulletin boards. A web site will be set-up in order to acts as repository for internal documents and for dissemination purposes. On the basis of the experience of all the project partners and to support future eGovernment processes (like the standard "DOMEA-Process") an eCommunications platform (groupware and portal) like the Share Point Portal Software from Microsoft will be recommended and, if approved, implemented. Systems like it will be show the project information, have workflow and document-management opportunities, manage the coordination of correspondence, meetings etc. and have also search and archive functionality. It covers also all aspects needs, from scanning over records, management up to workflow and archiving processes.

Usage of teleconferencing is foreseen to hold meetings as often as necessary to avoid delays in decision making, time lost in travels and travel expenses.

Periodic progress reports and deliverables will be produced in paper copy for formal presentation to the JU and for wider dissemination.

5.1.4 - Meetings

Regular meetings are crucial to maintain relationships, to promote information and exchange and to make agreements and major decisions.

At least every 6 months a full (face-to-face) meeting will take place during which the Project Assembly will meet and which is chaired by the Project Manager. To save costs face-to-face meetings shall be organized in such a way to cover multiple topics. E.g. it is intended to combine PA and TMC meetings whenever possible. Additionally, the meetings are held alternating at premises of the individual partners to share travel costs by fair means.

The TMC will meet at least every 4 months, in order to ensure that the technical developments and general progress are well coordinated.

Further, to these full meetings, meetings both at work package and task level can take place, although it is planned to heavily facilitate technical means such as telephone conferences to conduct these meetings in a virtual space to reduce travel costs. The organization of these meetings is in the responsibility of the respective Work Package or Task Leaders.

5.1.5 - Quality Control and Quality Assurance

The quality of the results achieved by the project will be controlled according to the following criteria:

- Contribution to the project objectives;
- Correspondence of solutions with ARTEMIS expectations;
- Accuracy and meaningfulness of the outputs;
- Respect of time and cost constraints planned for the project.

The technical and scientific quality of the project output and deliverables is ensured by an internal review process shown in Figure 5.2. First level of quality check is in the responsibility of the group creating the scientific output and is based on common rules for scientific work. Each document and deliverable is subject to an internal review after completion which is conducted by the Task leader, eventually supported by one or two project participants not directly involved in the compilation of the output. When accepted by these internal reviewers a review at work package level is performed. The work package leader, who is in charge of organization and supervision of the review process, reviews the documentation, eventually supported by one or two external reviewers selected by the IAB. After that the document will be forwarded to the Project Assembly and the General Manager for final approval. The Project Manager also does a final check for consistency, readability and for accordance of the content to the general requirements and objectives of the project.

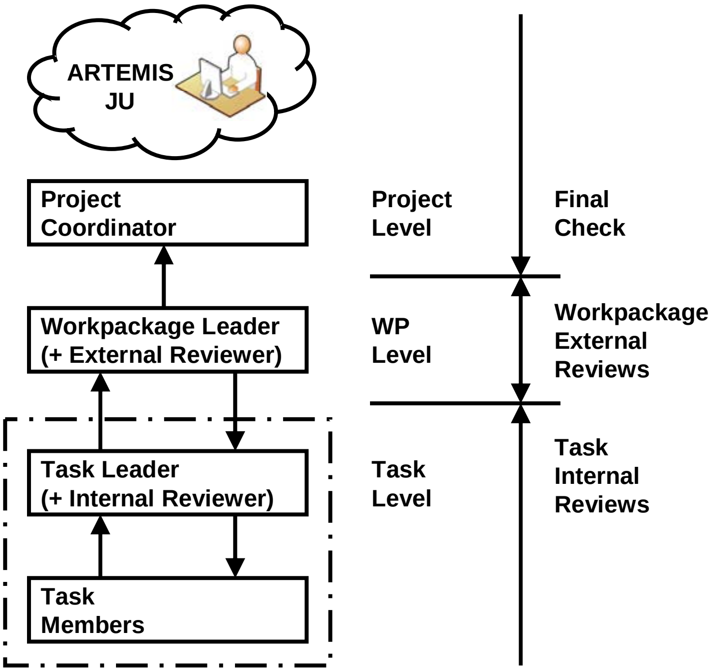


Figure 5.2 - Project internal review process

Templates for deliverables will be agreed at consortium level at project startup.

Record copies of deliverables and all project documentation will be kept in both electronic form (when available) and in hard copy in secure archives.

5.1.6 - Risk Management

Potential risks can be classified into the following groups:

- Partner problems (e.g., a partner is underperforming or a key partner is leaving the project)
- Expertise risks (e.g., a key person with a specific expertise is leaving the project)
- Market and user-related risks (e.g. the market environment or the user is subject to change and makes the results obsolete)
- Project execution risks (e.g., key milestones or critical deliverables are delayed)
- Agreement risks (e.g., consortium partners cannot agree because of differing interests)
- Technological risks (e.g., key technologies or components are not available at the expected time)
- Dissemination risks (e.g., no major customers for using the results are found)
- Competition risks (e.g., a competing solution comes up and makes the results less valuable)

Several of these potential risks can be assessed concerning their probability and level of (negative) impact. Risks with a high probability and a severe impact are handled with particular caution during the project. The following measures are foreseen to meet those risks:

- Potential risks will be identified and analysed in detail.
- For the ones with medium to high probability and severe impact countermeasures and contingency plans are discussed, and they will be flagged throughout the execution of the project as "risk items". This ensures that all levels of the project take special care of those items.

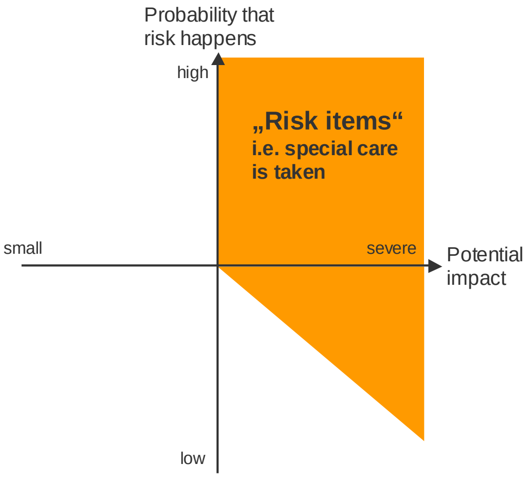


Figure 5.3 - Risks classification

- For the ones with low probability or low impact, and for the ones that cannot be foreseen at this stage, the IP Board will ensure that such are identified in an early phase, and that necessary countermeasures are taken.

The project management approach proposed for SHIELD provides mechanisms to identify and resolve potential risks. The IAB continuously controls the project plan with its milestones and critical paths. In addition the partners produce simplified internal monthly progress reports in order to ensure that the management is made aware of any potential problems on a timely basis, and can initiate countermeasures long before a problem becomes critical. The tight control both at the WP and IP management level ensures that solutions will be available in time. As an additional measure the PM will maintain an "issue" database, which will keep track of any issues, and describe the solutions and lessons learned.

5.2 - Individual participants

In this section for each participant in the SHIELD project is provided a brief description of the legal entity, the main tasks it has been attributed, and the previous experience relevant to those tasks. For each partner are also attached the CVs of the individuals who will have major roles in undertaking the work.

Organization	**SESM - FINMECCANICA**	**Short Name**	**SESM**	**Partner #**	**1**
Country	Italy	**Logo**	SESM A Finmeccanica Company		
Type	Private Research Organization				
Description	Founded in 1990, Consorzio SESM is a private industry participated by SELEX-Sistemi Integrati (third world leader in ATC systems) and Galileo Avionica S.p.A. As well as their owners, SESM is part of Finmeccanica Group. SESM has a long and consolidated experience in realizing and managing national and international research projects. It participates in several research programmes funded by Italian Organizations (like MURST, MISM, MIUR and others) and by European Organizations (European Commission and European Council), concerning National Development Plans, European Framework Programmes and other European Programmes, like ESPRIT, COMITT, etc.. SESM has been involving in two European thematic networks: Fire in Tunnels (FIT) and Safety in Tunnels (SafeT). SESM is also partner in the ETI Project: Pro-active intelligence and support programme to stimulate European SMEs Faced with research issues in the field of ICT security (SECURE-FORCE). SESM is also involved in SWIM-SUIT project.				
Qualification of the key personnel	Eng. Nicola Iarossi: Research & Software Architecture Specialist. Bachelor in Electronic Engineering, Specialization in Information & Communication Technologies. Recently he is leading the SESM effort in an EU funded project (FP7-Security-2007) integrating passive/bi-static sensors with an enhanced ATC radar for the improved surveillance of the skies and collaborate, as workgroup focal-point, to the realization of the SP6 work-program in ARTEMIS. **Antonio Di Marzo** was born on July 23th, 1975. He received the M.Sc in Electronic Engineering from Federico II di Napoli in 2001 discussing a thesis on “design, develop and application of Fault Analysis Methodologies for complex production chain”. He is currently employed in SESM a Finmeccanica Company located in Naples (Italy), as Senior Embedded System Engineer. Before he joins SESM, he worked for some years in ST Microelectonics S.p.a. as Testing Engineer and Design Engineer on Mixed Analog Chip.				

Organization	**Acorde Seguridad S.L.**	**Short Name**	**AS**	**Partner #**	**2**
Country	Spain	**Logo**	ACORDE		
Type	Small Enterprise				
Description	Seguridad is a recently created (2007) company of ACORDE group, a very dynamic business dedicated to the design and manufacture of microwave components, equipment and systems for satellite and terrestrial communications, with a high capacity in R&D. ACORDE Technologies (original company in which most of ACORDE Seguridad members worked) is an SME of 80 workers, 70% are Telecom engineers. That company was created in 1999 but its engineers have long expertise in the system engineering, RF and Microwave hardware development. Some of its senior engineers have more than 20 years of expertise and many of them have been working in this area for more than 10 years. ACORDE is the main provider of the Spanish Army of satellite communications transceivers, frequency converters, amplifiers, synthesizers and similar products. ACORDE is specialized also in design and development of custom articles, such us a light weight X-band Manpack Terminal, Radio over Fibre systems for UMTS, and Satellite Antenna System to provide INTERNET to High Speed Trains. The main business areas of ACORDE Seguridad are custom solutions (some of them designed and developed internally) for perimeter security, distributed monitoring, and secure networks. Seguridad staff members have long experience in R&D projects at national and European level since its origin, assuming in all the projects the Hw/RF designer and manufacturer role. ACORDE's involvement in European collaborative projects (IST, Aeronautics, Galileo, ESA) dealing with the mentioned topics could be sampled as: WISE (IST- Space and Aeronautics): design and manufacture of wireless sensors network mounted on aircrafts; Magnet/Beyond (IST-ICT): design and development of WPAN Low Date Rate (MMIC based) and High Data rate platforms (RF sections).Besides ACORDE Seguridad has a long expertise in R&D internal activities aimed at developing new products and solutions, and creating custom systems for specific customers.				
Qualification of the key personnel	**José Antonio TORRALBA SIMARRO** was born in 1972 in Manresa, Spain. He graduated in Electronic Physicist in 1997 from the University of Cantabria, Santander, Spain. In 2002 he joined IAM.S.A as General Manager until the integration in the ACORDE Group where he became the Head of the System Engineering Department. Once the group created the new firm (ACORDE Seguridad), he was named as General Manager. **Sergio FIGUEROA PÉREZ** was born in Santiago, Chile, in 1971. He studied Informatics Engineering in Universidad Nacional Andrés Bello (Chile).In 2008 he joined ACORDE Seguridad, to develop a specific trace and location tool, as well as providing his informatics knowledge insights to other internal developments of the company.				

Organization	**Ansaldo STS**	**Short Name**	**ASTS**	**Partner #**	**3**
Country	Italy	**Logo**	AnsaldoSTS A Finmeccanica Company		
Type	Industry				
Description	Ansaldo STS is a leading technology company listed on the Milan stock exchange and operating in the global Railway & Mass Transit Transportation Systems business with the provision of traffic management, planning, train control and signalling systems and services. It acts as lead contractor and turnkey provider on major projects worldwide. Ansaldo STS brings together the know-how, excellence and technological expertise of pioneering companies like *Ansaldo Signal, Ansaldo Trasporti Sistemi Ferroviari, Union Switch & Signal and CSEE Transport*. Ansaldo STS is headquartered in Genoa, Italy, and employs over 4,200 people in 28 different countries. In 2007, the revenues of Ansaldo STS reached € 973 M, with a gross operating margin of € 100,3 M and net profits of € 58,2 M.				
Qualification of the key personnel	**Dr. Concetta Pragliola** got her laurea and doctorate degrees in Electronic Engineering from the University Federico II of Naples in October 1985. From January 1987 to October 1992 she has worked in the Research Department of Ansaldo Transporti on Expert Systems and Simulation programs. From November 1992 to October 2001, she has worked in the Information Technology Department of Ansaldo Trasporti, being involved in PDM systems. From November 2001 to November 2006 she has worked in Elsag as an Account Manager. Since December 2006 she has worked in the Innovation unit of Ansaldo STS specializing on the design of security systems. **Dr. Francesco Flammini** got with honors his laurea (July 2003) and doctorate (December 2006) degrees in Computer Engineering from the University Federico II of Naples. From October 2003 to January 2007, he has worked in Ansaldo STS as a Software Engineer in the RAMS unit on the verification and validation of real-time control systems. In 2006-2008, he has been an Adjunct Professor of Computer Science and Software Engineering. Since February 2007, he has worked in the Innovation & Competitiveness unit on several research projects mainly focusing the protection of transportation infrastructures. He has authored more than 30 research papers published on international journals and conference proceedings.				

Organization	**ATHENA RC/ Industrial Systems Institute**	**Short Name**	**ATHENA**	**Partner #**	**4**
Country	Greece	**Logo**	I.S.I. Industrial Systems Institute		
Type	Public Research Institute				
Description	I.S.I is the only research institute for industrial systems in Greece and belongs to the wider public sector, being supervised by the General Secretariat for Research and Technology of the Greek Ministry of Development. It was founded in 1998 and has its headquarters in Patras, Greece. The main goals of I.S.I. include the active participation and substantial contribution in high-technology sectors, which relate to integrated industrial systems, with the objective of increasing the competitiveness of the industry through application of state-of-the-art technologies. I.S.I. has a wide experience in research project such as Intermedia, PABADIS PROMISE, E-NEXT, INNO, ASPIS.				
Qualification of the key personnel	**Dimitrios N. Serpanos** is a Professor of the Department of Electrical and Computer Engineering at the University of Patras, Greece, and Director of the Industrial Systems Institute (ATHENA). He holds a PhD in Computer Science from Princeton University, since 1990. His research interests include computer systems architecture, design and implementation with an emphasis on embedded systems, security systems, high-speed networks and network systems, multimedia systems, and parallel and distributed systems. **Athanasios Kalogeras** holds a Researcher C position at the Industrial Systems Institute. His research interests include Computer Integrated Manufacturing (CIM), industrial networking, industrial automation systems, enterprise interoperability, collaborative manufacturing, industrial multimedia and agent based systems. Dr Kalogeras has a total of 44 publications in journals and conference proceedings and is involved in many R&D projects funded by the EC and Greek programmes. **John Gialelis, Dr**, Researcher Electrical Engineer, MSc, Ph.D, since 2000 has been a research fellow in the Applied Electronics Lab in the Electrical and Computer Engineering Department at the University of Patras, Greece and he is member of the I.S.I. His research interests include collaborative manufacturing, integrated industrial information systems and interoperability, Model driven architecture and ontology engineering, semantically enriched agent based systems, wireless personal area networks for patient monitoring. Dr. Ioannis Gialelis has over 30 publications in journals and conference proceedings and he is involved in many Greek and EC funded R&D projects.				

Organization	**Critical Software**	**Short Name**	**CS**	**Partner #**	**5**
Country	Portugal	**Logo**	Critical software		
Type	Medium Enterprise				
Description	Critical Software provides solutions for mission and business critical information systems. Its customers are drawn from several markets including telecoms, the public sector, industry, aerospace and defence. Founded in 1998, the company today employs over 300 people at its various national and international sites with its headquarters and main technical centre in Coimbra, Portugal and auxiliary engineering facilities in Lisbon and Porto. Critical Software S.A. already performed actively several participations in EU RTD projects in FP5, FP6 and now in FP7. It has managed, as prime contractor, several research and critical technology European Space Agency (ESA) projects involving embedded systems, such as RTEMS and xLuna (besides MAGES, RiskEOS, RTEMS and PREMFIRE). Critical Software is also Project Coordinator of EMMON project (Embedded MONitoring), an ARTEMIS Call 2008 project, dedicated to the research and development in the area of Large Scale Wireless Sensor Networks (LSWSN). Critical Software is also a partner of CESAR project (another ARTEMIS Call 2008 project).				
Qualification of the key personnel	**Délio Almeida** Project Coordinator and Project Manager of strategic projects for the company in the Aerospace, Aeronautics, Defense and Transportation domains, covering all Competence Areas of the enterprise: 1.Project Manager of the “Madeira Project”, for Westland Helicopters in UK 2.Project Coordinator of the MGF External Interfaces project, part of the Galileo constellation system, for the European Space Agency; 3.CSW Project Coordinator of the Ambient Networks R&D project, for the development of 4th generation mobile systems; 4.Member of Critical Software Quality Council In 2001 graduated in UC/FCT/DEI - University of Coimbra, Technology and Sciences Faculty, Computer Science Department, with a 5 year Computer Science degree covering all computer science related subjects necessary for an engineering position. In 2008 got the PMP credential from Project Management Institute. **José Veríssimo (Security Expert)** Academic degree in Electrotechnical and Computer Engineering (Telecommunications Specialization) at University of Coimbra, having specific training in information security, namely CISA, and ISO 27001 Lead Auditor certification. Has a strong work experience in security, dependability, embedded systems, operating systems, and protocols. **Paulo Lourenço (Security Expert)** Graduated in Computer Science and Systems Engineering at Coimbra’s Superior Engineering Institute (ISEC) with final project in Synchronous Digital Hierarchy technology for use in telecommunication networks at NEC Portugal is now Chief Security Officer and Security & Infrastructure Area Manager at Critical Software. Professional experience evolved around Audit and Technological Consultancy projects.				

Organization	**Center for Wireless Innovation**	**Short Name**	**CWIN**	**Partner #**	**6**
Country	Norway	**Logo**			
Type	Public Research Institute				
Description	The Center for Wireless Innovation is a research cooperation between seven Norwegian Universities and University colleagues. UNIK - University Graduate Center is a founding member of CWI and represents CWI in this proposal. UNIK is a non-profit educational and research foundation owned by the University of Oslo (Unik/UiO), Norwegian University of Science and Technology (NTNU) and the three major research institutes: the Norwegian Defence Research Establishment (FFI), Institute for Energy Technology (IFE) and Telenor R&D. UNIK is a graduate educational institution for master's, graduate engineering and doctoral students, primarily from Unik/UiO and NTNU. The main focus of UNIK is on applied science. UNIK is partner of Telenor's Platform for Advanced Telecommunication Services (PATS.no) and provides services over the operational network of Telenor. Associate researchers and professors of UNIK have typically an additional role in industry or at another research institute to enhance dissemination of activities. In the SHIELD project UNIK participates through the group for Security and Mobility. The group has an experimental approach. The group has three professors, two post docs and more than 12 Ph.D students. The involved key personnel was involved in the FP6 projects ASG and ePerSpace, as well as the Eureka projects SUMO and WellCom.				
Qualification of the key personnel	**Prof. Dr. Vladimir A. Oleshchuk** is a Professor of Computer Science at the Department of Information and Telecommunications Technology and Head of System and security group, University of Agder, Norway. He was a visiting research fellow at University of Oslo, Norway, University of Pittsburgh, USA, and University of Aizu, Japan. His current research interests include formal methods and information security, safety and privacy preserving with special focus on telecommunication systems. He is a senior member of ACM, member of IEEE and Member of Agder Academy of Sciences and Letters. **Dr. Mohammad M. R. Chowdhury** is a Post Doctoral Fellow at the UNIK-University Graduate Center, Kjeller, Norway in the area of Security, Privacy and Trust in the Internet of Things. He completed his Ph.D. from the University of Oslo, Norway. His research interests include Security, Privacy and Trust in the Web, Identity Management, Semantic Technologies and Internet of Things. **Dr. Josef Noll** is a Professor at the University of Oslo in the area of Mobile Services. He is the founding member of the CWI. Previously he was Senior Advisor and group leader at Telenor R&I. He was use-case leader in the EU FP6 'Adaptive Services Grid (ASG)' projects, initiated the FP6 ePerSpace project and was project leader of 5 Eurescom projects. His research interests include mobile-based trust and authentication, personalised and context-aware service provisioning, the Internet of Things, and the evolution towards beyond 3G systems.				

Organization	**Elsag Datamat S.p.A.**	**Short Name**	**ED**	**Partner #**	**7**
Country	Italy	**Logo**	ELSAG DATAMAT A Finmeccanica Company		
Type	Industry				
Description	Resulting from the integration of Elsag and Datamat in 2007, Elsag Datamat is a company in Finmeccanica group, one of the world's leading industrial conglomerates. The professional skills of 4,000 employees, technology, know-how, the capacity to operate in critical contexts, and an innovative approach demonstrated by constant investment in Research & Development, are just some of the distinctive features developed over more than a century in business. Elsag Datamat develops, produces and sells IT products, solutions and systems for applications in its main business areas and as empowering technology infrastructure in other strategic areas. In Telecommunications and Utilities industries, Elsag Datamat addresses fixed and mobile operators, data and video networks with a wide-range offering: from consultancy to System Integration and solutions in OSS (Operation Support System), BSS (Business Support System), Networking & Security, IT Governance areas. Elsag Datamat has an intense R&D activities and it has been extensively involved in European research programs and has a strong background in Management and Network Management and security. Together with the above capabilities, Elsag Datamat includes in its portfolio several solutions for delivering services based upon SOA infrastructures and it offers to its customer solution and services for monitoring and managing complex infrastructures such as communication and power ones.				
Qualification of the key personnel	**Enrico Angori** received his master in Electronic Engineering from University “La Sapienza” of Rome in 1987. In the same year he started working at Datamat. He has worked in a number of projects, including military CMS and Message Handling systems, security systems for main Italian Administrations, AAA systems and Data Warehouses for Telco operators. He worked in some ICT projects as both project coordinator and WP leader. He has coordinated an FP6 IP named WEIRD He has been implementation WP leader in EuQoS FP6 project. He has been project manager for a EU funded project named CAS: implementation of a “Computerised Accounting System”, having KEK, Korporata Energietike e Kosoves, as end user, and funded by European Agency for Reconstruction in Kosovo. **Giuseppe Martufi** graduated in Electronic Engineering from University “La Sapienza” of Rome in 1997. When he started working for Datamat he had managed project focused on control protocols (SIP) and on IP-based data transport protocols. In this moment he is leading the R&D group of technicians in Elsag Datamat. This activity has provided him with a wide knowledge of existing communication standards, with a particular focus on IP-based standards. **Massimiliano Taglieri** graduated in Computer Engineering in December 2005 from University of Rome “Sapienza” and in February 2006 he started working for Datamat in R&D technical group. From April 2007 to June 2008 he has been involved in WEIRD FP6 project.				

Organization	**Fundación Tecnalia Research & Innovation**	**Short Name**	**Tecnalia**	**Partner #**	**8**
Country	Spain	**Logo**			
Type	Medium Enterprise				
Description	Fundación Tecnalia Research & Organisation (Tecnalia) is a non-profit foundation launched in 1993 by initiative of a group of leading European companies that work in the software field with the very active support of the European Commission and the Basque Government. Through R&D projects, Tecnalia develops and validates innovative approaches to produce high quality software, faster and at lower cost. These projects lead to products and services that facilitate technology transfer, and improve management and software engineering practices in an entrepreneurial context. Main key areas of technology research are: (i) Trust, Security & Dependability (TSD): The focus is on designing and architecting more trustable systems and improving system security and dependability by facilitating the design and development of secure software, together with TSD measurement definition, interception, and level calculation; (ii) Security Engineering on Software & Embedded Systems: The focus is on software intensive systems development methods and tools with specific emphasis in design, code generation, early verification and validation, certification and integration and interoperability; (iii) Trusted Platform Modules (TPM): The focus is approach security by hardware based solutions as TPM chipsets, which provide functionalities as secure key storage, asymmetric and symmetric encryption key generation, random key generation, etc.				
Qualification of the key personnel	**Mr. Iñaki Eguia** belongs to Research and Development Area at Tecnalia. He is a project leader and has participated in several European projects related to security and networks heterogeneity. He is member of INES and Prometeo, counterparts of NESSI and Artemis in Spain. He is also the responsible of International Innovation Unit of Prometeo that aims to push enterprises to do an international R&D. He is studying for his Ph. D. in 'R&D Management' at E.T.S Ingenieros Industriales y Telecomunicaciones de Bilbao. He obtained his degree in Computer Science from Deusto University and Lund University and his degree in Industrial engineering at Deusto University. **Dra. Estíbaliz Delgado** belongs to the 'R&D Project Area' at Tecnalia, being the head of the 'Trust, Security & Dependability' Dpt. She joined ESI in 1998, since she managed and participated in multiple R&D projects related to Information Security and Software Process Improvement. She also participates in several consultancy services in national and international companies, as well as she acts as instructor of training courses related to Information Security issues. She has been in charge of 2 Special Interest Groups on 'Security Policy Management' and 'Trust marks' within the ALPINE Working Group, she also belongs to the executive committee of the Spanish Technology Platform on Trust & Security – eSEC. She has a Ph.D on 'Trust Boosting Mechanisms for eCommerce' within the Inter-Schools Programme "Project Management", at E.T.S. Ingenieros Industriales y Ingenieros de Telecomunicaciones deBilbao (UPV/EHU). She belongs to the scientific committee of WISTP Conference (2007, 2008, 2009, 2010), IMIS 2010, and SecSE-ARES 2010, and participates as occasionally				

	reviewer of the BIT Magazine, and TRUST 2008 Conference.

Organization	**Eurotech S.p.A.**	**Short Name**	**ETH**	**Partner #**	**9**
Country	Italy	**Logo**	EuroTecH THE COMPLETE EMBEDDED PC SOLUTION		
Type	Industry				
Description	Eurotech Group S.p.A. operates in the areas of research, development and commercialization of pervasive systems. Eurotech in 2002 founded ETHLab, the research center of the group. Through ETHLab, Eurotech has oriented its research activities to the study of key high-growth sectors like pervasive computing. The Pervasive Computing paradigm allows making data and application services available to any authorized user anywhere, anytime and on any device. A pervasive system is an environment where almost “everything” is a computing node which communicates wirelessly and interacts seamlessly with other nodes and people. Eurotech Group designs and implements all the building blocks required in a pervasive system: smart objects, miniaturized computers (MicroPC and NanoPC), super computers (HPC), pervasive networks and software platforms for pervasive systems management. Eurotech Group gives a great importance to the study and development of advanced and frontier technologies. This policy allows maintaining a competitive advantage on a long period and gives the possibility to anticipate the evolution of future scenarios and reference markets. Research activities are intended both to sustain the roadmap of Eurotech’s products and to explore new and innovative frontiers in pervasive computing. SHIELD project represents an opportunity to increase and enforce SPD capabilities of Eurotech products in pervasive, wearable and nanocomputer markets. Eurotech can share its expertise in these fields very close to SHIELD and the project will provide important SPD guidelines to drive and suggest the evolution of Eurotech products in many technology markets. SHIELD project represents an investment for the future in terms of research, know-how and expertise.				
Qualification of the key personnel	**Paolo Azzoni** holds a Master Degree in Computer Science and a second Master Degree in intelligent Systems, both from the University of Verona, and is working towards the completion of a Master in Physics at the University of Parma. After a period of research in holographic memories conducted at the University of Parma, and on lambda-calculus and artificial intelligence, at the University of Verona, he joined ST Microelectronics where was involved on the formal verification of the SuperArgus architecture, a 64-bits risc cpu for embedded systems. In year 2001 he joined EDALab, the Embedded System Laboratory of the Verona University, where he was involved in many research and teaching activities in the areas of simulation tools for formal verification, hw/sw co-design and co-simulation and in the area of embedded circuits and multiprocessor systems. In 2006 he joined ETHLab, the EUROTECH Group research center, as Research Project Manager. In ETHLab he is responsible for national and international research projects, for all the activities related to Artemis and Eniac JTIs and for the research in the areas of pervasive computing, health care systems, wearable computing and custom integrated systems.				

Organization	**Hellenic Aerospace Industry S.A.**	**Short Name**	**HAI**	**Partner #**	**10**
Country	Greece	**Logo**	Hellenic Aerospace Industry		
Type	Industry				
Description	HAI was founded in 1975 and it is the largest defense industry in Greece with a vision of being the premier company in providing aviation support related services and products to the domestic and world marketplaces. Through consistent efforts towards developing the necessary capabilities and establishing high performance standards, HAI is now one of the growing leaders in providing efficient and high quality services and products within the scope of its operations, which involve: Aircraft, engine, accessories and avionics maintenance (overhaul, modification, upgrade, repair and logistic support) for military and civilian aircrafts; Design, development, manufacturing and after sales support of electronic, optoelectronic, telecommunication and information products for military and civilian use; Information systems for collection, assessment and processing data (development of software tools, decision making, provision of terminal equipments and systems integration). HAI's main involvement in SHIELD will be in the network and middleware fields (utilizing its experience in secure communication systems) and integration and lifecycle support (utilizing its expertise as integrators and solution providers of large-scale systems).					
Qualification of the key personnel	**Evangelos Ladis** received his BSc degree in Electrical engineering from Nottingham University in UK and his MSc degree in Digital techniques from Herriot Watt University in Edinburgh Scotland. He has been with HAI for 28 Years and he is currently the Director for Electronic Systems Strategy, Research and Development. He planned, organized, established and managed the Electronics activity in HAI for more than 18 years to cover production, research and development of new products and systems. He has been a member of several government committees to establish the space and satellite activities in Greece as well as Military Systems, Telecommunications and Aeronautics. He acted as evaluator of research proposals as well as Business investment proposals. He is a Member of the Technical Chamber of Greece. **Athanasios Poulakidas** graduated from the Department of Computer Engineering and Informatics, University of Patras (1990) and received his MSc and PhD from the Department of Computer Science, University of California, Santa Barbara (1997). Dr. Poulakidas has participated in several research projects in the USA (multiprocessor erosion emulator, Digital Library Initiative) and Europe (algorithms for mobile and wireless networks, risk management, network statistics and indicators, production optimization, distributed algorithms and simulator, supply chain optimization), and in development projects at HAI (C2 and C4I systems, communications). He has served as referee or committee member in several conferences and the Journal of Systems and Software. His research interests include distributed and parallel algorithms and systems, middleware, simulation, mobile computing, image compression.					

~~**Organization**~~	~~**Integrated Systems Development S.A.**~~	~~**Short Name**~~	~~**ISD**~~	~~**Partner #**~~	~~**11**~~
~~**Country**~~	~~Greece~~	~~**Logo**~~	~~ISD S.A Integrated Systems Development~~		
~~**Type**~~	~~Small Enterprise~~				
~~**Description**~~	~~ISD is active in the domain of Integrated Systems (IS) of guaranteed quality and performance. It is an R&D organization collaborating with system houses, software houses and integrated circuit manufacturers.~~ ~~Actually ISD acts as an original electronic equipment developer and integrator, providing services ranging from software development for embedded and general purpose platforms, to digital and analog/RF integrated circuit design, memory design, to digital signal processing for embedded/stand-alone applications and PCB design. Moreover ISD is a turn-key solution provider handling all aspects of product definition, design, development, documentation, production and support. ISD is also actively involved in the field of telemedicine. During the last eight years ISD is collaborating with HP Labs on the development of multi-camera pixel synchronized video capture systems for augmented reality and homeland security applications.~~				
~~**Qualification of the key personnel**~~	~~**Stefanos Skoulaxinos** was born in Greece in 1980. He graduated from the Electronic Engineering Department from the University of Heriot-Watt, Edinburgh UK in 2001. He received his Master's Degree in Embedded Systems from the Electrical & Electronic Department from the University of Heriot-Watt UK in 2002. From 2002 to 2005 he undertook research in the same University, the topic being "Reliable Embedded Software-Hardware Co-Design as applied in a Wireless Application" for which he obtained an M.Phil. He investigated means of deploying formal verification techniques using the PIN model checker currently used by NASA. Since 2005, he is with ISD SA working on camera and microphone arrays.~~ ~~**Mr Efstratios Politis** was born in Greece in 1970. He obtained a BSc from the University of Newcastle upon Tyne from the Department of Computer Science, and then proceeded to obtain a MSc from the University of Edinburgh. Since 2002 Estratios has been employed at ISD S.A. While working for ISD S.A. he has gained significant experience in all phases of embedded software's lifecycle by contributing to the design of SoCs targeting the consumer electronics market and multi camera arrays for security applications.~~ ~~**Mr Constantin Papadas** was born in Greece in 1966. He graduated from the Computer Science Dpt., Univ. of Crete, Greece in 1988. He received the Master Degree for his work on the reliability issues of MOS capacitors from the Inst. Nationale Polytechnique de Grenoble, Grenoble, France in 1991, and the Ph.D. Degree for his work on nonvolatile memory structures in 1993 from the same institute. Dr. Papadas is the main author or co-author of 34 publications in refereed international journals, 47 communications in referred international conferences with edited proceedings and he has also been awarded 9 US and Japanese patents.~~				

Organization	**Movation AS**	**Short Name**	**MAS**	**Partner #**	**12**
Country	Norway	**Logo**			
Type	Medium Enterprise				
Description	Movation is the leading independent resource center for open innovation in the Nordic. Movation helps start-ups and established companies to expand, extend and excel in their innovation activities. Movation was founded in 2006 by seven Norwegian companies, and was in 2009 transferred into an SME. Through Movation the partners created an arena where experts with different professional backgrounds and expertise exploited their knowledge in new ways to foster innovation. The seven partners who started Movation are among the leading ICT companies in Norway and have already shown that they can succeed with innovation. Det er Birdstep Technology, Comperio, Fast Search & Transfer (FAST), Nera Satcom, Opera Software, Radionor Communications og Telenor. It's Birdstep Technology, Comperio, Fast Search & Transfer (FAST), Nera Satcom, Opera Software, RadioNor Communications and Telenor. In Shield Movation will coordinate the contacts towards the Norwegian Industry, including the Norwegian Railway Authority and Telenor for the envisaged use-case. Movation will also disseminate and exploit the Shield results.				
Qualification of the key personnel	**Truls Berg** is a Norwegian entrepreneur, CEO and author, with more than 20 years experience in the IT industry. He holds a number of boards, is a frequently used speaker and is fixed chronicler of Computer World. He has so far helped to start up 10 enterprises, including the Component Software, Integrate and Comperio. In addition, he has assisted a number of other startup companies. Truls is the author of the book: Information Sea - a survival guide for tomorrow's knowledge workers. **Dr Josef Noll** is Chief Technologist in Movation, He is reviewer of the EU FP6 projects HYDRA and Pobicos, and evaluator of the EU's framework programme FP7, the Dutch IOP, the Austrian FIT, and the Cyprus research programmes. He is steering board member of Den Norske Dataforening (DND) "Semantic Web" and the "Mobile strategy" Special Interest Groups (SIG), co-editor of the Working Group 2 (WG2) White Paper "Semantic Services" and the cross-WP Outview User Profiles/Profiling for the Wireless World Research Forum (WWRF).				

Organization	Mondragon Goi Eskola Politeknikoa	Short Name	MGEP	Partner #	14
Country	Spain	Logo	MONDRAGON UNIBERTSITATEA		
Type	Public research Institute				
Description	Mondragon Goi Eskola Politeknikoa (Mondragon University's Faculty of Engineering) is a co-operative integrated in Mondragon Co-operative Corpora-tion which is a business group made of more than 250 companies and entities that incorporates eleven Research & Development Centres and the private corporative University (Mondragon University). The corporation has a long tradition participating in the E.U. Framework Programmes, since 1994. Our companies, R&D centres and University have participated in 140+ European projects leading 28. R&D activities constitute a key element for the ongoing updating and renovation of teachers' knowledge in line with the real situation of the business world, and play an important role in students' education. The main task of this group within the SHIELD project is focused on threat management and intrusion detection functionalities at communication level (including mobile ad hoc networking) and information correlation. On the other hand the Software Engineering Group complements Mondragon University's contribution by providing its expertise in Software Product Lines to enable the improvement of the evaluation of security, privacy and dependability requirements of the embedded software.				
Qualification of the key personnel	**Roberto Uribeetxeberria** obtained the PhD degree in Telecommunications from Staffordshire University (UK) in 2001. Previously he finished the BSc in Automatics and Industrial Electronics at Mondragon University (Spain) in 1999. He is nowadays working as lecturer/researcher in the department of Computing and Electronics in Mondragon University. His main research areas are data networks, computer security and embedded system security. He is the coordinator of the Telematics Group of the university and also coordinates the PhD degree program called New Information and Communication Technologies. **Urko Zurutuza** obtained the PhD degree in Computer Science from Mondragon University (Spain) in 2008. Previously he finished the Computer Engineering at Mondragon University (Spain) in 2004. He is nowadays working as lecturer/researcher in the Computing and Electronics Department in Mondragon University. His main research areas are network security, intrusion detection systems, honeypots and data mining applications. **Goiuria Sagardui** obtained the PhD degree in Computer Science from the university of the Basque Country (Spain) in 2000. Previously she finished the BSc in Software Engineering at Deusto University (Spain) in 1997. She worked as software engineer at ESI (European Software Institute) during 1999-2000. She is nowadays working as lecturer/researcher in the department of Computing and Electronics in Mondragon University. Her main research areas are software engineering: software product lines and MDE. She is the coordinator of the software engineering group of the university.				

Organization	**SELEX Communications S.p.A.**	**Short Name**	**SCOM**	**Partner #**	**15**
Country	Italy	**Logo**	SELEX Communications A Finmeccanica Company		
Type	Industry				
Description	SELEX Communications, a Finmeccanica company, is a Communications systems supplier for military and civil customers. SELEX Communications employs more than 5000 people worldwide, with offices and plants in Italy, the UK, USA, Germany, Turkey, Romania and South America. The Company's main business sectors involve design, production and supply of: Security systems and equipment to be used in civil and military communication networks; Land, naval and satellite communication systems and equipment, command and control systems, and integrated networks for land, naval and satellite defense for national security institutions and other governmental entities; Avionics equipment and integrated systems for communication, navigation; identification and mission control; government and Civil Communications for Professional and Telecom Operators where system has been implemented for fire departments, municipal police, harbors, civil defence, Italian highways, cost guard and railways networks. The characteristics of these products and the advanced technologies that are used in their production also allow their application and marketing in sectors other than defence, in which security and reliability are also fundamental requirements. Selex Communications research team, with over 1200 highly skilled engineers working in its Research and Development laboratories.				
Qualification of the key personnel	**Dr. Marco Cesena** fully graduated in Electronic Engineering at University of Genoa in 1991. From 1992 to 1998 he worked in Technical Directorate of Marconi S.p.A. as responsible for the FPGA development methodologies and PCB Simulation. From 1998 to 2006 has been manager of the Technical Directorate Methodologies Team of Marconi Mobile (after Selex Communication), committed to maintain the development company environments and methodologies up to date, giving support to the design teams and providing the designers training on the advanced design methodologies. Since 2006 is working as Design Methodologies Mngr. in the Technology department of Selex Communications. Since 2003 is also Mentor of the Electronic Systems Design Group of the Finmeccanica Technological Communities (MindSh@re).				

Organization	**THYIA Tehnologije d.o.o.**	**Short Name**	**THYIA**	**Partner #**	**20**
Country	Slovenia	**Logo**	Thyia Technologies		
Type	Medium Enterprise				
Description	THYIA TEHNOLOGIJE d.o.o. is SME, a spin-off of Thyia Technologies Sarl, Iskra Zascite d.o.o., and Industrial Electronics SPIN d.o.o. THYIA's core business activities are developing new technologies and products, R&D, networking, engineering and consulting. In the area of Emerging technologies THYIA is challenging the latest R&TD FP7 projects in different fields such as the future home networks, civil and military sensor networks with huge number of nodes that will be used for surveillance and other military applications. Therefore, THYIA interest is in various fields related to the Wireless Radio Communications and sensors, RFID, UWB and sensor networks. GPRS/UMTS, WiFI, WiMAX, Flexible Radio & SDR, Cognitive Radio (CR), channel propagation, modulation & coding, RF front-end, baseband processing, adaptive antenna arrays, signal processing, thrust, security and safety aspects, EMC, intelligent power management, and standardisation activities. THYIA will contribute in SHIELD in some key areas: developing a unified view on embedded security by analysing the functional requirements for embedded systems, especially those related to basic security functions, secure user identification by innovative multi-technology smart cards and RFID devices, temper resistance, secure network access, storage, and content security. The innovation envisioned are related to an intelligent pyramided security approach, which will have self-diagnostic functionalities and adaptive security mechanisms that optimise the overall performance of embedded devices.				
Qualification of the key personnel	**Dr. Spase Drakul** is CEO of THYIA. His research interests and expertise are broad in Telecom sectors and Management. In particular for SHIELD he will contribute as architect in different security areas related to sensor, sensor networks, wireless technology, interoperability aspects, SW & HW architecture, system requirements, specifications, user scenarios and business models. For overall SHIELD R&D activities he will assist the partners with expertise in wireless systems and networks and new multi-technology security solutions for embedded devices- **Dr. Gordna Mijic** is CTO of THYIA working in the fields of 3G & 4G technologies, microwave technologies, Wireless Grid, WiFi, WiMAX, UWB, SDR, MIMO, sensor technologies, homeland security, TETRA, TETRAPOOL, C4ISR. In the last 8 years she actively participated in the standardization activities for UMTS and UWB as well as other latest technologies development at ETSI, 3GPP and ITU.				

Organization	**Tecnologie nelle reti e nei sistemi S.p.A.**	**Short Name**	**TRS**	**Partner #**	**21**
Country	Italy	**Logo**	Tecnologie nelle Reti e nei Sistemi T.R.S. SpA		
Type	Medium Enterprise				
Description	TRS is an Italian System House and Software House. Across the years TRS has become an experienced company in designing, developing and installing complex architectures such as Air Traffic Management and Monitoring & Management systems.At the end of 2007 TRS employed approx. 150 high skilled professionals; more than half of them are university graduates. TRS's financial statements for the year 2007 show a production value of 10 millions euro with a significant growth vs. 2006. TRS knows the importance of a well-structured and disciplined Quality Management System, mandatory to provide control over project management. Our accredited ISO9001 Quality Assurance System is certified since 1994. Since 2002 TRS is ISO9001:2000 Quality Assurance System compliant. Documented quality system, ensures that TRS meets the expectations of our customers with quality. Products and Services delivered in a prompt and professional manner.				
Qualification of the key personnel	**Ing. Andrea Taglialatela** graduated in Electronic Engineering at University of Naples in 1997. Before joining TRS, he has worked in different Companies (Etnoteam, EDS) and has been involved in Projects in the Telco area as Project Manager and Senior Software Engineer (Vodafone, Marconi Mobile). From 2004 he is a Project Manager at TRS playing different roles in a number of activities. He is Project Leader and coordinator for TRS activities in Coflight. He is Project Leader in Multilateration System for the analysis and development of the Central Processing Function (CPF), devoted to Target Location and Identification based on Mode-S Short/Extended Squitter elaboration. He is Project Leader in the development of AVMS for ASAP (Airport Vehicle Management System for Advanced Service in Airport) ADS-B router services. He is Project Manager in ONTOMAN, a Research Project related to interoperability support among heterogeneous systems based on domain Onthologies and semantic reconciliation. He is Project Manager for the Instructor Training Desk of the PAAMS (Principal Anti Air Missile System) System. He is Responsible of Research Projects				

Organization	**Università di Genova – Dipartimento di Ingegneria Biofisica ed Elettronica**	**Short Name**	**UNIGE**	**Partner #**	**22**
Country	Italy	**Logo**	DIBE		
Type	Public research Institute				
Description	The Department of Biophysical and Electronic Engineering (DIBE) of the University of Genoa was founded in 1984 by researchers in Electronics, Telecommunications and Bio-physic fields. Department is one of the main Departments at Engineering Faculty of Genoa University. The Department joins research and didactic with expertise in design and development of systems and applications, as underlined by many contracts and collaborations with national and international enterprises and institutions (for instance FP5 REOST, FP6 TAMIRUT, and FP7 SEARISE). DIBE will cooperate with other partner for the definition, study and design of specific architectures requirements. Moreover, main activities will concern the contexts of environment awareness, self-reasoning, self-healing and learning capabilities aiming at improving SPD features of SHIELD platform at node and network transmission level and the definition of SPD metrics for the analysis of SHIELD architecture performances. Finally, DIBE will contribute in exploitation and dissemination phase through participation at international workshops and conferences and through publication of achieved research tasks and results in relevant scientific journals. Some most relevant previous experience: SMART-PRIN 2005 Project, financed by the Italian *Ministry of the University and Research (MIUR)*, “Progettazione di un livello fisico intelligente per reti mobili ad elevata riconfigurabilità” regarding the study of mode identification algorithms for SDR terminals and the design of radiating elements for smart antenna systems. Project “Linee Guida per lo studio sulle attività di baseline verso lo sviluppo di prodotti della linea ‘Broadband Wireless’” ('07-'09) in cooperation with Selex Communications regarding the study of product requirements for WiMAX-802.16e based devices including adaptive modulation and coding.				
Qualification of the key personnel	**Prof. Carlo Regazzoni** received the “laurea” degree in Electronic Engineering and the Ph.D. in Telecommunications and Signal Processing from the University of Genoa, in 1987 and 1992, respectively. He is Full Professor at DIBE since 2006. Since 1990 he is responsible of the vIdeo & SIgnal Processing for telecommunications Group (ISIP40) area of the Signal Processing & Telecommunications Group (SP&T) at DIBE. **Dr. Mirco Raffetto** graduated “summa cum laude” in Electronic Engineering at the University of Genoa in 1990, and the Ph. D. degree in "Models, Methods and Tools for Electronic and Electromagnetic Systems" from the same university in 1997. At present, he is an assistant professor in the Department of Biophysical and Electronic Engineering, University of Genoa. **Mrs Marina Ottonello** received the "master degree" in Telecommunications Engineering at University of Genoa, Italy, in 2006. She is currently a PhD student in Information and Communication Science and Technology at the University of Genoa, Italy. Her research is mainly focused on software defined radio, cognitive radio and reliable transmission methodologies.				

Organization	**Università di Roma – Dipartimento di Informatica e Sistemistica**	**Short Name**	**UNIRO MA1**	**Partner #**	**23**
Country	Italy	**Logo**			
Type	Public research Institute				
Description	The University of Rome is by far the biggest and oldest University of the Italian capital. It hosts several faculties, which, in turn, are organized in departments. The department involved in the project is the "Dipartimento di Informatica e Sistemistica (DIS)" (Department of Computer and System Sciences) of the Faculty of Engineering. DIS was involved in several FP-5 projects, such as WINE (Internet architecture for wireless access in a LAN environment) and WINDFLEX (high-bit-rate flexible and configurable ad-hoc network). In the FP-6, DIS participated or is currently participating in the following projects: SATSIX, DAIDALOS I & II (Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimised personal Services), WEIRD, IMAGES (Integrated Multiservice Architectures for next GEneration Services) and EuQoS (End-to-end quality-of-service support over heterogeneous networks). In FP-7 DIS is currently involved in OMEGA (Home Gigabit Access), P2P-Next and MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures).				
Qualification of the key personnel	**Prof. Francesco Delli Priscoli** was born in Rome in 1962. He graduated in Electronic Engineering "summa cum laude" from the University of Rome "Sapienza" in 1986. He received the Ph.D. in system engineering from the University of Rome "Sapienza". Since 1991 he is working at the University of Rome "Sapienza" where, at present, he is Full Professor and lectures several courses. He has researched on nonlinear control theory, on access techniques, secure QoS, broadcast/multicast, and mobility procedures for the third and forth generation of mobile systems. He is the author of more than 100 technical papers on the above topics and holds 4 patents. **Dr. Vincenzo Suraci** was born in Rome in 1978. He graduated in Computer Engineering with 110/110 cum laude in October 2004 at the University of Rome “Sapienza”. He received the Ph.D. in systems engineering in the Department of Computer Systems Science of University of Roma “Sapienza”. He managed several Integrated Projects: the FP6 DAIDALOS I and DAIDALOS II projects and Celtic IMAGES project. He is currently managing the FP7 OMEGA project and working in FP7 MICIE project. **Mr. Andrea Fiaschetti** was borne in Rome in 1982. He graduated in Automatic and Control Systems Engineering at the University of Rome "Sapienza", in 2009. He was responsible for EU-IST 6FP SATSIX project. Currently he is responsible of the EMERSAT Project, funded by the Italian Space Agency. His study focus on control of complex system, security, and on network control and management, with particular attention to algorithms that aim at providing QoS over heterogeneous networks; his principal skill concern the use of OPNET Modeler tool by OPNET Technologies to test BoD algorithms and protocols for multimedia broadband Satellite systems and network applications. He is author of some papers on these topics.				

5.3 - Consortium as a whole

The SHIELD consortium comprises 5 manufacturers and system integrators (ASTS, ED, ETH, HAI, SCOM), 4 universities (MGEP, UNIGE, UNIROMA1, CWIN), 7 SMEs (THYIA, TRS, Tecnalia, ~~ISD,~~ AS, CS, MAS) and 2 Industrial R&D organizations (SESM, ATHENA). All partners are from EU Member States and thereof one from a new member state (Slovenia). Most partners are member of ARTEMISIA, while the others will soon start the procedure to join it.

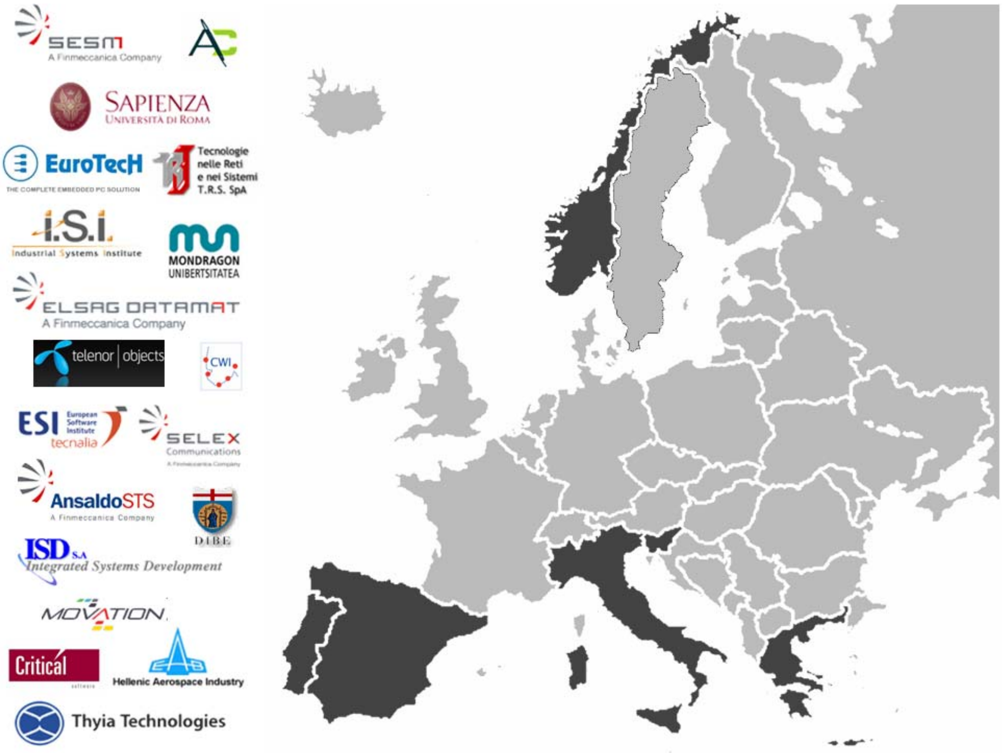


Figure 5.4 – SHIELD European Consortium

This consortium will mobilize the necessary critical mass at European level to achieve the objectives and to reach the impacts set for it.

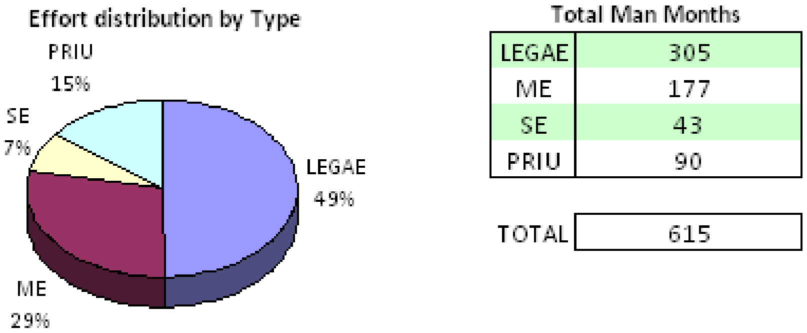
The participation by major European industry players in embedded systems security and dependability, who will assume leading roles in the project, ensures commercial exploitation of the results developed in the project. The leaderships cover all the main European countries involved in the project. It is once more a proof of the high level of European scope of the SHIELD team.

Responsibility	Beneficiary
Project Coordinator	Movation AS (MAS)
Technical Manager	ELSAG DATAMAT (ED)
WP 1 – Leader	Movation AS (MAS)
WP 2 – Leader	THYIA (THYIA)
WP 3 – Leader	SESM (SESM)
WP 4 – Leader	SELEX-COMMUNICATION (SCOM)
WP 5 – Leader	ELSAG DATAMAT (ED)
WP 6 – Leader	HELLENIC AEROSPACE INDUSTRY (HAI)
WP 7 – Leader	CWIN (CWIN)

Table 5.1 - Responsibilities of SHIELD beneficiaries

5.3.1 - SHIELD Consortium analysis

The SHIELD project aims to conceive and design an innovative, composable and high-dependable architectural framework. The SHIELD consortium has been setup to achieve this challenging objective.

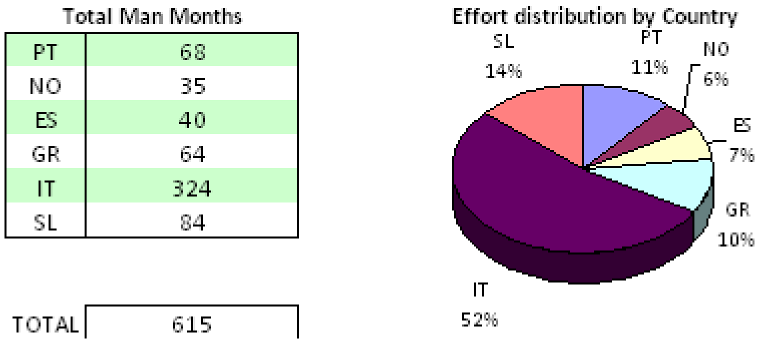


Total Man Months

LEGAE	305
ME	177
SE	43
PRIU	90
TOTAL	615

Table 5.2 – SHIELD effort distribution by type

Indeed Table 5.2 shows clearly that the project is leaded by an industrial partnership (85% of the effort) even if an important role is left to the universities and the research centres (15%) in order to bring the needed high innovation. In particular the large industries lead the project with the majority of the effort (49%). Great attention has been done to involve the SMEs: they have been selected among the most active and performing in the European and International SPD field and play a key role (36% of the overall effort) in the development of the new SPD technologies and their integration in the SHIELD platform.



Total Man Months

PT	68
NO	35
ES	40
GR	64
IT	324
SL	84
TOTAL	615

Table 5.3 – SHIELD Country involvement

It is worthwhile underlining that, according to the ARTEMIS concepts, the consortium comprises examples of the whole production chain. This is the case in particular of the Italian (52% of the total effort), the Norway (6%) and the Portugal (11%) clusters involved respectively in technologies development, and architectural design and final demonstration. Other two clusters from Greece (10%) and Spain (7%) are more focused on the development of the SPD technologies and methodologies and on their integration in the SHIELD platform.

From the manufacturer's point of view, SHIELD federates major “core-technology departments” from the European Industry both for hardware (SCOM, ETH), middleware/software (ED, HAI, CS) solutions for embedded system security and dependability and system integration (ASTS, CWIN)

The academic partners and R&D centres have a strong record and know how to conduct cutting-edge research and will disseminate the results through academic curricula. Leading academic experts for all the Embedded Systems layers under research by SHIELD are on board, opening the window to scientific committees of major conferences and fora. By setting up complex simulation tools at Node-, Cross- and network- layers, they will explore and evaluate the potential gain of the SHIELD Technology with respect to the state of the art.

5.3.2 - SME involvement

It is worth to note that SMEs play a key role in the project (36% of the overall effort, see Table 5.2) covering most of the challenging research aspects of SHIELD and guaranteeing a high level of complementariness.

More in detail the following research topics will be investigates: SPD middleware functionalities and interfaces (~~ISD,~~ CS, THYIA), cross-layer security (THYIA), SPD semantics (TRS), SPD metric definition and tracing (Tecnalia), intelligent nodes and smart transmission design and development (AS, CS).

5.3.3 - Complementarities

The SHIELD partners have been selected using a simple but effective criteria: to have the most representative European excellences (industries, universities, research centers and SMEs) in the field of SPD with the highest level of complementariness in order to cover each phase of the SHIELD project, from the design to the demonstration and to cover all the SPD challenges in the world of ES.

i) Sub-contracting:

Some activities within the SHIELD project will sub-contracted to other organizations in strict contact with the consortium members. The partners have already identified the main subjects of these sub-contracts: the mains are listed below.

SESM: Since some Mathworks © Products will be bought, there will be the need to pay for special courses on how to use this software. They will be:

- **Course Advanced VHDL Design Techniques**; The course highlights modeling, test-benches, RTL/synthesizable design, and techniques aimed at creating parameterizable and reusable designs. This course is held by Edaway s.r.l. Via Libertà 35 20019 Settimo Milanese (MI) ;
- **Course Best Practices for Maximizing FPGA Design Productivity**; it gives you the best ways to maximize productivity throughout the FPGA design cycle, while also maximizing design performance. Using recommended design methodology as a framework, you will see what is involved in preparing an FPGA design and what is required to implement it - from the creation of the design specification all the way to final sign-off. This course is held by Edaway s.r.l. Via Libertà 35 20019 Settimo Milanese (MI) ;
- **Course Design Planning Guidelines for High-Density FPGAs**; You will learn about : - Device Selection & Device Migration Planning - Programming/Configuration Method Selection - Early Pin Planning & I/O Analysis - Early Power Estimation - Planning Debug Options - Planning for Incremental Compilation - Early Timing Estimation; This course is held by Edaway s.r.l. Via Libertà 35 20019 Settimo Milanese (MI) ;
- **Course MATLAB & Simulink Training - Offered by The Mathworks**
- **Embedded Systems Software Development.** will learn the basic tool use and concepts required for the software phase of the design cycle, after the hardware design

is completed. Topics are comprehensive, covering the design and implementation of the software platform for resource access and management. Major topics include device driver development and user application debugging and integration. This course is held by Edaway s.r.l. Via Libertà 35 20019 Settimo Milanese (MI) and Politecnico di Milano Dip. Elettronica ed Informazione.

Subcontracting amount: 35,0 K€

ASTS: will subcontract part of work concerning the WP2 (Scenarios, user requirements and architecture design) and Task 6.4 (SPD Applications). In particular the subcontract amount is necessary for technical consultancy, outsourcing software development and deployment, support for on-the-field installation and assistance during testing on the trial vehicle and track. ASTS will show that its choice of supplier will be the 'best for the job' or, most likely, someone with whom it has a longer standing agreement for such work.

Subcontracting amount: 30,3 K€

ETH: Eurotech relies on some external services for the implementation of the hardware prototype of the power node. These activities cannot be performed inside Eurotech facilities for economic, strategic and practical reasons.

The following list describes the main activities that will be committed to external services for the prototyping:

1) Printed Circuits Board prototyping services:
    a. Simulation, placement and routing of electronic circuits;
    b. Printed Circuit Board manufacturing;
    c. Printed Circuit Board assembling, bring-up and debug;
2) Enclosure and Mechanics Prototyping service:
    a. Prototypes enclosure and mechanics mastering;
    b. Prototypes enclosure and mechanics manufacturing;
    c. External liquid cooling system design and manufacturing.

Motivations:

1a, 1b, 1c: Eurotech facilities are not equipped with instruments and tools to manage, manipulate and manufacture microelectronic circuits with the high level of integration required by the prototypes to be developed. The costs requested for purchasing this equipments and the cost to maintain them at the state of the art of microelectronic is too high for a prototyping activity.

2a, 2b: as the great part of the companies in this area, Eurotech facilities are not equipped with the machinery for enclosure and mechanics manufacturing. The cost of stereo litography systems, for example, and the limited amount of time they would be used in a prototyping activity make these equipments too expensive.

The previous activities will be committed to external services on which Eurotech tipically rely in its projects. The external services, depending on their availability, could be in example: Tecno77, 3D-Engineering, DAU, TTM, Multek, GDS, Ircona, etc..

The total budget for these activities is of 70K€.

~~*ISD*: intends to subcontract part of electronics design work to ASTUS SA, a company existing and organized under the laws of France. ISD has a frame collaboration agreement with ASTUS. In this particular case ASTUS will just implement and validate part of the electronics (i.e. no IPR will be generated).~~

~~Subcontracting amount: 70,0 K€~~

SCOM: specific implementation in HW/SW architecture of part of the Smart Node developed by SCOM, like

a. Sensing Structure
b. Identification and Modeling of the Communication Attacks
c. Attacks Recognition
d. Decisor for Countermeasure Strategy

will be subcontracted to Edaway S.r.l.

Subcontracting amount: 70,0 K€

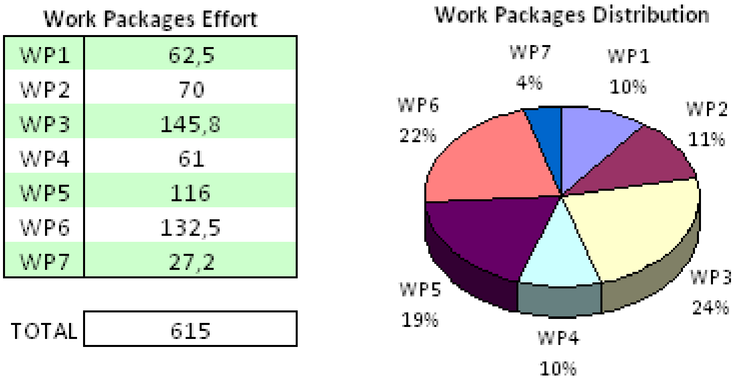
THYIA: Its employees are posted from the Switzerland to work in Slovenia. Due to this they have double employment status under E101 Article 14.2b of Council Regulation (EEC) No. 1408/71. Therefore, Thyia will pay this work under Consultancy agreement that already exsist between the companies Thyia d.o.o. (Slovenia) and Thyia Technologies Sarl (Switzerland)."

Subcontracting amount: 45,6 K€

5.4 - Resources to be committed

The SHIELD project aims at developing proof-of-concept prototypes and integrating them in a composable framework. Four (WP3-WP6) out of the seven work packages are each concerned with development and integration of novel technologies, counting on the 75% of the overall effort (see Table 5.4). In particular the hardware and firmware technologies in WP3 are more intensive and require the 24% of the effort. WP4 deals with SPD solutions at network level and benefit from the results of WP3 and WP5 thus is requires less effort (10%). WP5 develops innovative SPD solutions for middleware and develop a totally new SPD overlay, thus it needs 19% of the resources. WP6 focuses on the design of tools for the SPD lifecycle and the integration of composable technologies in the SHIELD platform and the pilot demonstrator. Thus WP6 is integral part of the R&D and requires a consistent effort (22%).

The system requirements, specification and design (WP2) takes the 11% of the project resources. The management of such project (see section 5.1 for details) has been taken into account and 10% of the total effort has been dedicated to it. The dissemination and exploitation activities use the 4% of the total effort to maximize the impact of the project at all level: SPD literature, certifications, standards and market.



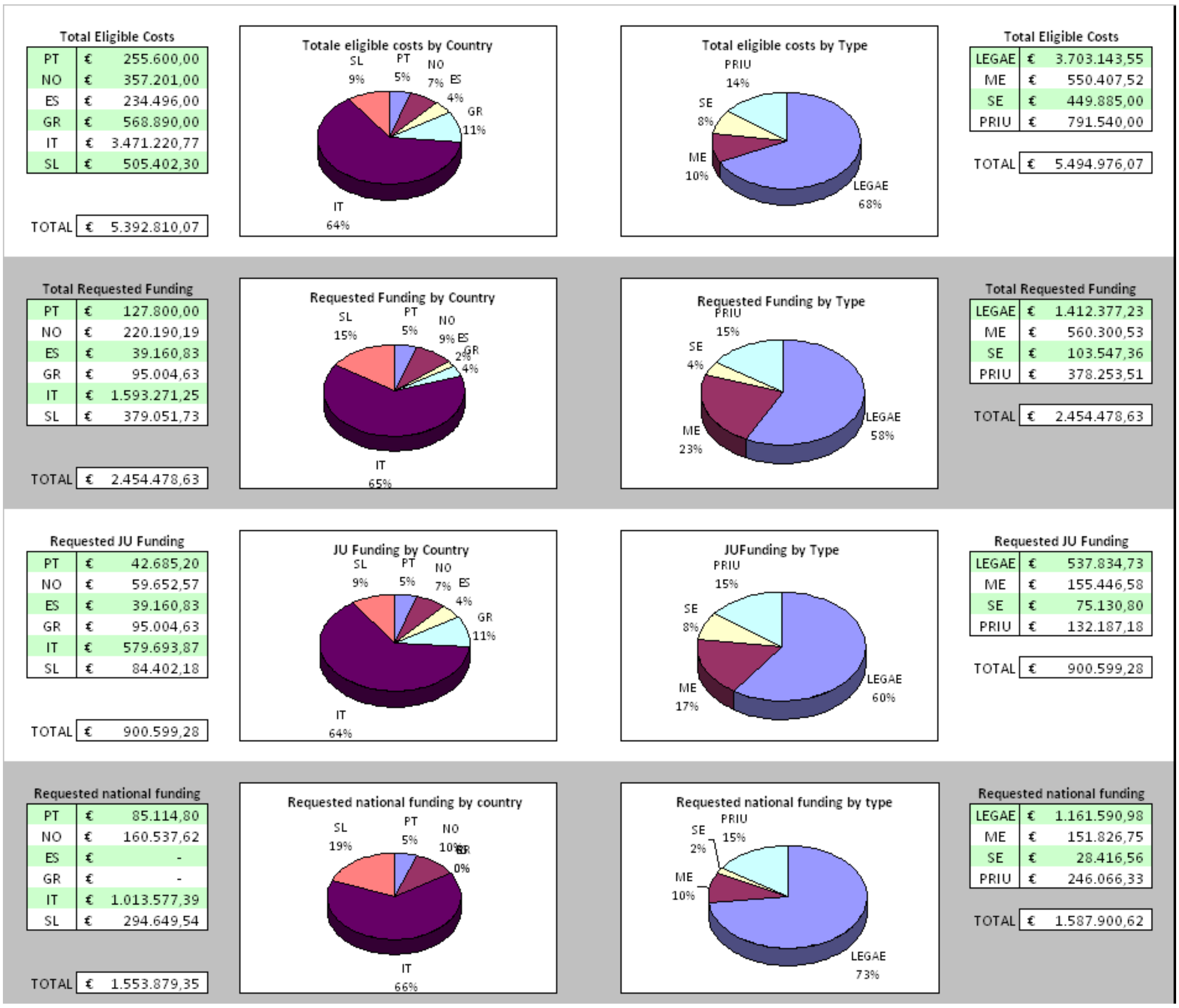
Work Packages Effort

WP1	62,5
WP2	70
WP3	145,8
WP4	61
WP5	116
WP6	132,5
WP7	27,2
TOTAL	615

Table 5.4 – Work Packages effort distribution

The challenging SHIELD objectives require an adequate budget, in order to be achieved. The project total cost is approximately 5,4 M€. The country distribution of the overall budget is almost the same as for the effort. The budget distribution by type sees the large enterprises to have the majority of costs (68%). It is due to the high effort of large enterprises but also to their higher costs associated to a man month. Indeed the man month costs for SMEs, universities and research centers are lower. SHIELD consortium will be founded with approximately 2,4 M€: 0,9 M€ will be provided by the JU and 1,5 M€ from the national funding.

Most of the resources requested are the personnel costs associated with this, but there are also substantial consumable costs associated with the hardware, firmware and software intensive work. The costs for equipment are minimized by the extensive use of the facilities already available to the partners. The costs are limited to items that ‘customize’ such equipment to specific project tasks. In addition equipment will be shared between partners, so that no funds are requested for duplicate resources.



Total Eligible Costs

PT	€	255.600,00
NO	€	357.201,00
ES	€	234.496,00
GR	€	568.890,00
IT	€	3.471.220,77
SL	€	505.402,30
TOTAL	€	5.392.810,07

Total Eligible Costs

LEGAE	€	3.703.143,55
ME	€	550.407,52
SE	€	449.885,00
PRIU	€	791.540,00
TOTAL	€	5.494.976,07

Total Requested Funding

PT	€	127.800,00
NO	€	220.190,19
ES	€	39.160,83
GR	€	95.004,63
IT	€	1.593.271,25
SL	€	379.051,73
TOTAL	€	2.454.478,63

Total Requested Funding

LEGAE	€	1.412.377,23
ME	€	560.300,53
SE	€	103.547,36
PRIU	€	378.253,51
TOTAL	€	2.454.478,63

Requested JU Funding

PT	€	42.685,20
NO	€	59.652,57
ES	€	39.160,83
GR	€	95.004,63
IT	€	579.693,87
SL	€	84.402,18
TOTAL	€	900.599,28

Requested JU Funding

LEGAE	€	537.834,73
ME	€	155.446,58
SE	€	75.130,80
PRIU	€	132.187,18
TOTAL	€	900.599,28

Requested national funding

PT	€	85.114,80
NO	€	160.537,62
ES	€	-
GR	€	-
IT	€	1.013.577,39
SL	€	294.649,54
TOTAL	€	1.553.879,35

Requested national funding by country
SL 19%
PT 5%
NO 10%
ES GR 0%
IT 66%
Requested national funding by type
PRIU 15%
SE 2%
ME 10%
LEGAE 73%

Requested national funding

LEGAE	€	1.161.590,98
ME	€	151.826,75
SE	€	28.416,56
PRIU	€	246.066,33
TOTAL	€	1.587.900,62

Table 5.5 – Budget distribution

Furthermore the project has been planned to leverage existing resources and technologies developed in other projects in order to minimize the resources requested for SHIELD. Each WP has carefully quantified their effort, taking this into account. All WPs have ensured that there is no duplication of effort between partners, with tasks properly integrated.

In addition equipment will be shared within the WP, and also across WPs, so the associated costs are minimized to interfaces and adaptors that are not available from any partner.

In summary, the strategy of the SHIELD partners is to ask only for the resources directly needed for the success of the project, with resources linked to measurement and production equipment being provided by that possessed by the partners.

Here it follows a detailed (indicative) list of the resources to be committed

#	Partners	Resources
1	SESM	[EQ] Mathworks, Matlab, Additional Packages (Simulink, DSP, etc.) - 30k€ [EQ] Altera Developer Kit Stratix Quartus included, Xilinx developer kit for Virtex4 - 15k€ [EQ] 4 Workstation with O.S., Office etc. - 10k€ [SUB] Subcontracting - 35K
2	AS	[CONS] Electronic components, substrates, chemical products for PCB creation, modules for power supply modules, software tools for prototype - 13k€ [OTH] Materials - 2K

#	Partners	Resources
3	ASTS	[OTH] 1 workstation to run the security management system simulator 3K [OTH] 1 rack server to run the pSHIELD middleware 5K [OTH] 1 rack POE Ethernet switch to connect the devices 0.7K [OTH] 1 intelligent IP camera to be used as a sensor 2K [OTH] 4 smart wireless sensors 2K [OTH] 1 gateway for wireless networks 1K [OTH] 1 rack UPS 0.8K [OTH] 1 wireless transceiver 1K [OTH] 1 intrusion detection junction box and related SW license 2K [OTH] 1 intrusion detection sensor 1K [OTH] 1 smart access control device 1.2K [SUB] Subcontracting 30.3K
4	ATHENA	*All necessary developing and computing equipment and consumables will be provided by LSI's own resources.*
5	CS	*All necessary developing and computing equipment and consumables will be provided by CS's own resources.*
6	CWIN	*All necessary developing and computing equipment and consumables will be provided by CWIN's own resources.*
7	ED	[EQ] 1 small size server for developing software and data storage systems - 2K€
8	Tecnalia	*All necessary developing and computing equipment and consumables will be provided by Tecnalia's own resources.*
9	ETH	[EQ] Electronics components (rugged custom rack and mechanics, cooling system components, high speed fpga and transceiver components, Intel Xeon CPUs and chipsets, high speed connection components, high speed memory, power circuitry components, high speed bus, solid state micro-SATA disk, sensor and control components, rugged connectors, etc.) and equipment (flash programmer, digital measurement devices, JTAG debug devices and cables, etc.) required to develop a power node prototype – 80 K€ [CONS] Intel (or equivalent) development kit, FPGA (Altera or equivalent) development kit, Operating System licenses, Linux development kit and licenses support, software CAD and tools for prototypes – 26 K€ [SUB] Subcontracting – 70 K€
10	HAI	*All necessary developing and computing equipment and consumables will be provided by HAI's own resources.*
~~11~~	~~ISD~~	~~[OTH] Special components to build, from scratch, cameras tailored for data fusion at 360 degree synchronization – 40K~~ ~~[OTH] Video grabber boards – 12K€~~ ~~[OTH] Video concentrator – 8K~~ ~~[OTH] FPGAs, memories, associated PCBs for prototypes - 8k€~~ ~~[OTH] Materials for population of two prototypes 7K€~~ ~~[CONS] General ICT consumables 15K€~~ ~~[SUB] Subcontracting – 70K€~~
12	MAS	*All necessary developing and computing equipment and consumables will be provided by MAS's own resources.*
14	MGEP	[CONS] Wireless communication components (wireless sensors, network devices) for construction of a heterogeneous mobile ad hoc network - 1k€
15	SCOM	[CONS] Generic consumables 3K€ [EQ] 1 servers for the HW and SW development - 7K [EQ] Set of licenses for the HW and SW design suites - 21K€ [SUB] Subcontracting – 70K€
20	THYIA	[EQ] Special equipment (e.g. embedded nodes) - 12K€ [CONS] other components (SW&HW test platform) for testing and prototyping - 15k€ [SUB] Subcontracting 45,6423 K€
21	TRS	[EQ] Computer platform - 2K€ [CONS] Programming & simulation license fee OS SW - 2 k€ [OTH] Laboratories 21K€

#	Partners	Resources
22	UNIGE	*All necessary developing and computing equipment and consumables will be provided by UNIGE's own resources.*
23	UNIROMA1	*All necessary developing and computing equipment and consumables will be provided by UNIROMA1's own resources.*

[EQ]	Durable Equipment
[CONS]	Consumables
[OTH]	Other National Costs
[SUB]	Subcontractig (see details in 5.3.3)

Table 5.6 – Resources to be committed for the SHIELD project

Table 5a Summary of effort and costs

Indicative breakdown of costs (in €)

This should be a breakdown table with common items of expenditure and, if necessary, additional customised columns

Partic. no.	Partic. short name	Personnel	Durable Equipment	Consumables	Travel & subsistence	Sub contracting	*(Other national categories)*	Indirect costs	Total costs
1	**SESM**	400.500,00	55.000,00	0,00	14.500,00	35.000,00	0,00	200.250,00	705.250,00
2	**AS**	84.000,00	0,00	13.000,00	0,00	0,00	2.000,00	16.800,00	115.800,00
3	**ASTS**	360.000,00	0,00	0,00	0,00	30.300,00	19.700,00	180.000,00	590.000,00
4	**ATHENA**	95.000,00	0,00	0,00	6.000,00	0,00	0,00	20.200,00	121.200,00
5	**CS**	204.000,00	0,00	0,00	9.000,00	0,00	0,00	42.600,00	255.600,00
6	**CWIN**	245.050,00	0,00	0,00	3.990,00	0,00	0,00	0,00	249.040,00
7	**ED**	392.805,00	2.000,00	0,00	0,00	0,00	0,00	196.402,50	591.207,50
8	**Tecnalia**	52.000,00	0,00	0,00	0,00	0,00	0,00	10.400,00	62.400,00
9	**ETH**	240.000,00	80.000,00	26.000,00	0,00	70.000,00	0,00	120.000,00	536.000,00
10	**HAI**	189.000,00	0,00	0,00	0,00	0,00	0,00	9.940,00	198.940,00
~~11~~	~~**ISD**~~	~~75.000,00~~	~~0,00~~	~~15.000,00~~	~~10.000,00~~	~~70.000,00~~	~~75.000,00~~	~~3.750,00~~	~~248.750,00~~
12 (C)	**MAS**	107.145,00	0,00	0,00	1.016,00	0,00	0,00	0,00	108.161,00
14	**MGEP**	46.080,00	0,00	1.000,00	0,00	0,00	0,00	9.216,00	56.296,00
15	**SCOM**	313.562,50	28.000,00	3.000,00	5.000,00	70.000,00	0,00	156.781,25	576.343,75
20	**THYIA**	410.760,00	12.000,00	15.000,00	22.000,00	45.642,30	0,00	0,00	505.402,30
21	**TRS**	68.679,60	2.000,00	2.000,00	0,00	0,00	21.000,00	13.735,92	107.415,52
22	**UNIGE**	83.328,00	0,00	0,00	0,00	0,00	0,00	41.664,00	124.992,00
23	**UNIROMA1**	160.008,00	0,00	0,00	0,00	0,00	0,00	80.004,00	240.012,00
Total		**3.526.918,10**	**179.000,00**	**75.000,00**	**71.506,00**	**320.942,30**	**117.700,00**	**1.101.743,67**	**5.392.810,07**

Table 5.7 - Summary of Effort and Costs

This page intentionally left blank

Annex A - Funding calculation forms

Annex A.1 (for partners established in ARTEMIS Member States)

Partner 1 SESM	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	573.750,00	184.933,05	33,3%
Experimental development	131.500,00	10.914,50	8,3%
Total	**705.250,00**	**€195.847,55**	
Total requested from the JU (16.7% of total above)	**117.776,75**		

Partner 2 AS	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	100.800,00	0,00	33,3%
Experimental development	15.000,00	0,00	33,3%
Total	**115.800,00**	**0,00**	
Total requested from the JU (16.7% of total above)	**19.338,60**		

Partner 3 ASTS	**Total eligible costs according to national rules (in €)**	**National Contribution requested (in €)**	**Percentage of the national subsidy to the beneficiaries applied for the calculation**
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	440.700,00	141.926,35	33,3%
Experimental development	149.300,00	12.391,90	8,3%
Total	**590.000,00**	**154.318,25**	
Total requested from the JU (16.7% of total above)	**€98.530,00**		

Partner 4 ATHENA	**Total eligible costs according to national rules (in €)**	**National Contribution requested (in €)**	**Percentage of the national subsidy to the beneficiaries applied for the calculation**
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	121.200,00	0,00	0,0%
Experimental development	0,00	0,00	0,0%
Total	**121.200,00**	**0,00**	
Total requested from the JU (16.7% of total above)	**20.240,40**		

Partner 5 CS	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	255.600,00	85.114,80	33,3%
Experimental development	0,00	0,00	33,3%
Total	**255.600,00**	**85.114,80**	
Total requested from the JU (16.7% of total above)	**42.685,20**		

Partner 6 CWIN	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	249.040,00	110.822,80	45,5%
Experimental development	0,00	0,00	50,0%
Total	**249.040,00**	**110.822,80**	
Total requested from the JU (16.7% of total above)	**41.589,68**		

Partner 7 ED	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	469.625,00	151.336,01	33,3%
Experimental development	121.582,50	10.091,35	8,3%
Total	**591.207,50**	**161.427,36**	
Total requested from the JU (16.7% of total above)	**98.731,65**		

Partner 8 Tecnalia	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	62.400,00	0,00	0,0%
Experimental development	0,00	0,00	33,3%
Total	**62.400,00**	**0,00**	
Total requested from the JU (16.7% of total above)	**10.420,80**		

Partner 9 ETH	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	501.000,00	161.684,97	33,3%
Experimental development	35.000,00	2.905,00	8,3%
Total	**536.000,00**	**164.589,97**	
Total requested from the JU (16.7% of total above)	**89.512,00**		

Partner 10 HAI	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	33,3%
Industrial/Applied Research	198.940,00	0,00	33,3%
Experimental development	0,00	0,00	18,3%
Total	**198.940,00**	**0,00**	
Total requested from the JU (16.7% of total above)	**33.222,98**		

~~Partner 11~~ ~~ISD~~	~~Total eligible costs according to national rules (in €)~~	~~National Contribution requested (in €)~~	~~Percentage of the national subsidy to the beneficiaries applied for the calculation~~
~~Fundamental/Basic Research~~	~~0,00~~	~~0,00~~	~~0,0%~~
~~Industrial/Applied Research~~	~~248.750,00~~	~~0,00~~	~~33,3%~~
~~Experimental development~~	~~0,00~~	~~0,00~~	~~8,3%~~
~~Total~~	~~**248.750,00**~~	~~**0,00**~~	
~~Total requested from the JU (16.7% of total above)~~	~~**41.541,25**~~		

Partner 12 MAS	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	33,3%
Industrial/Applied Research	108.161,00	32.015,66	29,6%
Experimental development	0,00	0,00	33,3%
Total	**108.161,00**	**32.015,66**	
Total requested from the JU (16.7% of total above)	**18.062,89**		

Partner 14 MGEP	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	56.296,00	0,00	33,3%
Experimental development	0,00	0,00	33,3%
Total	**56.296,00**	**0,00**	
Total requested from the JU (16.7% of total above)	**9.401,43**		

Partner 15 SCOM	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	487.088,75	157.056,44	33,3%
Experimental development	89.255,00	7.408,17	8,3%
Total	**576.343,75**	**164.464,61**	
Total requested from the JU (16.7% of total above)	**96.249,41**		

Partner 20 THYIA	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	505.402,30	294.649,54	58,3%
Experimental development	0,00	0,00	0,0%
Total	**505.402,30**	**294.649,54**	
Total requested from the JU (16.7% of total above)	**84.402,18**		

Partner 21 TRS	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	64.696,50	20.782,98	33,3%
Experimental development	42.719,02	3.545,68	8,3%
Total	**107.415,52**	**24.328,66**	
Total requested from the JU (16.7% of total above)	**17.938,39**		

Partner 22 UNIGE	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	124.992,00	39.996,36	33,3%
Experimental development	0,00	0,00	8,3%
Total	**124.992,00**	**39.996,36**	
Total requested from the JU (16.7% of total above)	**20.873,66**		

Partner 23 UNIROMA1	Total eligible costs according to national rules (in €)	National Contribution requested (in €)	Percentage of the national subsidy to the beneficiaries applied for the calculation
Fundamental/Basic Research	0,00	0,00	0,0%
Industrial/Applied Research	240.012,00	77.499,96	33,3%
Experimental development	0,00	0,00	8,3%
Total	**240.012,00**	**77.499,96**	
Total requested from the JU (16.7% of total above)	**40.082,00**		

i Participant number

Unfortunately on 26th January 2010 four Swedish partners have been withdrawn from the consortium for specific national reasons. Since most of the administrative documentation has been already produced with the old "partner numbers", we decided to keep the old numbers also in this updated Technical Annex, in order to keep it aligned with complementary documentation. Unused numbers are 13, 16, 17, 18. Now there are 19 partners

ii Project number

The project number has been assigned by the ARTEMIS Joint Undertaking as the unique identifier for your project. It cannot be changed. The project number **should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

iii Project acronym

Use the project acronym as given in the submitted proposal. It cannot be changed unless agreed so during the negotiations. The same acronym should appear on each page of the grant agreement preparation documents (part A and part B) to prevent errors during its handling. The **same acronym should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

iv Project title

Use the title (no longer than 200 characters) as given in the submitted proposal. Minor corrections are possible if agreed during the negotiations. The title should be understandable to the non-specialist.

v Starting date

In case a specific starting date is requested, insert this starting date of the project. During the negotiations the coordinator should present a written justification for the requested starting date. This starting date must be after the submission of the proposal and normally two months after the end of the negotiations.

vi Duration

Insert the estimated duration of the project in full months. Deviations from the duration in the original proposal must be justified in part B.

vii Call (part) identifier

The Call (part) identifier is the reference number given in the call or part of the call you were addressing, as indicated in the publication of the call in the Official Journal of the European Union. You have to use the identifier given by the ARTEMIS Joint Undertaking in the letter opening the negotiation.

viii Activity code(s) most relevant to your topic

Use as the first activity code the one set out in the letter opening the negotiation followed by the code(s) given in your proposal – if any. Changes are possible in case of material errors

ix Free keywords

Use the free keywords from your original proposal; changes and additions are possible. (maximum 100 characters including spaces, commas etc.).

x Abstract

Use the abstract from your original proposal and amend it to take account of several considerations. Use no more than 2,000 characters. The abstract should, at a glance, provide the reader with a clear understanding of the objectives of the project and how they will be achieved. The relevance of your project's objectives in the context of the objectives of the of the ARTEMIS annual work programme should be spelled out. This abstract will be used as the short description of the project for the public following signature of the grant agreement as well as in communications to the programme management committees and other interested parties. It must therefore be short and precise. It should not contain confidential information. Please use plain typed text, avoiding formulae and other special characters. If the project is written in a language other than English, please include an English version of the abstract in part B.

xi Maximum national contribution

Applicable for beneficiaries from countries that have concluded an administrative arrangement with the JU: subject to approval by the respective national funding authorities