# ARTEMIS JOINT UNDERTAKING

**Sub-Programme:**

ASP6: *Inter-networked ES for Security and Critical Infrastructures Protection*

**Industrial Priority:**

| # | 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: Collaborative Project, JTI-CP-ARTEMIS**

# Technical Annex

**Project Acronym:** nSHIELD

**Project Full Title:**
new embedded Systems arcHItecturE for multi-Layer Dependable solutions

**Grant Agreement No.:** 269317

**Date of Preparation:** May 1$^{st}$, 2011

**Version Number:** 2.2

**Date of Approval of Technical Annex by the Joint Undertaking:** 23/05/2011

**Call:** ARTEMIS-2010-1

**Project Start Date:** 01/09/2011

**Project Duration:** 36 Months

**Name of the coordinating person:** Luigi Trono (Selex Galileo – Finmeccanica)
**E-mail:** luigi.trono@selexgalileo.com

## List of participants:

| Part. No. * | Participant organisation name | Part. short name | Country | ARTEMIS Member state (Y/N) | Other EU Member or State/Ass. Country (Y/N) | National eligibility checked by applicant (Y/N) |
|---|---|---|---|---|---|---|
| 1 (Coord.) | Selex Galileo | SG | IT | Y | N | Y |
| 2 | Ansaldo STS | ASTS | IT | Y | N | Y |
| 3 | Acorde Technologies | AT | ES | Y | N | Y |
| 4 | ATHENA Research and Innovation Center | ATHENA | GR | Y | N | Y |
| 5 | ---- | --- | -- | - | - | - |
| 6 | Elsag Datamat | ED | IT | Y | N | Y |
| 7 | Fundacíon Tecnalia Research & Innovation | TECNALIA | ES | Y | N | Y |
| 8 | ESIS Norge | ESIS | NO | Y | N | Y |
| 9 | I.P.S Sistemi Programmabili - Eurotech Security | ETH | IT | Y | N | Y |
| 10 | Hellenic Aerospace Industry (Elliniki Aeroporiki Viomichana Anonymi Etaireia) | HAI | GR | Y | N | Y |
| 11 | Indra Software Labs | ISL | ES | Y | N | Y |
| 12 | Integrated Systems Development | ISD | GR | Y | N | Y |
| 13 | Movation AS | MAS | NO | Y | N | Y |
| 14 | Mondragon Goi Eskola Politeknikoa | MGEP | ES | Y | N | Y |
| 15 | Noom AS – Scandinavian Mobile Technology | NOOM | NO | Y | N | Y |
| 16 | Selex Communications | SCOM | IT | Y | N | Y |
| 17 | Security Evaluation Analysis and Research Lab. | S-LAB | HU | Y | N | Y |
| 18 | SESM scarl | SESM | IT | Y | N | Y |
| 19 | Swedish Institute of Computer Science | SICS | SE | Y | N | Y |
| 20 | T2 Data AB | T2D | SE | Y | N | Y |
| 21 | Telcred | TELC | SE | Y | N | Y |
| 22 | THYIA Tehnologije | THYIA | SI | Y | N | Y |
| 23 | Technical University of Crete | TUC | GR | Y | N | Y |
| 24 | Università degli Studi di Genova | UNIGE | IT | Y | N | Y |
| 25 | Università degli Studi di Udine | UNIUD | IT | Y | N | Y |
| 26 | Università degli studi di Roma "La Sapienza" | UNIROMA1 | IT | Y | N | Y |

## Project efforts, eligible costs and funding[1]:

| Participant no. | Part. short name | Total person months | Total Eligible Costs | Maximum National Contribution | Maximum JU contribution |
|---|---|---|---|---|---|
| 1(C) | SG | 136 | 1,737,950.00 € | 488,924.00 € | 290,237.65 € |
| 2 | ASTS | 36 | 448,800.00 € | 138,650.00 € | 74,949.60 € |
| 3 | AT | 64 | 386,903.00 € | 128,838.70 € | 64,612.80 € |
| 4 | ATHENA | 66 | 459,600.00 € | 382,846.00 € | 76,753.20 € |
| 5 | --- | 0 | 0.00 € | 0.00 € | 0.00 € |
| 6 | ED | 99 | 933,899.00 € | 275,915.99 € | 155,961.13 € |
| 7 | TECNALIA | 88 | 565,818.00 € | 188,417.40 € | 94,491.61 € |
| 8 | ESIS | 13 | 136,910.00 € | 45,591.03 € | 22,863.97 € |
| 9 | ETH | 50 | 300,000.00 € | 92,400.00 € | 50,100.00 € |
| 10 | HAI | 144 | 1,113,600.00 € | 370,828.00 € | 185,971.20 € |
| 11 | INDRA | 100 | 686,578.00 € | 159,972.00 € | 114,658.53 € |
| 12 | ISD | 72 | 553,000.00 € | 184,149.00 € | 92,351.00 € |
| 13 | MAS | 18 | 230,981.00 € | 76,916.00 € | 38,573.83 € |
| 14 | MGEP | 45 | 281,000.00 € | 93,573.00 € | 46,927.00 € |
| 15 | NOOM | 6 | 59,167.00 € | 19,702.00 € | 9,880.89 € |
| 16 | SCOM | 111 | 1,159,430.00 € | 329,760.19 € | 193,624.81 € |
| 17 | S-LAB | 108 | 621,500.00 € | 393,410.00 € | 103,790.50 € |
| 18 | SESM | 31 | 260,400.00 € | 86,713.00 € | 43,486.80 € |
| 19 | SICS | 26 | 286,130.00 € | 165,955.00 € | 47,783.71 € |
| 20 | T2D | 36 | 379,440.00 € | 60,710.00 € | 63,366.48 € |
| 21 | TELC | 9 | 94,860.00 € | 15,177.00 € | 15,841.62 € |
| 22 | THYIA | 143 | 1,014,024.00 € | 591,175.99 € | 169,342.01 € |
| 23 | TUC | 97 | 453,600.00 € | 377,848.00 € | 75,751.20 € |
| 24 | UNIGE | 60 | 467,706.00 € | 155,868.0€ | 78,106.90 € |
| 25 | UNIUD | 36 | 358,000.00 € | 108,714.00 € | 59,786.00 € |
| 26 | UNIROMA1 | 48 | 480,000.00 € | 159,840.00 € | 80,160.00 € |
| **Total** | | **1642** | **13,469,296.00 €** | **5,091,894.30 €** | **2,249,372.45 €** |

---

[1] Total eligible costs are determined according to the E2 forms received from the National Funding Authorities.

## Proposal abstract

The nSHIELD project is, at the same time, a *complement* and significant technology breakthrough of "pSHIELD", a pilot project funded in ARTEMIS Call 2009 as the first investigation towards the realization of the ***SHIELD Architectural Framework** for Security, Privacy and Dependability (SPD)*. The roadmap, already started in the pilot project, will bring to address SPD in the context of Embedded Systems (ESs) as "built in" rather than as "add-on" functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ES.
pSHIELD has covered the definition phase of this roadmap: nSHIELD will be in charge of the development and implementation phases. The SHIELD General Framework consists of four layered system architecture and Application Layer in which four scenarios are considered: 1) Railway, 2) Voice/Facial Recognition, 3) Dependable Avionic Systems and 4) Social Mobility and Networking.

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

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

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

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

In order to verify these important achievements, the project will validate the nSHIELD integrated system by means of relevant scenarios: (i) Railways Security, (ii) Voice/facial recognition , (iii) Dependable avionic systems, and (iv) Social Mobility and Networking

The project will have a great impact on the SPD market of the ESs. By addressing the reusability of previous designed solutions, the interoperability of advanced SPD technologies and the standardized SDP certificability, it is possible to estimate an overall 30% cost reduction for a full nSHIELD oriented design methodology. Additionally, for social mobility and networking scenario the expected market in few years will be 15% of 5 billion mobile users. Finally, this project by taking in consideration the current Directive 2009/125/EC and the future one motivate by conclusions of the Competitiveness Council of 28 May 2009 that pointed out "it is of particular interest to maintain strong R&D investments in high-tech industries in Europe, especially in manufacturing sectors with indispensable technologies," great social and economic impacts for European economy will be achieved.

## Table of Contents

## 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 |
| **BANs** | Body Area Networks |
| **BSNs** | Body Sensor Networks |
| **CDMA** | Code Division Multiple Access |
| **CHOP** | Configuring, Healing, Organazing, 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 |
| **IMA** | Integrated Modular Avionic |
| **IP** | Intellectual Property / Internet Protocol |
| **IPx** | Industrial Priority x |
| **ITH** | Internet of Things and Humans |
| **LBSN** | Location Based Social Networking |
| **MANET** | Mobile Ad Hoc Network |
| **MOSA** | Modular Open System Approach |
| **NMA** | Network Management Authority |
| **OLSR** | Optimized Link State Routing Protocol |
| **OTA** | Over-The-Air |
| **P2P** | Peer-to-Peer |
| **P3** | Peer-to-Peer-to-Place |
| **PPTMs** | Public and Privite Transportation Means |
| **QOS** | Quality of Service |

| | |
|---|---|
| **SBLs** | Street and Building Lights |
| **SMN** | Social Mobility and Networking |
| **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 |
| **UAV** | Unmanned Aerial Vehicle |
| **UCN** | Ubiquitous Computing Network |
| **U&PC** | Ubiquitous and Pervasive Computing |
| **UWCN** | Ubiquitous Wearable Computing Network |
| **WCN** | Wearable Computing Networks |
| **WLAN** | Wireless Local Area Network |
| **WPL** | Work Package Leader |
| **WWSN** | Worldwide Wireless Sensor Network |

This page intentionally left blank

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

## 1.1 - Relevance

This section highlights the relevance of the nSHIELD 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 nSHIELD contribution is discussed.

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

**SP6 - Inter-networked ES for Security and Critical Infrastructures Protection:** 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.

nSHIELD strategy is conceived to increase the technological development in the supply of Embedded Systems (ESs) technologies. To this aim, nSHIELD 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.

nSHIELD 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 nSHIELD solutions can be applied to any heterogeneous, possibly interconnected, managed and/or unmanaged Embedded Systems. In other words, nSHIELD 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 nSHIELD, 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 nSHIELD 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 nSHIELD architecture composability[2] relies on the so-called *SPD modules*. Indeed the nSHIELD architecture is composed by a mosaic of innovative SPD functionalities, each one

---

[2] "*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

included in a proper SPD module, *transparently* embedded into one of the considered layers. The nSHIELD 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 nSHIELD 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 nSHIELD 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. nSHIELD 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.

**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 nSHIELD 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, *nSHIELD 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 nSHIELD architecture proposes different level of dependability. If the component is nSHIELD-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 nSHIELD architecture reacts at the layer such components belongs to. Indeed, nSHIELD 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 nSHIELD 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, nSHIELD 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 nSHIELD 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 nSHIELD, the proposed solutions will be validated through proper test beds and demonstrators relevant to the four considered ambitious scenarios: **railway, recognition, avionics and social mobility**.

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 nSHIELD 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

nSHIELD 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 nSHIELD 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 a 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 nSHIELD project with respect to the ARTEMIS Targets. The correspondent impact of nSHIELD for each ARTEMIS target is instead detailed in Section 4.1.

**AT1 - Reduce the cost of the system design.**

The definition of the nSHIELD 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 nSHIELD-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 nSHIELD: 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 nSHIELD results.

# Section 2 - R&D innovation and technical excellence

## 2.1 - Concept and objectives

The nSHIELD 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, perceiving the strategy to be the first step towards SPD certification for the future ES, throughout an holistic approach.

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 nSHIELD 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 - From pSHIELD to nSHIELD

As already mentioned in the abstract, the nSHIELD basic concepts are currently under investigation in the ongoing pilot project **pSHIELD** (contract n° 100204), started on 1$^{st}$ June 2010 and ending on 31$^{st}$ of May 2011, coordinated by SESM (Finmeccanica Group).

pSHIELD is a reduced R&D project addressing the basic concepts of nSHIELD framework and participated by the core/key partners of the nSHIELD consortium (about 75% of the partners are in common). Its short duration (12 months) allows it to slight overlap the start of nSHIELD project, in order to guarantee liaisons and input/output exchange.

Since it is a pilot project, pSHIELD wants to investigate and validate a <u>reduced but still consistent and coherent</u> set of innovative concepts behind the nSHIELD philosophy (see next paragraphs), in a restricted scenario with a restricted (<u>but significant</u>) consortium.

The pilot has been foreseen to be a pioneer investigation to be enhanced with R&D activities that would have been proposed in the future ARTEMIS Calls: <u>nSHIELD is one of them. In fact nSHIELD will bring the nSHIELD framework from "theory to practice" and will allow ARTEMIS to have a return from the research started (and already funded) in the pilot project</u>. Continuity with the past is given by the coordinator: Selex Galileo (Finmeccanica Group), by the consortium and by the basic underlying concepts and objectives (see next paragraphs). The novelty and improvements are given by new partners and new (and more consistent) application scenarios.

In the following paragraphs the description of the above mentioned concept and objectives are given with high details, while in Paragraph 2.1.4 - the punctual difference between the pSHIELD and nSHIELD are carefully provided.

About the (complex) terminology, at this point should be plain the distinction:

- SHIELD: the framework and concepts to address SPD
- pSHIELD: the pilot project for initial nSHIELD investigation
- nSHIELD: the new project for improving and realizing nSHIELD

Anyway, from this point forward we will use the word nSHIELD both from the framework and the new project and the word pSHIELD for the pilot.

## 2.1.2 - nSHIELD Concepts

The leading nSHIELD 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.
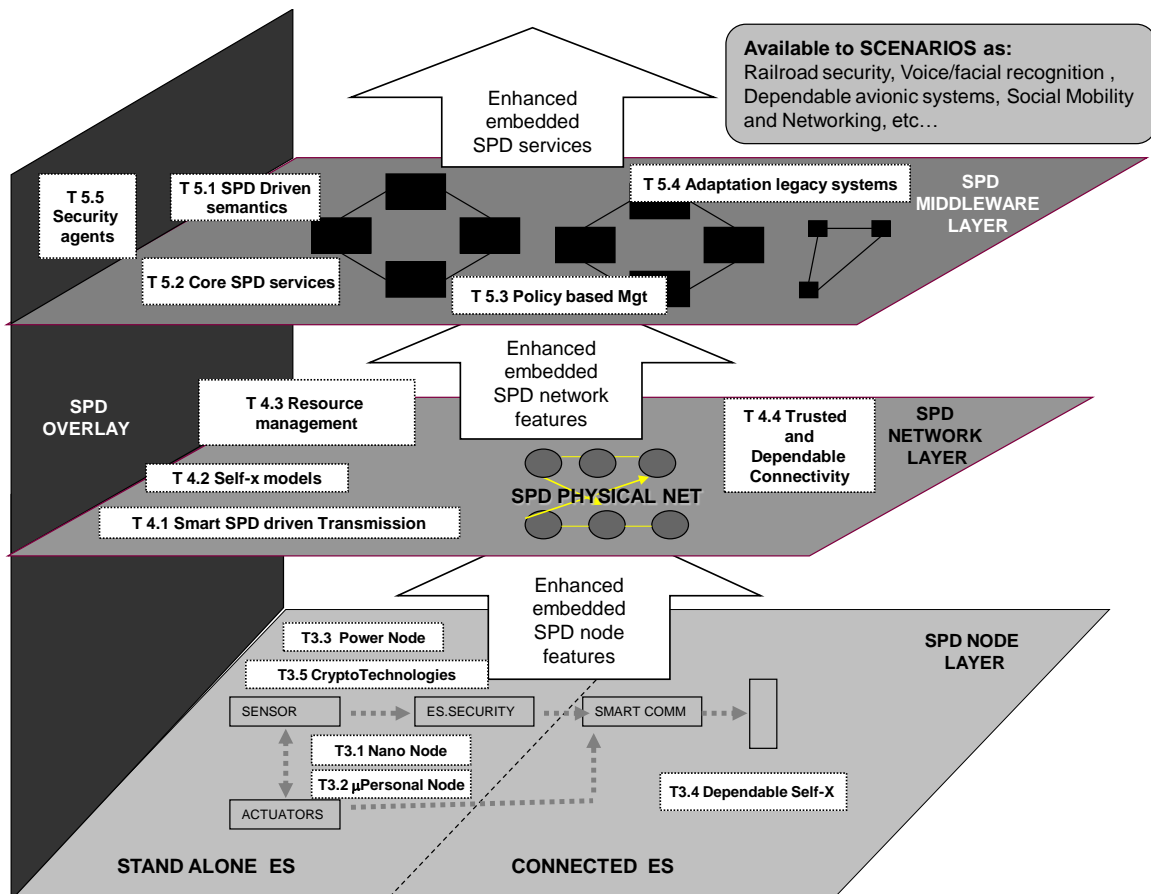


**Figure 2-1 - nSHIELD functional architecture overview**

Figure 2-1 shows how these ambitious goals can be obtained through the nSHIELD 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 nSHIELD 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 nSHIELD SPD requirements in a scalable and interoperable way. In particular nSHIELD 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 nSHIELD 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.

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 four application scenarios, 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 scenarios (railway, recognition, avionics, social mobility). 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 nSHIELD reference framework by using both the developed methodologies and tools, as well as the lifecycle support.

## 2.1.3 - nSHIELD Objectives

The project main objective is to conceive and design an 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. Four scenarios have been carefully selected in an industry exploitation perspective, in order to cover a wide and significant view of the foreseen industrial needs:

- dependable surveillance systems for urban railways security,

- dependable system for voice/facial recognition,

- dependable avionic system ,

- social mobility and networking dependable system.

The proposed ambitious application scenarios correspond to future product and services markets that are expected to exhibit fast growth rates due to socio-economic trends.

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

### 2.1.3.1  nSHIELD System Architecture

Figure 2-2 shows the preliminary nSHIELD System Architecture (SA) highlighting in grey the parts which will be specifically conceived, designed and implemented in the nSHIELD project.
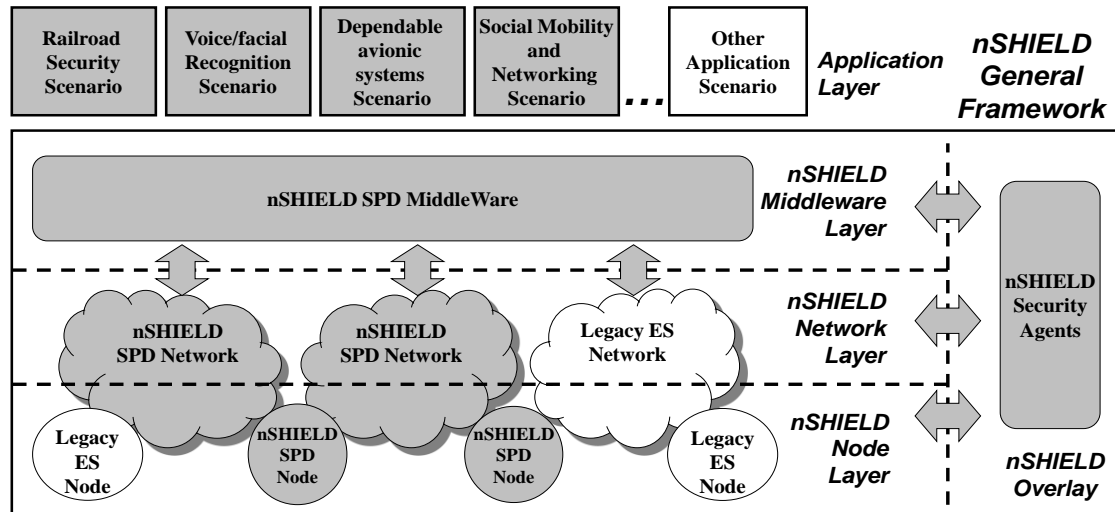


**Figure 2-2 - nSHIELD Architectural View**

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

### 2.1.3.2  nSHIELD 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 nSHIELD architecture will be conceived even to work in conjunction with legacy networks and nodes not provided with nSHIELD SPD modules.

### 2.1.3.3  nSHIELD seamless approach

The nSHIELD SPD functionalities will be conceived to be seamlessly introduced in the existing embedded systems. In particular, such functionalities will be embedded in nSHIELD 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 nSHIELD SPD functionalities which can be dynamically enabled/disabled and, in case of activation, properly configured following the decisions of the nSHIELD Overlay (see the next issue).

### *2.1.3.4  nSHIELD composability*

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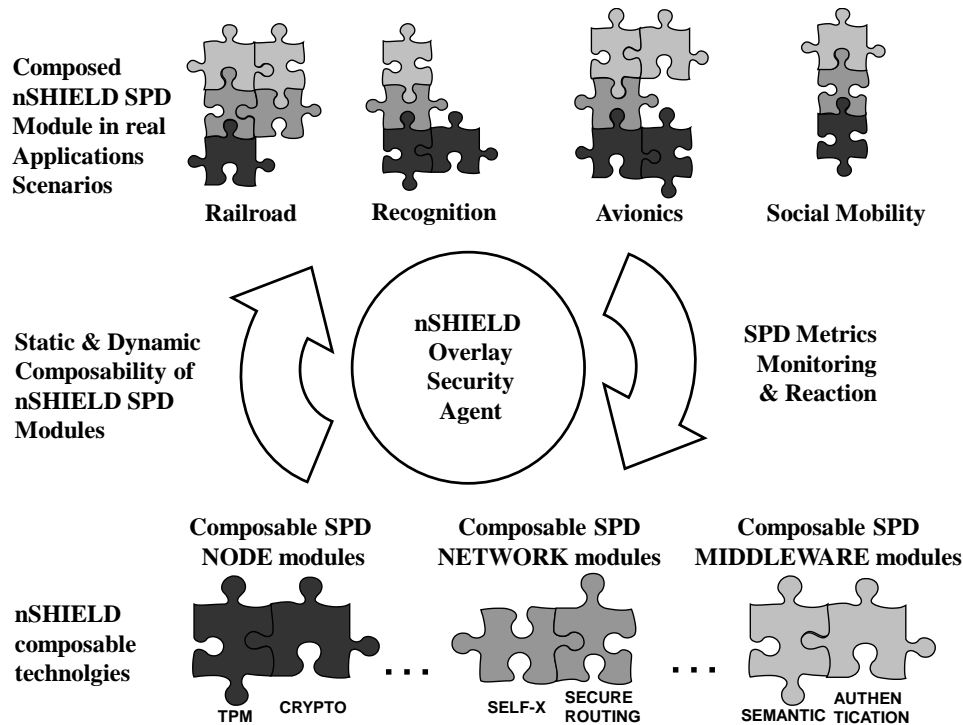


**Figure 2-3 - nSHIELD composability concept**

As shown in Figure 2-3 the nSHIELD 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: trusted platform module (TPM) and cryptographic techniques (CRYPTO). Modules belonging to different SPD layers (node, network or middleware) can be composed statically or dynamically by the nSHIELD overlay. Single nSHIELD 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.

### *2.1.3.5  nSHIELD innovative SPD functionalities*

Starting from the state of the art, nSHIELD will propose <u>new SPD functionalities</u> 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 nSHIELD 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 nSHIELD 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

nSHIELD (and, hence, the percentage which will be made available to nSHIELD with no charge), will be presented in the next section.

### 2.1.3.6 nSHIELD overlay
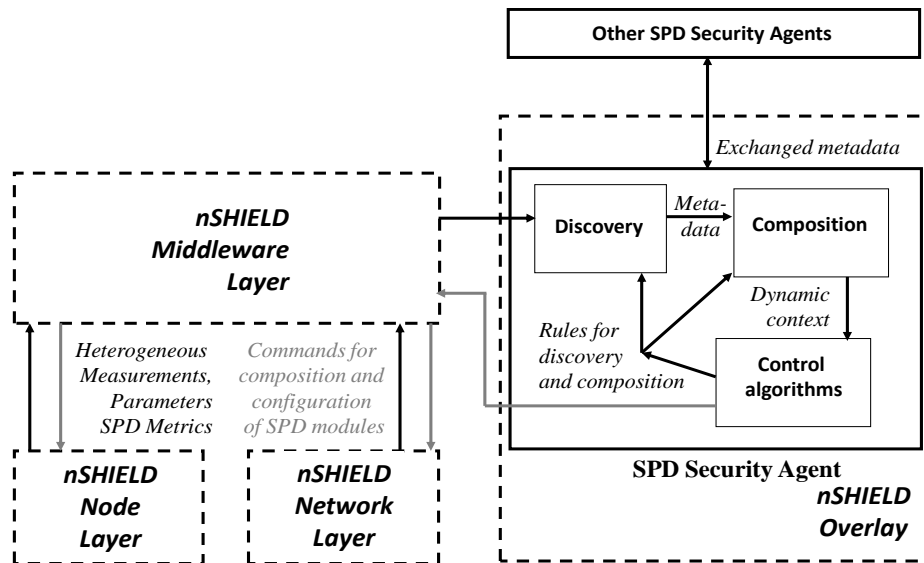


**Figure 2-4 - nSHIELD Overlay**

The nSHIELD project will design and implement <u>overlay security agents</u> 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.

### 2.1.3.7   nSHIELD SPD metrics

SPD metrics will be an nSHIELD key issue. First of all, the nSHIELD project will identify static and dynamic <u>SPD metrics</u> 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 nSHIELD 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 nSHIELD 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 nSHIELD 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, nSHIELD 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 nSHIELD framework in terms of required SPD levels independently from a specific domain

| Problem dimensions / Classes | STATIC | | | DYNAMIC | | |
|---|---|---|---|---|---|---|
| | 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**

### 2.1.3.8   nSHIELD Applications to prove its effectiveness

The nSHIELD 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 ones actually achieved by implementing the SPD nSHIELD solutions; integrating them in a complete platform; testing such platform in the previously mentioned meaningful demonstrators carefully selected in an industry exploitation perspective in order to cover a wide and significant view of the foreseen industrial needs. The four demonstrators are related to the following application scenarios:

1. Railways security

2.   Voice and Facial recognition

3.   Dependable Avionic Systems

4.   Social Mobility and Networking

To have an idea of the composition of a demonstration scenario, the punctual analysis of one of these scenarios will be now provided.

EXAMPLE: The fourth use case deals with the social aspects of the envisaged reduction of carbon dioxide, in the area of personal mobility. The scenario addresses new forms for commuting and travelling, including CO2-neutral electrical transportation. Mobile (SMS)-based request and registration of a vehicle and NFC -based vehicle access are the key technological components, using embedded systems to keep control of the vehicles. Socialtainment addresses the social aspects of future transportation.
Commuting and work-related travel is a substantial part of this emission, and nSHIELD will provide the security, privacy and dependability solution to enable a change in mobility.

The project nSHIELD is considering SMN as a scenario of humans that are moving from one place to other by walking, using public means of transport or personal one, such a bicycle, car, etc, and they desired to communicate with other persons or things (here we are referring to the future **I**nternet of **T**hings and **H**umans, named here ITH). There will be two different sub-scenarios, indoor and outdoor.  Indoor sub-scenario is related to social mobility of people inside the houses, buildings, etc. Outdoor sub-scenarios is related to social mobility of people on the streets in cites/towns, villages, highways, and other roads. In the scope of SMN in the nSHIELD project we are aiming to present this as a common R&D area in which SPD play an extremely important role for a successful implementation of SMN scenario. Figure 2-5 illustrates how different filed will interact jointly in this scenario. There are four fundamental overlapping areas:

1.   new Street and Building Lights (SBLs),
2.   Public and Private Transportation Means PPTMs,
3.   the future Internet of Things and Humans (ITHs), and
4.   Ubiquitous and/ Pervasive Computing (U&PC)

that have a common one, i.e., SPD aspects that are considered in details in this project in which a common nSHIELD system architecture is composed of four layers: node, network, middleware and overlay, that play an important role in the implementation of SMN scenario. In SMN scenarios a focus will be given to intelligent systems and intelligent ICT, since intelligent street lighting is maturing and providing cost-effective approach to manage municipal street lighting. Even though several attempts that have tried to merge the two worlds could not reach the masses, experts expect that future mobile social networking systems possibly even exceed the success of their Internet bound counterparts. We believe that two key features are the user's permanent reachability and location awareness, which is called P3 (Pear-to-Pear-to-Place).
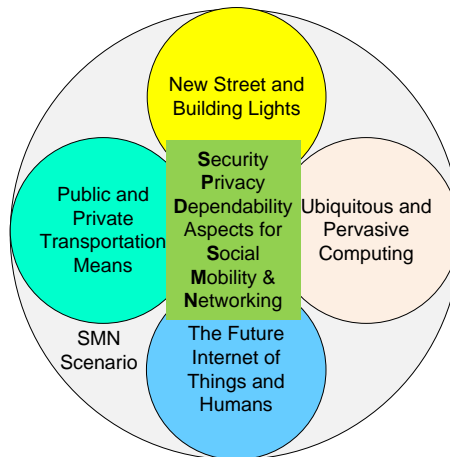
**Figure 2-5 - Social Mobility and Networking Scenario.**

There were 4.1 billion mobile phone users around the world in the year 2008 that surpassed the total number of Internet users. It is anticipated that at least 15% of mobile phone users will be involved in mobile social applications over the next few years.  The nSHIELD system architectural concept with emphasis on SPD aspects will contribute even more to a highest penetration of social networking. For that we need to integrate the old and new communication infrastructures. This lead to the creation of large and complex networks called real-life networks that include: electrical power grid, World Wide Web, the Internet backbone, collaboration and citation networks, and airline connection networks. Step-by-step, we are moving into a world of ubiquitous and pervasive computing (U&PC), Security, Trust, Privacy and Dependability Privacy (STPD) issues will be in focus more than ever before.

Finally, the nSHIELD project will <u>test the effectiveness</u> 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 ones actually achieved by implementing the SPD nSHIELD solutions; integrating them in a complete platform; testing such platform in the previously mentioned meaningful demonstrators (railway, recognition, avionics, social mobility), carefully selected in an industry exploitation perspective in order to cover a wide and significant view of the foreseen industrial needs.

### 2.1.3.9   nSHIELD improved technologies

On the light of the above concepts, from the nSHIELD 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 nSHIELD leads furthermore to include in the framework the development of innovative SPD technologies as requested by the market that will be developed within the project.

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**<br>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<br>- Lightweight HW and SW crypto technologies<br>- Asymmetric cryptography for low cost nodes<br>- Intrinsically secure ES firmware | - Automatic Access Control<br>- Data compression techniques<br>- Lightweight HW and SW crypto technologies<br>- Asymmetric cryptography for low cost nodes | - Power Supply Protection<br>- Self-re-configurability and self-recovery of sensing and processing tasks<br>- Easy and Dependable interfaces with sensors<br>- Embedded camera array auto-calibration and auto configuration techniques |
| **Network**<br>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<br>- Reputation based Secure Resource Management Procedures at transmission level | - Anonymity and Location-privacy techniques<br>- Dependable authentic key distribution mechanisms | - Waveform-agile and reliable transmission methodologies<br>- Distributed self-management and self-coordination schemes for unmanaged and hybrid networks |
| **Middleware**<br>This layer designs and implements secure resource management techniques, secure service management functionalite*s*, lifecycle support and highly-dependable interfaces. | - Secure Resource Management Procedures at middleware level<br>- Secure service discovery, composition and delivery protocols | - Secure Offline Authentication with mobile devices | - Policy-based SPD management |
| **Overlay**<br>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<br>- Situational-aware and Context-aware SPD | - Semantic representation of the dependability knowledge domain |

**Table 2.2 - nSHIELD SPD Features & Technologies to be improved**

## 2.1.4 - *nSHIELD vs pSHIELD*

The concept and objectives described up to now are the same for pSHIELD and nSHIELD, but they are investigated in completely different way. In order to better understand the complementarities of the two projects, a detailed description will be given:

*pSHIELD project is focused on:*

1) **Demonstrate composability:** The mechanism behind the composability is being investigated but limited to the design level and to static composability of well-known technologies

2) **New technologies:** A reduced set of the previous nSHIELD technologies is being used

3) **Innovative, modular, composable, expandable and high-dependable architectural framework:** the pilot project is being in charge of designing the core of this architectural framework, thus leaving to a future project its refinement and development. Moreover the interacting components are very few

4) **Metrics:** elementary metrics, reduced in scope, are being investigated in the pSHIELD project and used to validate the first basic functionalities of the framework

5) **Validate the nSHIELD integrated system in one application scenario:** the pilot project is validating the architectural framework in a single stand-alone and static scenario.

6) **Certification aspects:** are not being covered by the pilot project at all

*nSHIELD project will be focused on:*

1) **Demonstrate composability:** Composability of SPD functionality at different layers among different technologies will be refined and developed, taking into account performances and dynamic composability of any kind of technologies

2) **New technologies:** A wide set of technologies will be used to realise SPD composability and design guidelines will be provided to make any "nSHIELD compliant technology" composable with the others

3) **Innovative, modular, composable, expandable and high-dependable architectural framework:** nSHIELD will refine and develop the framework in a complex scenario

4) **Metrics:** A complete exhaustive set of metrics for SPD description will be refined and consolidated in the nSHIELD project and used to validate the whole functionalities of the framework

5) **Validate the nSHIELD integrated system in one application scenario:** the new project will validate the architectural framework by means of four (complex) scenarios relevant in an industrial perspective.

6) **Certification Aspects:** nSHIELD will be the first step towards SPD certification for future ES.

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

### 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 nSHIELD 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, nSHIELD 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, nSHIELD 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 *nSHIELD 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.

nSHIELD 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 nSHIELD progress beyond the state-of-the-art, is the design and the implementation of the <u>Overlay Security Agents</u> (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 <u>allowing the identification of possible SPD weak points in the secure service chain</u> which need further work. Even more, the <u>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.</u>

In the following section, additional nSHIELD 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 nSHIELD modules*: they will be assessed, <u>improved</u> to provided added value respectively in Security, Dependability or Privacy and adequately <u>refined</u> to be "nSHIELD" compliant, i.e. able to realize nSHIELD innovative functionalities (composability, overlay, measurement,…).

While the *"nSHIELD" 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

Trusted Computing (TC) is a technology developed and promoted by the Trusted Computing Group . The term is taken from the field of trusted systems and has a specialized meaning. In Trusted Computing context, the computer will consistently behave in expected ways, and those behaviours will be enforced by hardware and software[3,4]. In practice, Trusted Computing uses cryptography to help enforce a selected behaviour, and its main functionality is to allow someone else to verify that only authorized code runs on a system. This authorization covers initial booting and kernel and may also cover applications and various scripts. TC aims at increasing the security of the core Operating Systems. This begins at the lowest level of the platform with a controlled loading of an operating system and goes on level by level, verifying the process after each level. Just by itself TC does not protect against attacks that exploit security vulnerabilities introduced by programming bugs. The core components of a Trusted Computing System are the following:

(a) Trusted Platform Module, (TPM[5] ), which is a hardware component providing tamper resistant security functions. It is a secure crypto-processor that can generate and store cryptographic keys, generate pseudo-random numbers and that includes capabilities such as

[3] Trusted Computing Group. http://www.trustedcomputinggroup.org/
Stefik, Mark, "Shifting The Possible: How Trusted Systems And Digital Property Rights Challenge Us To Rethink Digital Publishing", 1997, http://www.law.berkeley.edu/journals/btlj/articles/vol12/Stefik/ html/reader.html
[4] Stefik, Mark, "The Internet edge: social, technical, and legal challenges for a networked world", 1999, ISBN: 0-262-19418-X
[5] TPM Main Specification, http://www.trustedcomputinggroup.org/resources/tpm_main_specification

remote attestation and sealed storage; (b), Secure Storage, provides a secure space for storing sensitive information, like cryptographic keys, licenses, etc.; (c), Authentication Boot, uses the TPM and provides mechanisms for monitoring boot process ensuring that no software attack has taken place in the kernel of Operating System; (d), Remote Attestation, provides the possibility to an external observer, e.g. a vendor, or system's manufacturer, to obtain information regarding correct operation of a remote system; (e), Virtualization, which provides mechanisms that allow multiple, concurrent virtual machines to run independently into the system.

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[6] 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. Furthermore a variety of initiatives and other projects related with the Trusted Computing Architectures have either been done or are on-going, showing the importance of these technologies in the context of security in embedded systems. Examples of such projects-initiatives are, (a) openTC[7] , which is a Research & Development European funded project focusing on the development of trusted and secure computing systems based on open source software; (b) European Multilaterally Secure Computing Base (EMSCB[8]) aims at developing a trustworthy computing platform with open standards that solves many security problems of conventional platforms; TOPAS[9] , works on providing the necessary framework for creating trusted – or trustworthy – personal devices, devices that are as familiar to their users as their mobile phones are and that can be used in security-relevant or sensitive application scenarios. The major objective of TOPAS is the development of a framework of Mobile Trusted Platforms that can be used on a variety of mobile and embedded systems, cost-effectively providing trusted computing technologies to these platforms, irrespective of the security features of the underlying system.

→The contribution of nSHIELD would cover a big part of those new requirements. In particular nSHIELD 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)

---

[6] ChangXiang Shen, HuanGuo Zhang , HuaiMin Wang, Ji Wang, Bo Zhao, Fei Yan, FaJiang Yu, LiQiang Zhang and MingDi Xu, "Research on trusted computing and its development", SCIENCE CHINA Information Sciences, vol. 53, pp. 405-433, 2010, http://www.springerlink.com/content/a44nt6xg44801533/
[7] open Trusted Computing, http://www.opentc.net/
[8] Towards Trustworthy Systems with Open Standards and Trusted Computing, http://www.emscb.com/
[9] Towards Trusted Computing for Embedded Devices, http://www.iaik.tugraz.at/content/research/trusted_computing/topas/

- Implement additional mechanisms to improve product endurance and increase product lifespan

To be in line with TCG guidelines, nSHIELD 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 nSHIELD 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.

## Access Control and Denial-of-Service

Access control and denial of service mechanisms are in charge of preventing non authorized/malicious entities to access the physical resources of the ES nodes that can be reached over the network.

There are several ways to implement 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 Wi-Fi

Denial of Service[11] 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. Large scale networks of embedded devices

---

[11] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-Service Attack Detection Techniques," *IEEE Internet Computing,* vol. 10, no. 1, 2006.

can comprise of various types and capabilities systems (nano, micro and power) which in conjunction with the diversified environments and the dynamic formulation pose an extra challenge in dealing with denial of service attacks. The problem is even more challenging in limited resources environments where the constrained protection capabilities together with the inherited characteristics (e.g. limited power, unattendance) constitute them more vulnerable[12].

Denial of service attacks that target networking resources can be mount on all different layers[13] and can have the form of jamming, resource exhaustion, misrouting, flooding and many more, including those that target the application layer. One should not exempt other denial of service attacks like unattended device tampering, attacks that cause permanent fatal damage which constitute the device inoperable, e.g. those that target firmware updates (phlashing)[14], and the ones that target valuable limited resources, e.g. memory. Denial of service due to extensive power consumption that is caused by unauthorised use of resources is another threat that has to be dealt with especially for nano and micro/personal nodes.

Incidents and research revealed the fact that poor design decisions in network protocols and operating systems can become a serious obstacle in DoS (and/or Distributed DoS) resilient systems and services. The IP protocol is vulnerable to such attacks due to early assumptions about trust of network nodes. Also, and basic software design methodologies don't take into account security requirements that would enable DDoS resilient services[15].

As a result, the majority of the aforementioned attacks originate from attackers who take advantage system vulnerabilites in conjunction with limited or poor authentication and access control mechanisms that can lead to unauthorised assignment of resources. Therefore, sound access control mechanisms and the correlative authentication mechanisms are vital for ensuring availability, provision of undisrupted services to legitimate users, and fair resources allocation to participating entities.

→nSHIELD aims to protect the distinct areas that attackers can mount denial of service attacks such as network layers, resources consumption, and location related data. It is planned to address the critical design steps that will enable secure node firmware/software deployment and updates as well as network protocols resilient to (D)DoS 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 (D)DoS 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).

The network protocols that will be designed as part of the nSHIELD infrastructure, will take into account the past flaws of Internet Protocol, quantify the notion of DoS resilience[16] and provide a set of measuring mechanisms that can evaluate the strength of a deployment

---

[12] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In IEEE Pervasive Computing, volume 7, pages 74–81, 2008.
[13] Wood A. D. and Stankovic J. A. "A taxonomy for denial-of-service attacks in wireless sensor networks", in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.
[14] Rich Smith - HP Labs, PhlashDance, Discovering permanent denial of service attacks against embedded systems, EUSecWest 2008.
[15] 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.
[16] Aad, I., Hubaux, J., and Knightly, E. W. 2008. Impact of denial of service attacks on ad hoc networks. IEEE/ACM Trans. Netw. 16, 4 (Aug. 2008), 791-802.

methodology or a newly developed service against those kinds of attacks. Security mechanisms should be inherited and part of the developed system and not patched to existing unsecure designs.

## **Cryptographic Technologies**

At node level cryptographic operations are expected to be performed by low-energy low-processing devices. A TPM is an example of a component providing HW/SW cryptographic technologies (see above for more details). The SW embedded on such a cryptographic component has a direct impact on both its size (through its code size and memory footprint: memory elements are taking an important part of the component surface), its costs (directly linked to the surface of the component), its speed (optimized code provide its computation results more quickly) as well as its power consumption (the quicker you can execute a set of instruction, the quicker you can put the component back in sleep mode where power consumption is reduced).

A certain amount of effort has already been spent on the question of optimization. The point is thus to make this improvement without negatively impacting the security of the chip.

The term lightweight crypto refers to algorithmic designs and implementations best suited to constrained devices (e.g., RFIDs, contactless smart cards, sensor nodes, mobile devices). A number of surveys[17][18] list the current state of the art in this area. In this task in particular we are interested in symmetric ciphers, stream ciphers and hash functions. These primitives could be used in a standalone fashion or as building blocks of lightweight crypto/security protocols (e.g., for authentication).

Two symmetric ciphers developed for minimal hardware requirements are DESL[19] and Present[20]. Researchers have put a lot of effort into porting more established algorithms, like AES[21], IDEA, TEA and the older DES, into low cost implementations. As a result, several mature block ciphers are available and their security (strength against a number of attacks) is well understood. On the other hand, stream cipher designs are still at the edge. A number of efficient hardware designs were developed in the context of the eSTREAM Project[22]. The security they provide on a constrained device is still quite risky. Hash functions designs too, are not lightweight so far[23]. The SHA-3 competition has improved our understanding substantially but still hashes based on block ciphers may have an advantage.

→nSHIELD will spend efforts on the code optimization (time and memory) and fine-tuning to improve the characteristics of the component while maintaining the high level of security of the component. Another aspect will consist also in reducing the requests of the SW on the HW resources.

→ As lightweight crypto has many dimensions and major challenges remain in cryptographic algorithm design there is no single optimal solution. For constrained devices, we will take into

---

[17] Bart Preneel, "Research Challenges in Lightweight Cryptography", WiSec 2009 invited talk.
[18] Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel, "A Survey of Lightweight-Cryptography Implementations", IEEE Design & Test, Volume 24, Issue 6, November 2007
[19] G. Leander et al., "New Lightweight DES Variants", Proc. Fast Software Encryption (FSE 07)
[20] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher", Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES 07)
[21] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES Implementation on a Grain of Sand," IEE Proc, vol. 152, no. 1, Oct. 2005, pp. 13-20
[22] The eSTREAM Project, http://www.ecrypt.eu.org/stream/
[23] Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, M.J.B. Robshaw, Yannick Seurin. "Hash Functions and RFID Tags : Mind The Gap", Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008), LNCS, Springer-Verlag, 2008

account the target platform's special properties when choosing cryptographic algorithms and also a number of tradeoffs. We will revisit protocols for constraint systems that are sound in theory but they cannot be used in practice because the primitives they are based on (e.g. hashes) cannot yet be efficiently implemented. In those areas we will investigate alternative constructions to achieve the same goals.

→ The expected outcome in this field is the reference implementation of an embedded cryptographic library that will provide, as part of the nSHIELD framework SDK, a set of optimized cryptographic algorithms for embedded devices and a standardized approach in SPD node software cryptographic operations. Special care shall be made in incorporating Side-Channel Attack (SCA) countermeasures within the optimized implementations such that the optimized implementations do not introduce new leakage channels.

→ A possible approach consists in the design and implementation of an embedded operating system 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).

## 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[24] (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 nSHIELD 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 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

---

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

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.

→nSHIELD 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[25] 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 data path 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 data path unit. The middle level is represented by the BCE that combines the data path 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

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,

---

[25] 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)

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[26] is a process where multiple un-calibrated images are used to directly determine internal camera parameters. In contrast to classic camera calibration[27], 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[28]. The second stage uses relatively unsophisticated, commonly known 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.

---

[26] 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.

[27] 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

→In this field, nSHIELD 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[29]. These methods will be developed to exploit the continuity of these images for tracking, geometric recovery, and compression.

Moreover the contribution of nSHIELD 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[30], 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.

## Easy and Dependable interfaces with sensors

There are two levels of interfaces at the SPD node used in telemetry. The first one (internal) comprises basic wired communication between the sensor electronics and the SPD node. Aside from the necessary bandwidth determined by the particular application (flowmeter, etc.) the most important parameter is power consumption because the number of battery-powered devices is still growing.

→Within this project interfaces and algorithms should be developed and communication protocols optimized in order to extend the minimal service period. The SPD node should be disposed as an integral part of the smart sensor and therefore the communication needs no encryption.

The second one (external) is the wireless interface of the SPD node. Continuous active operation of the SPD node, however, consumes significant amounts of power. Therefore the device is prone to require a larger power supply and/or more frequent change of the battery. Both larger batteries and more frequent battery charging are not viable alternatives in the industrial environment.

→This project will focus on the development of protocols for wireless node which don't need to remain constantly it in active mode and will optimize the life of power supply. Some partners will adapt the use of TPM in order to achieve low power consumption of the SPD node and high degree of security simultaneously. The developed prototypes of HW and SW modules will be verified using experimental facilities of one of the industrial partners.

## Data compression techniques

In several scenarios intelligent ES nodes generate large amount of data (sensors). These data have either to be processed locally and/or sent to other nodes for further processing. As these nodes often do not have the resources (computational and power) or complete enough

---

[29] "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).
[30] 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).

information about the extended environment to make proper processing, the latter case (involving data transmission) is very common.

Compression provides (at least) a two-fold advantage: Firstly, when the nodes need to store data locally, either because they cannot send them immediately or because the available bandwidth is not enough, it allows for more data to be stored in their limited local memory. Secondly, if the node sends the data wirelessly (a typical case), it consumes a large part of its power[31].

→On the other hand, compression requires higher processing power and introduces delays, especially for large amount of data[32]. To counter these, optimized implementations[33] are required without compromising the SPD properties of the node. nSHIELD will research an approach utilizing reconfigurable hardware which accelerates compression algorithms while consuming less power[34]. This approach enables also combing compression with self-re-configurability and self-recovery properties, as this type of hardware can be partially reconfigured[35], while less energy can be consumed in situations where compression is not needed or can be degraded without altering the node[36].

## 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[37]. Pervasive computing adds to mobile computing smart space, invisibility, localized scalability and uneven conditioning[38].

Ashok and Agrawal are giving inside on wearable computing platforms/nodes and technologies[39]. 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 information even when not in use, such as a new e-mail alert. Unlike intelligent wristwatches,

[31] N. Kimura and S. Latifi, "A Survey on Data Compression in Wireless Sensor Networks," *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC),* Vol. 2, pp. 8-13, 2005.

[32] S. Servetto, K. Ramchandran, M. Orchard, "Image coding based on a morphological representation of wavelet data", *IEEE Trans. Image Processing*, Vol. 8, pp. 1161- 1173, 1999.
K.W. Peng and J.C. Kieffer, "Embedded Image Compression Based on Wavelet Pixel Classification and Sorting", *IEEE Trans. Image Processing,* vol. 13, pp. 1011-1017, 2004.

[33] K. Barr and K. Asanović, "Energy aware lossless data compression," *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services* ( MobiSys)*,* pp. 231-244, 2003.
W. Bajwa, J. Haupt, A. Sayeed,  R. Nowak, "Compressive wireless sensing," *Proceedings of the 5th International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 134-142, 2006.
T. Arici, B. Gedik, Y. Altunbasak, L. Liu, "PINCO: a Pipelined In-Network Compression Scheme for DataCollection in Wireless Sensor Networks," *Proceedings of 12th International Conference on Computer Communications and Networks*, 2003.

[34] I. Papaefstathiou, "Titan II : An IPComp Processor for 10Gbit/sec network," *IEEE Design & Test (D&T)*, 2004.
J.L. Núñez, S. Jones, "Gbit/Second Lossless Data Compression Hardware",  *IEEE Transactions in VLSI Systems (TVLSI),* Vo. 11 (3), pp. 499-510, 2003.

[35] T. Todman, G. Constantinides, S. Wilton, O. Mencer, W. Luk, P. Cheung, "Reconfigurable Computing: Architectures and Design Methods." *IEE Proc.Computers and Digital Techniques,* Vol 152 (2), pp. 193–207, 2005.

[36] S. Banerjee, E. Bozorgzadeh, N. Dutt, "Physically-aware HW-SW Partitioning for Reconfigurable Architectures with Partial Dynamic Reconfiguration", *Proceedings of the 42nd annual Design Automation Conference (DAC)*, pp. 335-340, 2005.

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

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

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

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[40]. 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[41]. 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[42]. nSHIELD 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.

## Multipurpose node for telemetry

Wireless sensor networks[43] are mainly used for monitoring of events and collection of data. There are some important limitations with respect to their design like limited memory capacity of the network nodes, limited computing power and especially limited power consumption. The last mentioned property affects not only the range of computations but enforces also non-continuous operation of the transmitter and receiver of the node.
Limited power of the transmitter causes that the transmission of data can't proceed directly from the node to the control center but over intermediate nodes, what increases the danger of

---

[40] Dan Chalmers et al., Ubiquitous Computing: Experience, Design and Services," http://www-dse.doc.ic.ac.uk/Projects/UbiNet/GC/Manifesto/manifesto.pdf
[41] Lei Shu et al., "Sharing Worldwide Sensor Network," http://lei.shu.deri.googlepages.com/swdmnss2008CameraReady.pdf
[42] 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.
[43] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer Networks 52 (2008) 2292–2330.
D. Boyle, T. Newe, Security Protocols for use with Wireless Sensor Networks, Proceedings of the Third International Conference on Wireless and Mobile Communications (ICWMC'07).
Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, A survey of key management schemes in wireless sensor network, Computer Communications 30 (2007) 2314–2341.

the network attacks. It is necessary to use effective methods for data encryption and verification of data source origin. The optimized TPM module will help to minimize the power consumption for data encryption and secure key management.

The overall performance of the wireless sensor network will be optimized also using a sophisticated routing algorithm. The limited period of active state of the transmitter enforces the use of compression and aggregation algorithms.

The length of the runtime of the receiver has also substantial influence on the overall power consumption of the node. Sophisticated algorithms must be used at the link layer of communication like B-MAC, Z-MAC, etc.

Sensor networks can work in data collection mode or in query-and-collect mode. In both cases the real-time operation and event processing are required.

→Within this project UWB in cooperation with STM/CZ and other partners will develop a universal wireless node of sensor network. The node is composed from low power microcontroller, TPM module, non-volatile memory, receiver and transmitter and also the internal sensor interface. A part of the development will be the design and implementation of modular control program that contains modules for data aggregation and compression, routing, encryption, etc.

The developed structures and prototypes will be verified using experimental facilities of ELIS.

## 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 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. Symmetric ciphers serve mainly for message integrity checks, entity authentication, and encryption, whereas asymmetric ciphers additionally provide key-management facilities and nonrepudiation. Asymmetric ciphers are computationally far more demanding, in both hardware and software. The performance gap on constrained devices such as 8-bit microcontrollers is huge. For example, an optimized asymmetric algorithm such as elliptic-curve cryptography (ECC) performs 100 to 1,000 times more slowly than a standard symmetric cipher such as the Advanced Encryption Standard (AES) algorithm, which correlates with a two- to three orders- of-magnitude higher power consumption.

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

Among public-key algorithms, there are three established families of practical relevance: ECC, RSA, and discrete logarithms. ECC is considered the most attractive family for embedded environments because of its smaller operand lengths and relatively lower computational requirements. TinyECC[44], a software package providing ECC-based operations is intended for sensor platforms running TinyOS. Recently, even though an old idea, HyperElliptic Curve Cryptography (HECC)[45] is catching up[46]. The main benefit for curve-based cryptography e.g. ECC and HECC is that they offer equivalent security as RSA for much smaller parameter sizes. The advantages result in smaller data-paths, less memory and lower power consumption.

→The technology to be improved during the nSHIELD project shall provide an optimized hardware implementation for an ECC[47] or HECC public-key algorithm. A crucial parameter, that will affect the cost as well, will be the key sizws that maps the need for short, medium or long term security. Using a hardware-software codesign can substantially increase public-key performance with minimal area. However, in some situations public-key cryptography must

---

[44] TinyECC: Elliptic Curve Cryptography on TinyOS (version 1.0)
http://discovery.csc.ncsu.edu/software/TinyECC/
[45] N. Koblitz, "Hyperelliptic Cryptosystems", Journal of Cryptology, 1(3):129–150,1989.
[46] Junfeng Fan, Lejla Batina, Ingrid Verbauwhede, "HECC Goes Embedded: An Area-Efficient Implementation of HECC", Selected Areas in Cryptography 2008
[47] 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.

be implemented purely in software because changes to the hardware aren't possible. Hardware-software codesign seems to produce the best trade-off between size and speed for many pervasive computing applications[48]. As we mention earlier in this section, we will revisit protocols for constraint systems that are sound in theory but they cannot be used in practice because the primitives they are based on (e.g. public key crypto in this case) cannot yet be efficiently implemented. In those cases we will investigate alternative constructions to achieve the same goals.

→In the run of the nSHIELD 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 parametarized against side-channel attacks (SCA) – which might have a major impact on implementation cost - 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, depending on the potential applications and capabilities, shall reach a security level which will make it ready 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[49], CONFIDANT[50] and OCEAN[51] 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[52] 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[53] 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

---

[48] Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel, "A Survey of Lightweight-Cryptography Implementations", IEEE Design & Test, Volume 24, Issue 6, November 2007

[49] 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)

[50] 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)

[51] 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).

[52] 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).

[53] 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).

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.

→nSHIELD 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 upon personal observation. Using secondhand information can significantly accelerate the detection and subsequent isolation of malicious nodes in MANETS[54].

## 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[55]. The studies a new attack on the anonymity of location data is given here[56]. 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[57]. 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[58].

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[59].
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

---

[54] 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).
[55] 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.
[56] Philippe Golle and Kurt Partridge, "On the Anonymity of Home/Work Location Pairs,"
[57] Ge Zhong and Urs Hengartner, "Toward a Distributed k-Anonymity Protocol for Location Privacy," http://www.cs.uwaterloo.ca/~uhengart/publications/wpes08.pdf
[58] Marco Gruteser and Baik Hoh, "On the Anonymity of Periodic Location Samples," http://www.winlab.rutgers.edu/~gruteser/papers/gruteser_anonymityperiodic.pdf
[59] 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.

the problems[60]. For traffic monitoring system privacy, anonymity and location concerns are given here[61].

→It is demonstrated[62] 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 nSHIELD 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 nSHIELD scenarios and user requirements.

## SPD of Embedded Systems in Challenged Networks

Embedded Systems are an integral part of networks with unusual characteristics, like long communication delays, unpredictable link availability, and lack of end-to-end communication paths. Delay/Disruption Tolerant Networking (DTN) architectures are proposed to address requirements of such challenged environments. New protocols and techniques are needed for covering SPD in these environments; incorporating such mechanisms in the already constrained embedded systems is a complex and complicating issue. It is still an open problem in the research literature and projects funded by EU like Haggle  and N4C.

→nSHIELD will identify and explore the SPD requirements for utilizing the embedded systems in the challenged environments. Further, nSHIELD will extend the appropriate SPD mechanisms developed within the context of the project in such environments. Long-term secure storage of private information will be a core issue to be studied within nSHIELD.

## Reputation-based Secure Resource Management Procedures

Certain types of services, such as those provided in Wireless Sensor Networks, depend heavily on the integrity of the platform, applications and stored data for providing sound, per definition, services, such as measurements taken by the a sensor. Validating the integrity of the platform and assuring that this has not been compromised at the time of the service provision is important for the undisputed integrity of the network's functionality. The integrity of service requester platform is also important prior to allocating resources or revealing information. Care must be taken though so that secure resource management will not become a bottleneck in network performance and service provision.

WS-Attestation[63] is a recent mechanism developed by IBM that enables Trusted Platform Module remote platform attestation by means of web services. The proposed scheme

---

[60] 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),"
[61] 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.
[62] 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.
[63] White Paper: WS-Attestation: Enabling Trusted Computing on Web Services
 http://www.trl.ibm.com/people/sachikoy/papers/RT0695.pdf

leverages Trusted Computing Group[64],[65] and WS-Security technologies to "increase trust and confidence in integrity reporting".

→ In order to improve this technology, nSHIELD project will design an abstract layer that will consider device's security as a service, so that nSHIELD 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.

→ nSHIELD can examine the capacity of ESs to handle the WS-attestation mechanism for checking system's integrity prior to using its resources and sharing information with it. ES integrity assured through an adapted WS-attestation mechanism, when combined with robust authentication mechanisms can provide the necessary assurance to satisfy policy constraints. Moreover, it will elaborate the recently proposed WS-Attestation mechanism and propose the use of a reputation-based scheme which can work on top or in collaboration with WS-Attestation which explores the integrity mechanisms provided by the Trusted Computing Group.

→ Finally, it will work on ITEA2[66] project TECOM[67] results. TECOM seeks, among the others, to provide a solution in determining the level of trustworthiness of a participating device by applying the concept of trusted platform to real-time embedded systems.

## **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.

→nSHIELD 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.

---

[64] Trusted Computing Group, TPM Main Specification, http://www.trustedcomputinggroup.org/
[65] TCG Specification Architecture Overview, Revision 1.2 28 April 2004.
[66] http://www.itea2.org/
[67] http://www.tecom-itea.org

## 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[68] was marked by most tumultuous transformations in the information and communication technologies (ICT) domain, which are radically and rapidly changing our world[69].

An interesting overview on self-management and related projects from EC is presented here[70]. Autonomous and Autonomic Computing are presented as an interesting fusion for the future networks[71]. 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[72]. 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[73].

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 changing physical environment, and must serve the needs of a highly autonomous user group[74].

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

---

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

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

[70] 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

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

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

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

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

not an option decentralized self-management is required. Therefore, distributed energy resource self management is a challenge for nSHIELD framework on hybrid networks.

Rammig presented[75] 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.

## Dependable authentic key distribution mechanisms

Key distribution, either for initialisation[76] or re-keying, has been a challenging topic especially for limited resources environments. The majority of the schemes are symmetric key based with emphasis given on pre-deployment/pre-distribution while location aware and identity based approaches have also been proposed[77].

However, although energy efficient schemes have been proposed[78], key management based on secret keys has proven expensive and ineffective especially in dynamically formulated infrastructures. Attempts have been made to map key establishment techniques to applications but these were limited to the use of symmetric keys and on a framework level[79]. These inherited difficulties have led the community to invest more on public-key[80] (e.g., ECC) based solutions, as diverse capabilities of participating nodes require to consider constrains of nano devices. Most public-key based systems do not adequately consider the peculiarities of the environment where these systems operate.

Due to the novel introduction of asymmetric cryptography down to low cost distributed ES new innovative key distribution mechanism will be necessary. For authentication based on ECC it is not necessary that the verifying party is holding a secret key, it is possible to distribute authentic public keys via insecure channels. This allows, for example that the key database of a mobile node may be updated at any time, according to a pre-defined schedule or ad-hoc, even from different databases (e.g. mirror sites) either when the authenticating node is already running the authentication protocol or while in idle state.

As an example, a mobile node used for access control to the cruise liner in the maritime scenario, may be equipped with all expected keys for the next check in procedure to work efficiently in off-line mode when passengers arrive. In case of short-hand changes or booking updates an online connection may be provided, either by a local WLAN or through a mobile network (e.g. long term evolution - LTE - network). In contrast to today's distributed embedded systems - where updates of keys may only be handled via special secured communication channels - there is no need to establish a secure connection at that moment, since authenticity of the ad-hoc provided keys can be checked by one or more system

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

[76] Cynthia Kuo, Mark Luk, Rohit Negi, Adrian Perrig. "Message-In-a-Bottle: User-Friendly and Secure Key Deployment for Sensor Nodes", In Proceedings of the ACM Conference on Embedded Networked Sensor System (SenSys) 2007

[77] Barry Doyle, Stuart Bell, Alan F. Smeaton, Kealan McCusker, and Noel O'Connor. Security considerations and key negotiation techniques for power constrained sensor networks. The Computer Journal (Oxford University Press), 49(4):443–453, 2006

[78] J. Huang, J. Buckingham, R. Han, "A Level Key Infrastructure For Secure and Efficient Group Communication in Wireless Sensor Networks", First IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm) 2005, pp. 249-260.

[79] K.M. Martin and M.B. Paterson, An application-oriented framework for wireless sensor network key establishment, Proceedings of the Third Workshop on Cryptography for Ad-hoc Networks WCAN'07 (2007), Electronic Notes in Theoretical Computer Science 192(2), 31 - 41, 2008.

[80] Malan, David J., Matt Welsh, and Michael D. Smith. 2004. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. IEEE SECON 2004: 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks: 4-7 October, 2004, Santa Clara, California, 71-80. Piscataway, N.J.: IEEE.

signatures where the appropriate public keys of the system have been provided beforehand. Thus a number of variants of flexible and dependable key distribution mechanisms may be exploited.

→Secure and effective key distribution mechanisms necessary for establishing secure channels and exchanging secure messages among the communicating parties will be investigated considering the peculiarities of the use case scenarios. Low-cost key management will be in the center of this research while the services of third party solutions that can compensate for the shortage of embedded systems computational power may prove necessary for constrained environments. The chosen mechanisms will be closely related to policy requirements and satisfy the restrictions that participating systems impose. For instance, certain parameters of the chosen key, such as algorithm, length, entropy and use can be chosen based on the policy requirements that the node has.

## Secure service discovery, composition and delivery protocols

Services in distributed networks must be discovered, composed and delivered in a secure way. OASIS[81] (Organization for the Advancement of Structured Information Standards) has been working on web services provision and has progressively released related standards including the approved WS-Security, WS-Policy, WS-Trust, and WS-Secure conversation. Current trend and efforts to bring web services into embedded systems has brought forward the need for adapting these specifications so that the intricacies of those systems are taken into account.

Recently developed OASIS standards Devices Profile for Web Services  (DPWS[82]) and Web Services Dynamic Discovery (WS-Discovery[83]) specify the use of web services based communications in resource-constrained and ad-hoc environments dealing with issues like, discovery of devices in dynamic environments, security and integrity for discovery, metadata exchange and service usage. However, current standards only specify a minimum set of requirements that promote interoperability among diversified environments. As a consequence, further tuning is needed in order to account for the peculiarities of the targeted environments. Such work has been undertaken by SOA4D (Service-Oriented Architecture for Devices), an open source initiative which promotes the development of service-oriented software components adapted to constrained embedded devices[84].

Further work being carried out by the working group 6LoWPAN[85] considers the use of DPWS over low power wireless area networks that have adopted IPv6. However, this work is only taking its first steps and no specifications have been formulated yet. Still though, these early drafts can provide valuable input to the intended work.

→nSHIELD will implement and (if possible) refine the aforementioned OASIS/SOA4D specifications to release a working implementation of some of these mechanisms. Among them, the most interesting issue is the definition of WS-Security Policy. WS-Security Policy is a standard that regulates a security assertion model, a security binding abstraction and policy considerations. Moreover, nSHIELD will consider the work undertaken by the 6LoWPAN

---

[81] OASIS: Advancing open standards for the global information society
http://www.oasis-open.org
[82] Driscoll and Mensch, "OASIS Devices Profile for Web Services (DPWS) Version 1.1", 2009,
http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01
[83] OASIS Web Services Dynamic Discovery (WS-Discovery)
http://docs.oasis-open.org/ws-dd/ns/discovery/2009/01
[84] SOA4D Forge, https://forge.soa4d.org/
[85] IPv6 over Low power WPAN (6lowpan), http://datatracker.ietf.org/wg/6lowpan/

working group and contribute to it. nSHIELD will elaborate on the work of the Web Services for Devices (WS4D) initiative which aims to bring web services and other internet technologies in environments populated by embedded systems. Finally, nSHIELD will exploit the results of the related ITEA2 projects SOCRADES[86], and its predecessors, SODA[87] and TERESA[88].

## Situational-aware and Context-aware SPD

The Security, Dependability and Privacy characteristics of system depends on the context and the situation in which the system operate. Usually, systems implementing critical applications in physically and logically unprotected environments require higher level of security and dependability than for example entertainment or gaming application. Furthermore the same system can operate in environments with different risk levels.

→Because the implemented level of security is paid in terms computational and transmission resources (due the increasing complexity of encryption algorithms and redundancy) an adaptable context aware approach can benefit the optimization of the available resource and the maximization of the performance. nSHIELD will realize this capability by means of context ontology, which can be used to describe the domain in which the system is going to operate.

## Policy-based SPD management

Policies permit the declarative specification of security strategies separately from the implementation code of I-ES (Intelligent - Embedded System) nodes. Node policy must be formulated and populated in a structured unambiguous form prior to engaging in any activity. 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. Unstructured policy requirements are a burden to interoperability. Dynamic policy management is the key to achieve higher levels of security, privacy and dependability.

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

→ In this aspect, nSHIELD 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 developed in the SERENITY[89] (System Engineering for Security & Dependability, FP6) and MASTER[90] (Managing Assurance, Security and Trust for Services, FP7) 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

---

[86] Service Oriented Cross-layer Infrastructure for Distributed Smartembedded Devices - SOCRADES, http://www.socrades.eu
[87] Service Oriented Device & Delivery Architecture – SODA, http://www.soda-itea.org/
[88] Trusted Computing Engineering for Resource Constrained Embedded Systems Applications – TERESA http://www.teresa-project.org
[89] http://www.serenity-project.org/
[90] http://www.project-master.eu/

simply an adaptation of an existing one, but, on the contrary, designed for the particularities of the ESs.

→ nSHIELD will build on W3C specifications regarding web services policy[91,92] and utilize a number of specifications defined by OASIS (Organization for the Advancement of Structured Information Standards), such as the WS-SecurityPolicy Standard[93], which targets more security related policy requirements. This specification defines policy assertions for the security properties for Web services. The primary goal of this specification is to define an initial set of patterns or sets of assertions that represent common ways to describe how messages are secured on a communication path. The intent is to allow flexibility in terms of the tokens, cryptography, and mechanisms used, including leveraging transport security, but to be specific enough to ensure interoperability based on assertion matching. Oasis WS-Trust[94] specification uses the base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Finally, the Oasis WS-SecureConversation[95]specification defines extensions to allow security context establishment and sharing, and session key derivation. This allows contexts to be established and potentially more efficient keys or new key material to be exchanged, thereby increasing the overall performance and security of the subsequent exchanges.

## 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.

→nSHIELD 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[96]. Diameter protocol and its extensions are already strongly adopted in many IP systems[97] in order to support Strong Security, Accounting and Resource Management. nSHIELD will adopt the same

---

[91] W3C Recommendation, "Web Services Policy 1.5 - Framework", September 2007,
    http://www.w3.org/TR/ws-policy/
[92] W3C Recommendation, "Web Services Policy 1.5 - Attachment", September 2007,
    http://www.w3.org/TR/ws-policy-attach/
[93] http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/ws-securitypolicy.pdf
[94] http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf
[95]http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.pdf
[96] P. Calhoun and others (September 2003) RFC 3588, "Diameter Base Protocol", IETF (http://tools.ietf.org/html/rfc3588)
[97] 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.

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 nSHIELD 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.
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 nSHIELD 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. In call *ARTEMIS-2009-1* only one project, pSHIELD, has been funded as primary investigation of SPD issues in ES. For that reason nSHIELD represent itself the very first milestone towards such harmonization and the necessary prosecution of the pSHIELD project.

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

**pSHIELD**

pSHIELD, a 12 month project started in March 2010, 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 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 basis that will become the reference for a new generation of "SPD-ready" ESs. The composability of the nSHIELD architectural framework will have great

impact on system design cost and time to market of new SPD solutions. At the same time, the integrated use of SPD metrics will have impact on the qualification, (re-) certification and (re-) validation process, making them faster, easier and more widely accepted.

Other projects that have been funded by ARTEMIS (2008 and 2009 calls), not particularly under sub-programme 6, and which involve some unresolved SPD aspects as well as some concept that nSHIELD would like to address include the following.

## 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.

nSHIELD 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 nSHIELD 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.

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

## CHIRON

Addressing growing health-care concerns, CHIRON will combine state-of-the art technologies and innovative solutions into an integrated framework designed for an effective and person-centric health management over the complete care cycle. It will address and harmonize the needs of all the three main beneficiaries of the healthcare process, i.e., the patients using the services, the medical professionals and the whole community, putting the citizens at the core of the whole healthcare cycle by considering them as "persons" with specificities and identities, empowering them to manage their own health.

CHIRON will enlarge the boundaries of healthcare by fostering a seamless integration of clinical, at home and mobile settings, in a concept of a "continuum of care", with a focus on

moving from treatment to prevention. By developing a reference-architecture for personal healthcare, CHIRON will ensure the interoperability between heterogeneous devices and services, offer reliable and secure patient data management and a seamless integration with the clinical workflow. The CHIRON system will provide powerful supporting ICT tools and at the same time it will ensure that the patients and the doctors remain the protagonists of the healthcare process that has been designed around them.

nSHIELD will consider the CHIRON results for the social mobility scenario that is planning to address. More specifically, the requirements identified by CHIRON regarding interoperability and data security together with the provided reference architecture will stipulate the solutions provided by nSHIELD for this scenario.

## 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.

nSHIELD 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.

## eSONIA

eSONIA will realize the asset-aware and self-recovering plant through pervasive, heterogeneous (wireline and wireless) IPv6-based embedded devices with on-board specialized services, glued together by middleware capitalizing on the service oriented approach. All of this will be used for the first time in industry to support continuous monitoring, diagnostics, prognostics and control of assets, regardless of their physical location. The data gathered allow efficient automatic maintenance schedules and improved operator dispatch and repair performance. eSONIA means greater predictability of plant behaviour and visibility, reduced safety risks, enhanced security and cost efficiency.

nSHIELD will benefit from the experience gained through the eSONIA project in the fields IPv6 enabled devices and the service oriented approach. The service management system for enhanced manufacturing control that is planned to be delivered by eSONIA can form the basis for applying the enhanced nSHIELD services and architecture in the manufacturing scenario.

## 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 performing 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.

nSHIELD, 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[98]; we have identified some potential starting point that nSHIELD will improve with its outcome and approach.

## TERESA

TERESA (**T**rusted Computing **E**ngineering for **R**esource Constrained **E**mbedded **S**ystems **A**pplications) plans to define, demonstrate and validate an engineering discipline for trust that is adapted to resource constrained embedded systems. We define trust as the degree with which security and dependability requirements are met.

TERESA has the following objectives:

- Provide guidelines for the specification of sector specific RCES trusted computing engineering.
  Software process engineers in a given sector can then use the guidelines to define a trusted computing engineering process that is integrated with the software engineering process used in their RCES sector.
- Define a trusted computing engineering approach that is suited to the following sectors:
  - Automotive
  - Home control
  - Industry control
  - Metering

nSHIELD can build on the guidelines defined by TERESA and realize them through the architectural framework that nSHIELD will deliver. Moreover, it will apply these guidelines and the TERESA's trusted computing approach on the four distinct scenarios considering the related work carried out in TERESA's sectors.

## 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.

nSHIELD 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 nSHIELD, in terms of basic functionalities and specifications, each device can be composed to provide a valuable platform also (but not limited to) critical applications.

---

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

## 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.

Other embedded systems security oriented projects funded under the 6th Framework Programme and other funding schemes, like ITEA2, include the following:

## SMEPP

SMEPP (Secure Middleware for embedded peer to Peer Systems), a 3-year FP6 project, aimed to develop a new secure and generic middleware, based on a new network centric abstract model for embedded Peer-to-Peer systems. Its suitability was demonstrated by the development of two real-life applications in the domains of Enviromental Monitoring in Industrial Plants and Mobile Telephony.

nSHIELD will consider the problems faced and the proposed solutions for the design of the middleware level solution of the four-level architecture that it will provide.

## TECOM

TECOM (Trusted Embedded Computing) is a consortium research project funded in part by the Information Technology for European Advancement (ITEA2) programme.

Industrialised societies are increasingly dependent on embedded systems that are getting more and more complex, dynamic, and open, while interacting with a progressively more demanding and heterogeneous environment. As a consequence, the reliability and security of these systems have become major concerns. Unfortunately, current systems provide little or no support to determine their level of dependability and trustworthiness. An increasing number of external security attacks as well as design weaknesses in operating systems, especially in the PC world, have resulted in large economic damages, and as a consequence difficulties to attain user acceptance and getting accepted by the market.

The strategic objective of TECOM is to investigate solutions and architectures for embedded systems platforms which need to meet both security and integrity requirements. The TECOM approach will be to apply the concept of trusted platforms to real-time embedded systems.

TECOM deals with some of the objectives of the nSHIELD project such as facing denial of service and preventing malicious unauthorised access to data by providing secure solutions and architectures emphasizing on embedded system's integrity. The corresponding technological issues that will be investigated by nSHIELD will leverage the work carried out

by TECOM.

nSHIELD 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; nSHIELD consortium believes that, rather than 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 36 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 nSHIELD framework.
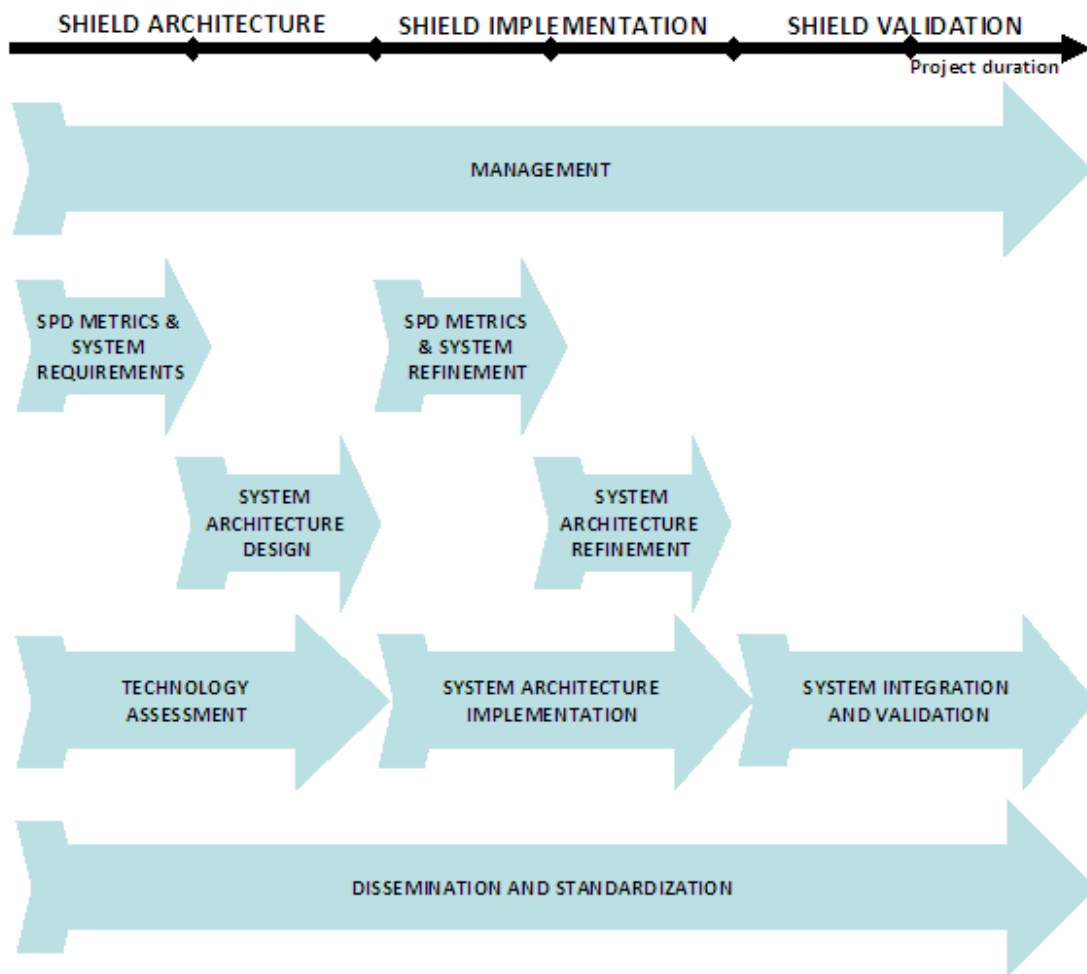


**Figure 3-1 – nSHIELD Phases**

| Phase | Related activities |
|---|---|
| **Technologies assessment** | **Classification of technologies** pertaining to the nSHIELD 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 nSHIELD have participated to most of the main European research projects** with results in the scope of nSHIELD 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 nSHIELD 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 so that, after 18 months, **a first release of implementations will be delivered**. 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 application scenarios. Particular attention will be devoted to this phase in order to **understand which performance indicators and peculiar requirements are the most suitable for each selected application domain**. |
| **Architecture tailored Refinement** | The **general system architecture will be personalized and tailored on the selected scenarios** (railways, recognition, avionics, social-mobility). According to continuous evolution in ESs research and development activities (e.g. other ARTEMIS projects outcomes), a refined **enhanced nSHIELD implementation will be designed leading to the delivery of a second release of implementation**; this release will be **included in the final test-bed**. |
| **System Integration and Validation** | The **system integration** phase **will lead to the final test-bed**. **Extensive trials, basing on defined SPD metrics, will be performed to test the selected Value Added Service**. Therefore, test beds and field trial set-ups, including prototypes, performances will **prove nSHIELD'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**. **Pilots and demonstrations** will be setup at the end of first phase and 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 six month market check** has been foreseen in order to guarantee that the nSHIELD project will always be **in line with industrial and market trends**. |

nSHIELD has been organized in 8 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** | **SG** | |
| Task 1.1 | Project management | SG | 136 |
| Task 1.2 | Liaisons | **SG** | |
| **WP2** | **SPD Metric, requirements and system design** | **THYIA** | |
| Task 2.1 | Multi-technology requirements & specification | THYIA | |
| Task 2.2 | Multi-technology SPD metrics | TECNALIA | 141 |
| Task 2.3 | Multi-technology architectural design | HAI | |
| **WP3** | **SPD Node** | **ETH** | |
| Task 3.1 | SDR/Cognitive Enabled node | THYIA | |
| Task 3.2 | Micro/Personal node | ETH | |
| Task 3.3 | Power node | ISD | 328 |
| Task 3.4 | Dependable self-x Technologies | UNIGE | |
| Task 3.5 | Cryptographic technologies | UNIGE | |
| **WP4** | **SPD Network** | **SCOM** | |
| Task 4.1 | Smart SPD driven transmission | SCOM | |
| Task 4.2 | Distributed self-x models | ATHENA | 258 |
| Task 4.3 | Reputation-based resource management technologies | HAI | |
| Task 4.4 | Trusted and dependable Connectivity | ISL | |
| **WP5** | **SPD Middleware & Overlay** | **ED** | |
| Task 5.1 | SPD driven Semantics | ED | |
| Task 5.2 | Core SPD services | UNIROMA1 | |
| Task 5.3 | Policy-based management | HAI | 236 |
| Task 5.4 | Adaptation of legacy systems | ED | |
| Task 5.5 | Overlay monitoring and reacting system by security agents | UNIROMA1 | |
| **WP6** | **Platform integration, validation & demonstration** | **HAI** | |
| Task 6.1 | Multi-Technology System Integration | HAI | |
| Task 6.2 | Multi-Technology Validation & Verification | ED | 238 |
| Task 6.3 | Lifecycle SPD Support | TECNALIA | |
| **WP7** | **SPD Applications** | **MAS** | |
| Task 7.1 | Railways Security | ASTS | |
| Task 7.2 | Voice/Facial recognition | ETH | 223 |
| Task 7.3 | Dependable Avionic System | SG | |
| Task 7.4 | Social Mobility Networking | MAS/THYIA | |
| **WP8** | **Knowledge exchange and industrial validation** | **MGEP** | |
| Task 8.1 | Dissemination | MGEP | |
| Task 8.2 | Standardization | SG | 82 |
| Task 8.3 | Exploitation | ISL | |
| | TOTAL | | 1642 |

It is important noting that the nSHIELD breakdown structure reflects the System Architecture described in Section 2. In particular, WP3, deals with the design and development of nSHIELD SPD modules at node level, WP4 deals with the design and development of nSHIELD 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 nSHIELD 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. Finally WP7 is in charge of validating the nSHIELD framework by means of significant application scenarios. The project WBS is depicted below.
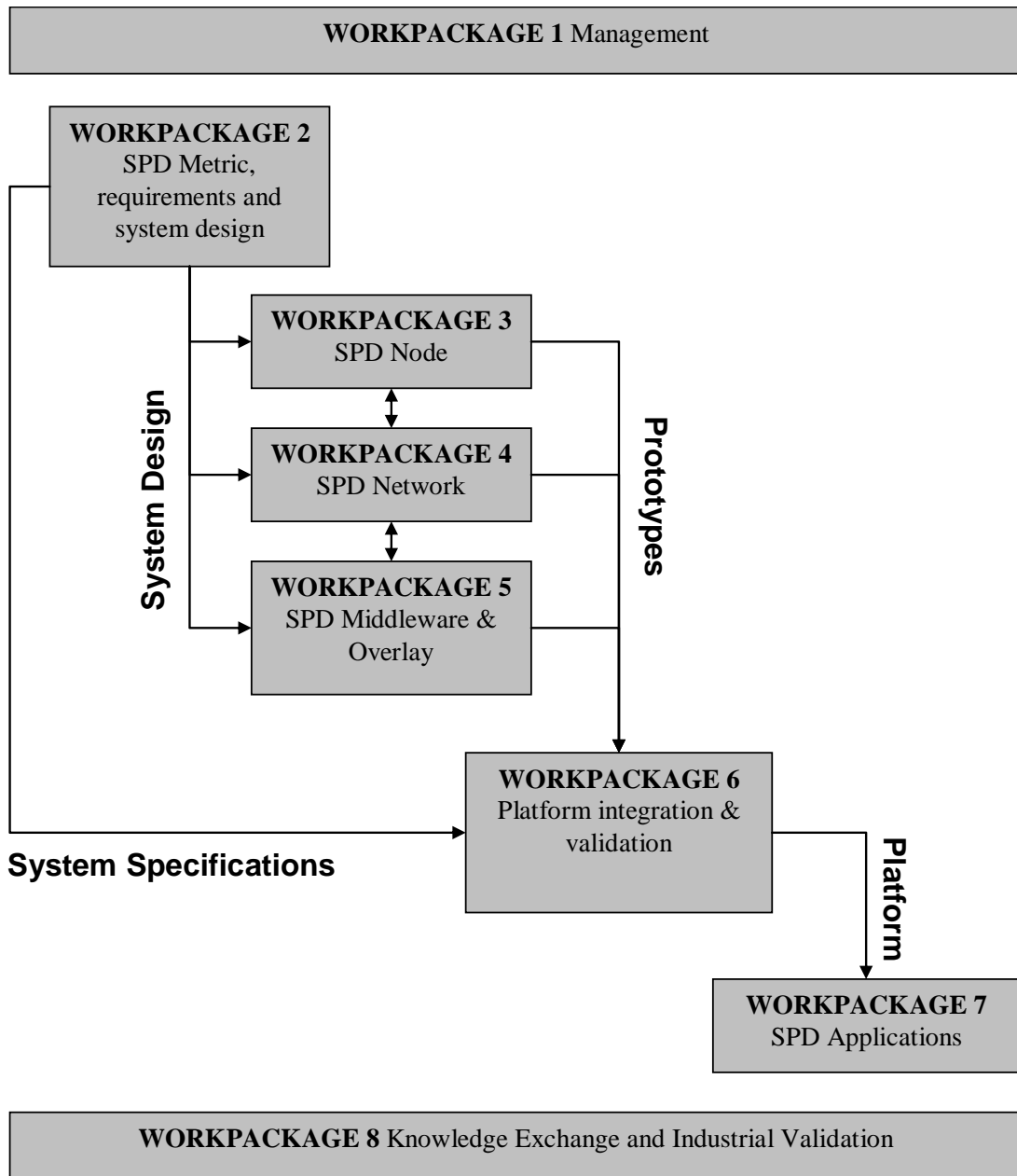


**Figure 3-2 – nSHIELD Work Breakdown Structure**

# 3.1.2 - Gantt chart[91]



---
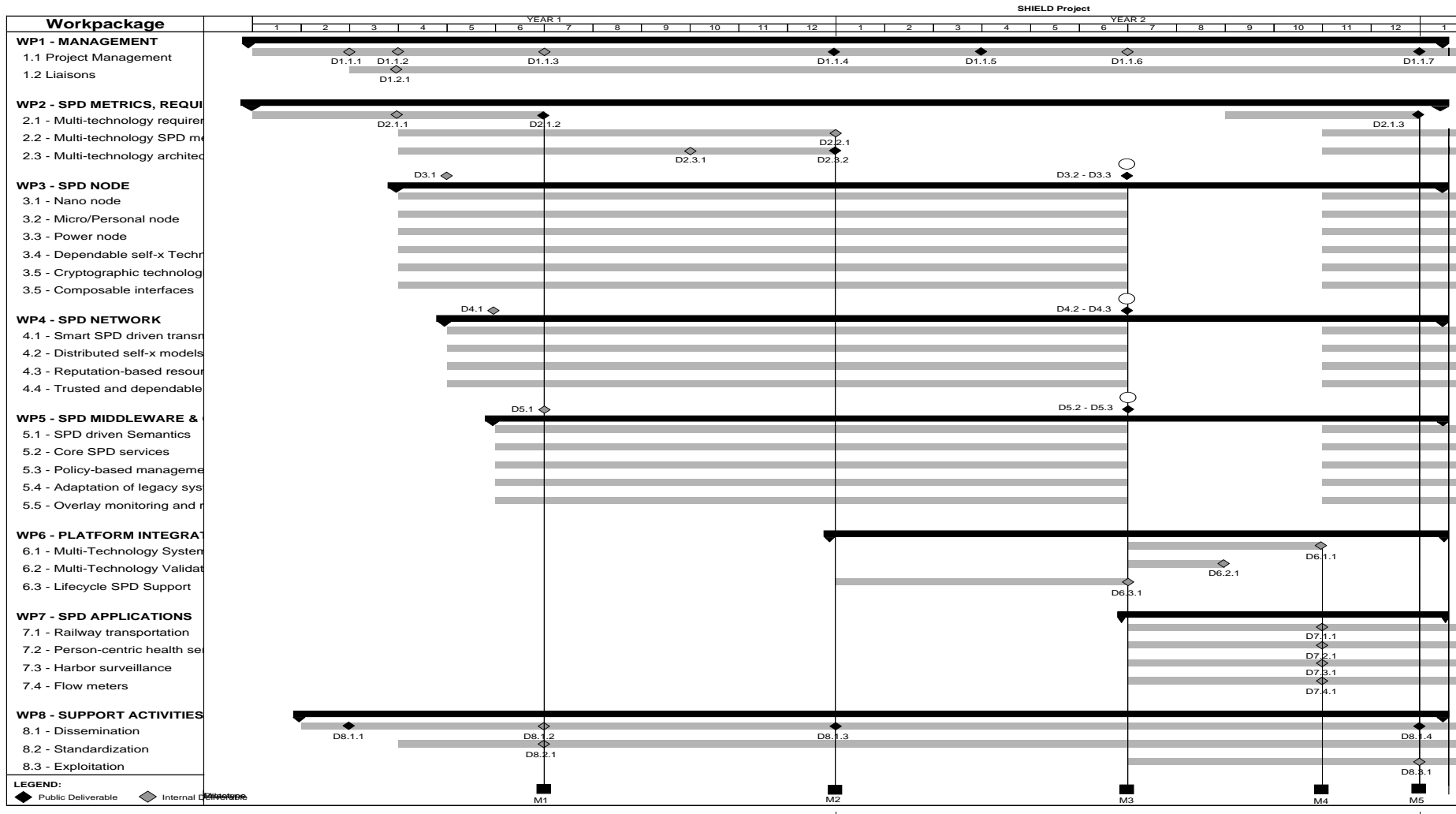
[91] This Gantt chart shows only the temporal view of nSHIELD tasks and workpackages. Their relations have been represented in the Pert diagram.

## 3.1.3 - Workpackages

## Work package list

| Work package no[92] | Work package title | Lead partic. no.[93] | Lead partic. short name | Person-months[94] | Start month[95] | End month |
|---|---|---|---|---|---|---|
| WP1 | Project Management | 1 | SG | 136 | 0 | 36 |
| WP2 | Scenarios, requirements and system design | 22 | THYIA | 141 | 0 | 26 |
| WP3 | SPD Node | 25 | ETH | 328 | 3 | 30 |
| WP4 | SPD Network | 16 | SCOM | 258 | 4 | 30 |
| WP5 | SPD Middleware & Overlay | 6 | ED | 236 | 5 | 30 |
| WP6 | Platform integration, validation & demonstration | 10 | HAI | 238 | 12 | 36 |
| WP7 | SPD Applications | 13 | MAS | 223 | 18 | 36 |
| WP8 | Knowledge exchange and industrial validation | 5 | MGEP | 82 | 1 | 36 |
|  | TOTAL |  |  | 1642 |  |  |

---

[92]     Workpackage number: WP 1 – WP n.
[93]     Number of the participant leading the work in this work package.
[94]     The total number of person-months allocated to each work package.
[95]     Measured in months from the project start date (month 1).

# List of Deliverables

| Del. no. [96] | Deliverable name | WP no. | Nature [97] | Dissemination level [98] | Delivery date [99] (proj. month) |
|---|---|---|---|---|---|
| D1.1 | Collaborative tools and document repository | 1 | O | PP | 2 |
| D8.1 | Web Site | 8 | O | PU | 2 |
| D1.2 | Quality Control Guidelines | 1 | R | PP | 3 |
| D1.3 | Liaisons Plan | 1 | R | PP | 3 |
| D2.1 | Preliminary System Requirements | 2 | R | CO | 3 |
| D3.1 | SPD node technologies assessment | 3 | R | CO | 4 |
| D4.1 | SPD network technologies assessment | 4 | R | CO | 5 |
| D5.1 | SPD middleware and overlay technologies assessment | 5 | R | CO | 6 |
| D1.4 | Periodic Management Report 1 | 1 | R | PP | 6 |
| D2.2 | Preliminary System Requirements and Specifications | 2 | R | PU | 6 |
| D8.2 | Dissemination Plan | 8 | R | PP | 6 |
| D8.3 | Standardization Plan | 8 | R | PP | 6 |
| D2.3 | Preliminary system architecture design | 2 | R | CO | 9 |
| D1.5 | Periodic Annual Report 1 | 1 | R | PP | 12 |
| D2.4 | Reference system architecture design | 2 | R | PU | 12 |
| D2.5 | Preliminary SPD Metrics specifications | 2 | R | CO | 12 |
| D8.4 | nSHIELD Operational Manual v1 | 8 | R | PU | 12 |
| D1.6 | Quality Control Report 1 | 1 | R | PU | 15 |
| D1.7 | Periodic Management Report 2 | 1 | R | PP | 18 |
| D3.2 | Preliminary SPD node technologies prototype | 3 | P,O | RE | 18 |
| D3.3 | Preliminary SPD node technologies prototype report | 3 | R | PU | 18 |
| D4.2 | Preliminary SPD network technologies prototype | 4 | P,O | RE | 18 |
| D4.3 | Preliminary SPD network technologies prototype report | 4 | R | PU | 18 |

---

[96]     Deliverable numbers in order of delivery dates. The numbering convention is as requested from numbering rules of the negotiation tool.

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

[98]     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).

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

| Del. no. [96] | Deliverable name | WP no. | Nature[97] | Dissemination level[98] | Delivery date[99] (proj. month) |
|---|---|---|---|---|---|
| D5.2 | Preliminary SPD middleware and overlay technologies prototype | 5 | P,O | RE | 18 |
| D5.3 | Preliminary SPD middleware and overlay technologies prototype report | 5 | R | PU | 18 |
| D6.1 | Lifecycle and SPD Support Plan | 6 | R | CO | 18 |
| D6.2 | Prototype validation and verification | 6 | R | RE | 20 |
| D6.3 | Prototype integration report | 6 | R | RE | 22 |
| D7.1 | Railways security demonstrator - integration and validation plan | 7 | R | CO | 22 |
| D7.2 | Voice/Facial Recognition demonstrator - integration and validation plan | 7 | R | CO | 22 |
| D7.3 | Dependable Avionic Systems demonstrator - integration and validation plan | 7 | R | CO | 22 |
| D7.4 | Social Mobility and Networking demonstrator - integration and validation plan | 7 | R | CO | 22 |
| D1.8 | Periodic Annual Report 2 | 1 | R | PP | 24 |
| D2.6 | Final System Requirements and Specifications | 2 | R | PU | 24 |
| D8.5 | Preliminary Exploitation Plan | 8 | R | PP | 24 |
| D8.6 | nSHIELD Operational Manual v2 | 8 | R | PU | 24 |
| D2.7 | Final system architecture design | 2 | R | PU | 26 |
| D2.8 | SPD Metrics specifications | 2 | R | PU | 26 |
| D1.9 | Quality Control Report 2 | 1 | R | PU | 27 |
| D1.10 | Periodic Management Report 3 | 1 | R | PP | 30 |
| D3.4 | SPD node technologies prototype | 3 | P,O | RE | 30 |
| D3.5 | SPD node technologies prototype report | 3 | R | PU | 30 |
| D4.4 | SPD network technologies prototype | 4 | P,O | RE | 30 |
| D4.5 | SPD network technologies prototype report | 4 | R | PU | 30 |
| D5.4 | SPD middleware and overlay technologies prototype | 5 | P,O | RE | 30 |
| D5.5 | SPD middleware and overlay technologies prototype report | 5 | R | PU | 30 |
| D6.4 | Lifecycle and SPD Support Report | 6 | R | PU | 30 |
| D1.11 | Liaisons Report | 1 | R | PU | 34 |
| D6.5 | Platform integration report | 6 | R | PU | 34 |
| D7.5 | Railways Security - integration report | 7 | R | PU | 34 |
| D7.6 | Voice/Facial Recognition - integration | 7 | R | PU | 34 |

| Del. no. [96] | Deliverable name | WP no. | Nature[97] | Dissemination level[98] | Delivery date[99] (proj. month) |
|---|---|---|---|---|---|
| | report | | | | |
| D7.7 | Dependable Avionic Systems demonstrator - integration report | 7 | R | PU | 34 |
| D7.8 | Social Mobility and Networking demonstrator - integration report | 7 | R | PU | 34 |
| D1.12 | Periodic Annual Report 3 | 1 | R | PU | 36 |
| D6.6 | Platform validation and verification | 6 | R | PU | 36 |
| D7.9 | Railways security demonstrator-validation and verification report | 7 | R | PU | 36 |
| D7.10 | Voice/Facial Recognition demonstrator - validation and verification report | 7 | R | PU | 36 |
| D7.11 | Dependable Avionic Systems demonstrator - validation and verification report | 7 | R | PU | 36 |
| D7.12 | Social Mobility and Networking demonstrator - validation and verification report | 7 | R | PU | 36 |
| D8.7 | nSHIELD Operational Manual v3 | 8 | R | PU | 36 |
| D8.8 | Standardization Report | 8 | R | PU | 36 |
| D8.9 | Dissemination Report | 8 | R | PU | 36 |
| D8.10 | Final Exploitation Plan | 8 | R | CO | 36 |

# Milestones

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 [100] | Means of verification [101] |
|---|---|---|---|---|
| M1 | **Preliminary System Requirements and Specification** | WP2 | M6 | D2.1.2 |
| M2 | **Preliminary SPD metrics and System Architecture Design** | WP2 | M12 | D2.2.1, D2.3.2 |
| M3 | **Preliminary composable SPD prototypes** | WP3, WP4, WP5 | M18 | D3.3, D4.3, D5.3 + Prototypes + Workshop #1 |
| M4 | **Preliminary integrated Platform** | WP6 | M22 | D6.1.1 |
| M5 | **Final System Requirements and Specification** | WP2 | M24 | D2.1.2 |
| M6 | **Final SPD Metrics and Tailored System Architecture Design** | WP2 | M26 | D2.2.2, D2.3.3 |
| M7 | **Final composable SPD prototypes** | WP3, WP4, WP5 | M30 | D3.5, D4.5, D5.5 + prototypes |
| M8 | **Final integrated platform and applications specific demonstrators** | WP6, WP7 | M34 | 6.1.2, 7.1.2, 7.2.2, 7.3.2, 7.4.2 |
| M9 | **Integrated platform validated and verified** | WP6 | M36 | 6.2.2 + Workshop #2 |

---

[100] Measured in months from the project start date (month 1).
[101] 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.

# Work packages description

| 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 | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 40 | 2 | 9 | 3 | 0 | 11 | 5 | 0 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 1 | 15 | 10 | 2 | 0 | 3 | 0 | 12 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 0 | 0 | 0 | 0 | 0 | 13 | 4 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 0 | 3 | 3 | | | | | |

**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: SG)

*Task 1.1: Project management (Leader: SG - Partners: ASTS, AT, ATHENA, ED, TECNALIA, ETH, HAI, ISL, ISD, MGEP, SCOM, THYIA, TUC, UNIUD, 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.

As this task is mainly devoted to management, SG will take the lead. All other participants are included according to the described management structure.

*Task 1.2: Liaisons (Leader: SG - Partners: ED, HAI, SC, THYIA)*

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 nSHIELD. 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 nSHIELD identified technologies and solutions will represent a reference guideline for the design and development of ESs where SPD capabilities are required. In particular, the nSHIELD 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*

D1.5    Periodic Annual Report 1 (M12)

D1.6    Quality Control Report 1 (M15)

D1.8    Periodic Annual Report 2 (M24)

D1.9    Quality Control Report 2 (M27)

D1.12 Periodic Annual Report 3 (36)

D1.11  Liaisons Report (M34)

*Internal*

D1.1    Collaborative tools and document repository (M2)

D1.2    Quality Control Guidelines (M3)

D1.3    Liaisons Plan (M3)

D1.4    Periodic Management Report 1 (M6)

D1.7    Periodic Management Report 2 (M18)

D1.10  Periodic Management Report 3 (M30)

| 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 | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 10 | 9 | 8 | 6 | 0 | 12 | 12 | 0 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 2 | 22 | 0 | 0 | 0 | 0 | 0 | 1 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 10 | 0 | 6 | 10 | 0 | 20 | 10 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 0 | 3 | 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 four application scenarios;

- 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 nSHIELD 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: THYIA - Partners: SG, ASTS, ED, ETH, HAI, S-LAB, SICS, T2D, THYIA, TUC, SCOM)*

This task will identify the requirements and describe the specifications of the overall nSHIELD 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 WP7 application scenarios. These scenarios 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 the 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 descriptions of the application scenarios from WP7.

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 (WP7).

*Task 2.2 Multi-technology SPD metrics (Task Leader: TECNALIA - Partners: SG, ASTS, ATHENA, ED, HAI, S-LAB,  THYIA, TUC, SCOM)*

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 based on the definition of scenarios and use cases that will be identified in WP7.

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, which will be based on the four scenarios proposed in WP7. Within the project, this task builds the basis for all subsequent steps by providing standard metrics for the integration and test of the 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 scenarios.

*Task 2.3 Multi-technology architectural design (Task Leader: HAI - Partners: AT, ATHENA, ED, SICS, T2D, THYIA, TUC, SCOM)*

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*

D2.2    Preliminary System Requirements and Specifications (M6)

D2.4    Reference system architecture design (M12)

D2.6    Final System Requirements and Specifications (M24)

D2.8    SPD Metrics specifications (M26)

D2.7    Final system architecture design (M26)

*Internal*

D2.1    Preliminary System Requirements (M3)

D2.3    Preliminary system architecture design (M9)

D2.5    Preliminary SPD Metrics specifications (M12)

---

**Milestones**

M1    Preliminary System Requirements and Specification (M6)

M2    Preliminary SPD metrics and System Architecture Design (M12)

M5    Final System Requirements and Specification (M24)

M6    Final SPD Metrics and Tailored System Architecture Design (M26)

| Work package number | WP3 | Start date or starting event: | | Month 3 | | | |
|---|---|---|---|---|---|---|---|
| Work package title | SPD Node | | | | | | |
| Participant no. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Participant short name | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 16 | 0 | 22 | 8 | 0 | 0 | 6 | 0 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 25 | 4 | 0 | 58 | 0 | 0 | 0 | 8 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 12 | 15 | 20 | 26 | 6 | 30 | 30 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 30 | 12 | 0 | | | | | |

**Objectives**

This WP is dedicated to:

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

**Description of work** (WP Leader: ETH)

In the following section the technologies examined in the nSHIELD project are described. Part of these technologies are examined partially in the pSHIELD project, nSHIELD will complete the technologies started in the pSHIELD project and the remaining ones.

At the start-up of the project an assessment will be done on the technologies that the pSHIELD project has examined, in order to full address the rights technologies for the nSHIELD project.

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: SDR/Cognitive Enabled node, nano and micro 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 scenarios, described in detail in WP7, will drive the identification of the Intelligent ES nodes that need to be developed and 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 and subsequently updated according to first technology prototypes release, will permit the development of nSHIELD framework first level.

The activities will start from SPD simple nodes creation, the nanonodes, 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 and will be furthermore developed and enriched, in order to satisfy the SPD more complex requirements of the higher node levels (i.e. micro and SDR/Cognitive Enabled nodes).

The effectiveness of the results will be guaranteed by an iterative process of refinement and enrichment, obtained designing two times the three previously described node levels. 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 nSHIELD 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* SDR/Cognitive Enabled node *(Task Leader: THYIA - Partners: SG, SICS, TUC, UNIUD, SCOM)*

SDR/Cognitive Enabled 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 SDR/Cognitive Enabled node that will provide the enhancement of the following technologies in terms of SPD:

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 nSHIELD architecture, particular care will be devoted to this task. Moreover, the development of intrinsically secure ES firmware will affect activities performed in WP4 and WP5 concerning the design of nSHIELD framework other levels enabling the improvement of security-oriented features and services both at network and middleware layers. As a consequence, system integration tasks (see WP6) will take advantage from such a strategy specifically tailored to an iterative process of refinement and enrichment not only within a single layer (e.g. SPD Node) but also among all nSHIELD layers.

Power supply protection: this technique aims to maintain operation even if external power supply is removed (i.e. blackout / malicious or not). The research which will be performed under the nSHIELD 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 and WPs, 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.

On the basis of the results of the R&D activities 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 SDR/Cognitive Enabled node to interface with the rest of nSHIELD platform.

The research results obtained in this task are not limited to SDR/Cognitive Enabled nodes and, from a technological point of view, will be adopted when needed also for the design and development of the micro/personal and power nodes.

*3.2 Micro node (Task Leader: ETH - Partners: SG, AT, SICS, T2D, TELC, THYIA, TUC, SCOM)*

This class consists of devices richer than the SDR/Cognitive Enabled nodes in terms of hardware and software resources, network access capabilities, mobility, interfaces, sensing capabilities etc.. Considering the computing power, these nodes remain confined in the class of embedded computers. The presence of an advanced OS, the typical environment in which they are used and the category of user interested introduces several potential risks in terms of SPD that must be considered and solved. Good representatives of this class are the device for identification/access control proposed in Scenario 3 and the device for telemetry adopted in Scenario 4. To increase SPD capabilities of these nodes, Task 3.2 will focus on the following technologies:

- Trusted ESs based on TPM or smartcard which offer facilities for the secure generation of cryptographic keys, and limitation of their use, in addition to a hardware pseudo-random number generator (T3.5). For instance, TPM for trust ESs also includes capabilities such as remote attestation and sealed storage. Such a Trusted Platform Module can be used to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication. One possible application of this technology is the verification that a system seeking access is the expected system (T3.5). The development of this technology relies on the identification and definition of proper trust-oriented specification as well as on the conceiving and design of innovative architectures (WP2) and is strictly connected with SPD Network level (WP4) of nSHIELD framework supporting secure and dependable communication strategies among different nodes.

- Easy and dependable interfaces with the sensors will be focusing on the implementation of protocols for wireless node which don't need to remain constantly in active mode, optimizing the life of power supply. Moreover, the use of TPM will be adapted in order to achieve low power consumption of the SPD node and high

degree of security simultaneously. The developed prototypes of HW and SW modules will be verified in the proposed scenarios using experimental facilities.

- Advanced biometric algorithms that are capable to identify the most significant features of the face and of the voice of a person. From these information the algorithms extract a visual biometric profile that is as much as possible unique for that person. A second set of algorithms will compare these biometric profiles with the ones stored in a database, trying to provide a result consisting in the name of a person and the matching percentage for both face and audio contexts. The algorithms will be studied specifically for embedded systems.

As for task 3.1, 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 micro nodes interoperation with the rest of nSHIELD platform.

*Task 3.3 Power node (Task Leader: ISD - Partners: SG, AT, SESM, SICS, T2D, TUC, SCOM)*

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:

Surveillance systems utilizing cameras that operate at the visual or infrared spectrum are widely used in applications that require advanced security features. Surprisingly this is not the case for sound-based surveillance that could act as a valuable complementary source of information that, in addition, does not suffer from problems such as out-of-field-of-view spots.

In the context of nSHIELD, ISD will develop a novel audio based surveillance system. The system will be able to interface hundreds of hardware synchronized microphones and transfer the combined audio stream to memory at real time.

Since the sensors will be hardware synchronized, the system will enable higher levels of software to perform, via signal processing, operations such as:

i) Abnormal event detection using simple peek detection on the incoming signals.

ii) Detection of the direction of the source generating the abnormal

event using triangulation as the peak detection will happen at different points in time when the sensors are placed at a large distance.

The main outcome of task 3.3 will be prototypes, matching with WP2 requirements, specification and interface design.

*Task 3.4 Dependable self-x Technologies (Task Leader: UNIGE - Partners: ATHENA, TECNALIA, HAI, S-LAB, THYIA, TUC, SCOM)*

This task will provide horizontal SPD technologies that will be adopted in task 3.1-3.2-3.3 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 nSHIELD'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 data path 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, nSHIELD 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;

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

*Task 3.5 Cryptographic technologies (Task Leader: UNIGE - Partners: AT, ATHENA, TECNALIA, S-LAB, SICS, TELC,THYIA, TUC)*

This task will provide horizontal SPD technologies that will be adopted in task 3.1-3.2-3.3 at different level depending on the complexity of the node and considering its HW/SW capabilities, its requirements and its use. The research will rely mainly on the following technologies:

Hardware and software crypto technologies. At node level cryptographic technologies will be foreseen to be performed by low-energy low-processing devices and become interesting for nSHIELD. A node will become trusted through the secure generation of cryptographic keys and limitation of their use, in addition to a hardware pseudo-random number generator and capabilities such as remote attestation and sealed storage. A Trusted Platform Module (TPM) can be used to authenticate hardware devices: since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication. In addition to available TPM, it will support future evolutions of cryptographic/hash functionalities, will be provided with alternative communication interfaces better adapted to ES and will provide additional cryptographic protocols (e.g. elliptic curves). The adoption of the TPM will require the design and implementation of an embedded operating system with lower resources requirements, in order to be suited to the HW features of ES. From cost point of view, algorithms and protocols for asymmetric cryptography, usually used with powerful hardware, could be considered for low cost nodes. They must be adapted to limited resources devices, both in terms of computing capability

and energy constraints. The solution could be an optimized hardware implementation for an elliptic curve cryptography based public-key authentication algorithm. 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 cost node would have its own secret, revealing one key does not immediately compromise the whole system, but only the very one entity. In addition to asymmetric technology, a secure authentication protocol based on ECC shall 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. The implementation shall also be secured against side-channel attacks, such as simple power analysis and differential power analysis, as well as their electro-magnetic counterparts SEMA, DEMA and fault attacks.

Data compression techniques are required in order to face the large amount of data generated by nodes (sensors). These data have either to be processed locally and/or sent to other nodes for further processing. As these nodes often do not have the resources (computational and power) or complete enough information about the extended environment to make proper processing, the latter case (involving data transmission) is very common. Therefore, aiming at improving the SPD features of the system and at enabling more reliable and secure transmissions and communications at network level we will research an approach utilizing reconfigurable hardware which accelerates compression algorithms while consuming less power. This approach enables also combining compression with self-re-configurability and self-recovery properties, as this type of hardware can be partially reconfigured, while less energy can be consumed in situations where compression is not needed or can be degraded without altering the node.

The cryptographic technologies will be implemented in the prototypes on M18 and M30.

Concluding, it is relevant to point out that beyond the proposed application domains, the identified technologies and solutions will represent a reference guideline for the design and development of embedded systems operating in other Artemis contexts where SPD capabilities are required.

**Deliverables**

*Public*

D3.3     Preliminary SPD node technologies prototype report (M18)

D3.5     SPD node technologies prototype report (M30)

*Internal*

D3.1     SPD node technologies assessment (M4)

D3.2     Preliminary SPD node technologies prototype (M18)

D3.4     SPD node technologies prototype (M30)

**Milestones**

M3       Preliminary composable SPD prototypes (M18)

M7       Final composable SPD prototypes (M30)

| Work package number | WP4 | Start date or starting event: | | Month 4 | | | |
|---|---|---|---|---|---|---|---|
| Work package title | SPD Network | | | | | | |
| Participant no. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Participant short name | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 10 | 0 | 0 | 10 | 0 | 6 | 14 | 0 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 0 | 15 | 34 | 0 | 0 | 20 | 0 | 78 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 0 | 0 | 0 | 0 | 0 | 12 | 14 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 25 | 12 | 8 | | | | | |

**Objectives**

The objectives of WP4 are:

- Improve SPD technologies at Network level;

- Develop a prototype to be integrated in the demonstrators.

**Description of work** (WP Leader: SCOM)

In the following section the technologies examined in the nSHIELD project are described. Part of these technologies are examined partially in the pSHIELD project, nSHIELD will complete the technologies started in the pSHIELD project and the remaining ones.

At the start-up of the project an assessment will be done on the technologies that the pSHIELD project has examined, in order to full address the rights technologies for the nSHIELD project.

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: SG, THYIA, TUC, UNIGE)*

This task will focus on the design and development of SPD-based transmissions

methodologies among nSHIELD node levels, exploiting the SPD built-in features of nodes developed in WP3. To reach this goal, the architectural, technical and practical specifications and guidelines emerged from WP2 in terms of communications and of defense against network attacks will be followed.

Firstly, effort will be devoted to implementation of smart SPD driven transmission techniques to nano-node level. The first release of the SPD communication environment will point out new important features that will be integrated in the second release of the nano-nodes. This design and development process will be applied also at the other node levels (micro/personal and power nodes communications). Broadly speaking, the necessity to provide SPD communications also when information exchanged are more complex will be faced performing a furthermore abstraction step, that applies on the higher node levels.

The design and development of the Smart Transmission Layer 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 evaluated according to previously defined metrics (see WP2). 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.

*Task 4.2 Distributed self-x models (Task Leader: ATHENA - Partners: THYIA, TUC, UNIGE, UNIUD, SCOM)*

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.

Taking into account smart transmission methodologies and previously defined specifications and requirements concerning SPD features, nSHIELD 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 parameter dynamic configuration such as adaptive modulation and coding and multiple antennas. 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. For instance, adaptive modulation and coding enables robust and spectrally-efficient transmission over time-varying channels. Basing on channel measurements, provided by the physical layer, we aim at dynamically adapting the modulation, coding and data rate in order to meet the required QoS level (which will quantitatively and qualitatively verified with respect to SPD metrics). To reach this goal, a continuous monitoring of the radio channel will be performed, especially if heterogeneous communication standards are employed in the considered frequency band, in order to avoid harmful interference among users.

*Task 4.3 Reputation-based resource management technologies (Task Leader: HAI - Partners: SCOM, TECNALIA, INDRA, MGEP, TUC, UNIROMA1)*

This task will develop proper schemes for reputation-based cooperation enforcement and scalable resource management based on distributed mechanisms aiming at identifying malicious users and performing a secure routing through secure paths.

The design and development of innovative resource management methodologies as efficient solutions based on trust and reputation-based schemes for secure routing and intrusion

detection systems at the communication level will represent a key feature of nSHIELD framework allowing a complete interoperability with other platform layers through, for instance, the capability of authenticate resources and component without a central certification authority but basing on individual certification.

The main goals which, according to defined requirements and to the overall system implementation strategy (development activities will be both tailored to and influenced by the joint iterative refinement process involving all nSHIELD layers (see WP3 and WP5)), will be pursued are:

- 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.

*Task 4.4 Trusted and dependable Connectivity (Task Leader: ISL - Partners: SG, SCOM, ED, TECNALIA, HAI, MGEP, THYIA, TUC)*

Main 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.

This task, exploiting also features and methodologies developed from T4.1 to T4.3, will represent a key element of Secure Service Chain (SSC). The overall goal of nSHIELD framework at network level will be to guarantee secure and dependable transmissions/communications while respecting user privacy. The proposed approach will be integrated with other technologies developed in different nSHIELD's layers to generate added value to the entire system and validated in the selected application scenarios (see WP7).

Finally, particular attention will be devoted to the compliance with existing standards and technologies (according to our proposed built-in approach) as well as to the capability of guarantying the proposed architecture to be future-proof, to support the installation, download and upgrade cycle in a continuous improvement perspective.

**Deliverables**

*Public*

D4.3    Preliminary SPD network technologies prototype report (M18)

D4.5    SPD network technologies prototype report (M30)

*Internal*

D4.1    SPD network technologies assessment (M5)

D4.2    Preliminary SPD network technologies prototype (M18)

D4.4    SPD network technologies prototype (M30)

**Milestones**

| M3 | Preliminary composable SPD prototypes (M18) |
| M7 | Final composable SPD prototypes (M30) |

| Work package number | WP5 | | Start date or starting event: | | | Month 5 | | |
|---|---|---|---|---|---|---|---|---|
| Work package title | SPD Middleware & Overlay | | | | | | | |
| Participant no. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Participant short name | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 10 | 0 | 0 | 14 | 0 | 43 | 20 | 0 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 0 | 27 | 18 | 0 | 0 | 8 | 0 | 0 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 28 | 0 | 0 | 0 | 0 | 19 | 16 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 0 | 0 | 33 | | | | | |

**Objectives**

The objectives of WP5 are:

- Define a common semantic to describe the SPD interfaces and functionalities;

- Improve SPD middleware technologies;

- Provide support to legacy SPD systems;

- Introduce the Overlay concepts and functionalities;

- Develop a prototype to be integrated in the demonstrators.


**Description of work** (WP Leader: ED)

In the following section the technologies examined in the nSHIELD project are described. Part of these technologies are examined partially in the pSHIELD project, nSHIELD will complete the technologies started in the pSHIELD project and the remaining ones.

At the start-up of the project an assessment will be done on the technologies that the pSHIELD project has examined, in order to full address the rights technologies for the nSHIELD project.


*Task 5.1 SPD driven Semantics (Task Leader: ED - Partners: SG, TECNALIA, HAI, MGEP, THYIA, TUC, UNIROMA1)*

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 all the exchanged information between the node, network, middleware and overlay layer. The designed semantic language will be used also to represent profiles and policies according to interoperable and self describing formats. The exploitation of semantic technologies will allow meaningfully representing and reasoning about context and policy information.

The outcome of this task will be 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. The semantic ontology will be part of the prototypes delivered by WP5.

*Task 5.2 Core SPD services (Task Leader: S-LAB - Partners: SG, ED, TECNALIA, MGEP, THYIA, TUC, UNIROMA1)*

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

- service management functionalities such as secure service discovery and delivery, service compositions, measurement systems and data distribution systems (DDS);
- context awareness features to refine and extend the existing middleware implementations in order to improve their performance in the application domains identified by WP2;

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 (like DDS) 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. Moreover experimental validation and benchmarking tools in state-of-art, such as RTI DDS, will be analyzed to guarantee the effectiveness of the results.

The problems of data transportation already addressed in WP4 will be extended to the upper software level. The services provided by the middleware will be used both by the ES Network Layer and by the Service Layer. These middleware services will be standard ones like resource and memory managements, scheduling and dispatching issues, HAL (Hardware Abstraction Layer), and additional ones like security and trustiness support, resilience and so on. The SPD middleware level will be implemented by adopting a Network Management Authority (NMA), that will establish and control trust relationships between different nodes and applications. Schedulers taking into account different level of criticality (e.g. according

to IEC 61508, DO-178B or ISO 26262), will be investigated.

One of the most challenging issues in this task will be the definition of a mechanism to encapsulate dependability features and embed (weave) them with functionalities corresponding to "kernel" functionalities.

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. The SPD modules will become part of the prototype delivered by WP5 on M18 and M30.

*Task 5.3 Policy-based management (Task Leader: HAI - Partners: ED, TECNALIA, ISL, THYIA, TUC)*

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 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 Adaptation of legacy systems (Task Leader: ED - Partners: ATHENA,  THYIA, TUC)*

This task aims to design highly-dependable interfaces, adapters, and enablers to make heterogeneous legacy SPD solutions (protocol, standards, mechanisms, techniques, etc.) for ES nodes, networks and middleware interwork transparently with the enhanced capabilities provided by the nSHIELD approach. The main outcome of this task will be the development of prototypal software adapters to make legacy devices capable to support the nSHIELD SPD-functionalities.

*Task 5.5 Overlay monitoring and reacting system by security agents (Task Leader: UNIROMA1 - Partners: ATHENA, ED, HAI, S-LAB, THYIA, TUC)*

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 nSHIELD architecture.

The security agent will be designed to *interpret* and *elaborate* the SPD information generated by the nSHIELD 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 nSHIELD 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 (on M18 and M30) ready to be integrated in the nSHIELD platform.

**Deliverables**

*Public*

D5.3    Preliminary SPD middleware and overlay technologies prototype report (M18)

D5.5    SPD middleware and overlay technologies prototype report (M30)

*Internal*

D5.1    SPD middleware and overlay technologies assessment (M6)

D5.2    Preliminary SPD middleware and overlay technologies prototype (M18)

D5.4    SPD middleware and overlay technologies prototype (M30)

**Milestones**

M3      Preliminary composable SPD prototypes (M18)

M7      Final composable SPD prototypes (M30)

| Work package number | WP6 | Start date or starting event: | | | Month 12 | | |
|---|---|---|---|---|---|---|---|
| Work package title | Platform integration, validation & demonstration | | | | | | |
| Participant no. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Participant short name | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 10 | 6 | 19 | 21 | 0 | 17 | 15 | 4 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 3 | 32 | 24 | 6 | 7 | 3 | 1 | 9 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 29 | 0 | 0 | 0 | 0 | 12 | 10 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 0 | 6 | 4 | | | | | |

**Objectives**

- Integration of software components;

- Validation of implemented solution through an iterative and incremental process.

**Description of work** (WP Leader: HAI)

*Task 6.1 Multi-Technology System Integration (Task Leader: HAI - Partners: SG, ASTS, AT, ATHENA, ED, ESIS, ETH, ISL, ISD, MAS, MGEP, NOOM, SCOM, S-LAB, THYIA, TUC, UNIROMA1)*

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

A vertical testbed covering various layers of nSHIELD will be the integration result, targeting to the demonstration of the interoperability of the various nSHIELD 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 scenarios defined from WP7 and validated against the SPD metrics and requirements defined in Task 2.2.

*Task 6.2 Multi-Technology Validation & Verification (Task Leader: ED - Partners: ASTS, AT, ATHENA, HAI, MAS, S-LAB, THYIA, TUC, UNIUD)*

Testbed validation requires initially an assessment of the interface conformance following a specified test procedure. This is followed by testing attacks in wireless communication scenarios, as well as situation of communication overheads impacting on communication efficiency.

Validation of such integrated testbed is a challenging research task due to the heterogeneous environments in which the different modules (components) have been developed. In particular, each interface 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, field trial tests will provide a fundamental mean for validating all the nSHIELD SPD features and concepts. In particular, field trial results will be analyzed even taking into account the feedbacks received from potential end-users in real scenarios.

*Task 6.3 Lifecycle SPD Support (Task Leader: TECNALIA - Partners: ATHENA, HAI, S-LAB, TUC)*

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.

A SOA-based middleware can provide simple high-level APIs that hide the complexity due to the heterogeneity of systems which the applications will run on. Being targeted to embedded systems, the middleware must be lightweight enough to fit into such severely constrained devices.

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

For the development of the proposed framework, specific tools will be required 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. Finally, a set of tools will have to be developed to support security certification. Those tools will automate the Validation & Verification tasks associated with security certification.

**Deliverables**

*Public*

D6.5    Platform integration report (M34)

D6.6    Platform validation and verification (M36)

D6.4    Lifecycle and SPD Support Report (M30)

*Internal*

D6.1    Lifecycle and SPD Support Plan (M18)

D6.2    Prototype validation and verification (M20)

D6.3    Prototype integration report (M22)

---

**Milestones**

M4      Preliminary integrated Platform (M22)

M8      Final integrated platform and applications specific demonstrators (M34)

| Work package number | WP7 | Start date or starting event: | | | Month 18 | | |
|---|---|---|---|---|---|---|---|
| Work package title | SPD Applications | | | | | | |
| Participant no. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Participant short name | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 30 | 16 | 2 | 0 | 0 | 10 | 8 | 8 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 18 | 23 | 0 | 6 | 8 | 0 | 5 | 0 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 24 | 16 | 0 | 0 | 3 | 32 | 9 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 5 | 0 | 0 | | | | | |

**Objectives**

Validate nSHIELD platform on real application demonstrators

**S1**: Urban railways protection

**S2**: Voice/Facial recognition

**S3**: Avionic Computer that is an embedded system by definition: to provide a methods for dependable design in order to make possible a high "functionality" integration.

**S4**: There objective for SMN application scenarios is to provide proof of the concept by using 4 key building blocks for this scenario:

1.     new Streets and Building Lights (SBLs),

2.     Public and Private Transportation Means PPTMs,

3.     the future Internet of Things and Humans (ITHs), and

4.     Ubiquitous and/ Pervasive Computing (U&PC)

that have a common one, i.e., SPD enhanced functionalities as new technologies that are considered in details in this project. For this scenario the primary goal is to demonstrate an intelligent street and building lighting system that created a social network of humans and things.

**Description of work** (WP Leader: MAS)
The role of this Work Package becomes significant halfway through the project, when the

technology prototypes, developed and documented by WP3, WP4 and WP5, are ready and delivered. Starting from these inputs and taking into account some specific requirements defined in WP2, the four application leaders will produce their own integration plan (one for scenario D7.1.1, D7.2.1, D7.3.1, D7.4.1) to adapt the general purpose nSHIELD platform to their peculiarities and to select the most appropriate prototypal SPD modules. This plan will contribute to guide technology improvements to ensure they are compliant with their application scenarios.

Then, on M30, when the new technology prototypes are delivered, each application scenario works on building the demonstrators, that will be delivered (D7.1.2, D7.2.2, D7.3.2, D7.4.2) two months before the end of the project, and validated and verified through adequate reports (D7.1.3, D7.2.3, D7.3.3, D7.4.3) that will be the final output of the project.

This WP is divided into four Tasks, each one in charge of producing a specific demonstrator in a specific application scenario to validate the nSHIELD framework in significant industrial fields.

*Task 7.1 Railways security (Task Leader: ASTS - Partners: AT, ED, HAI, ISD, MAS, S-LAB, TELC, THYIA, TUC)*

The aim of this task is to adapt the nSHIELD framework for urban railways protection purposes. In fact, physical security systems for infrastructure protection have already been designed by the Task Leader Ansaldo for metro railways (mainly subways, i.e. featuring underground stations and tunnels); in these systems, heterogeneous intrusion detection, access control, intelligent video-surveillance and intelligent sound detection devices are integrated in a cohesive Security Management System (SMS). In this task will be developed a sample application of nSHIELD to a reference SMS architecture which includes a reduced yet significant set of devices employed for environmental sensing, event detection, situation monitoring, information fusion and countermeasure actuation. To achieve such an objective, some sensing devices will be converted into smart-sensors by integrating the sensor unit with the nSHIELD "standard" processing units (both hardware and software) at the node level; then the (possibly wireless) sensor networks will be integrated by the nSHIELD middleware before data is collected by the SMS and used at the presentation level. SMS will then process received data considering sensors as fully trusted information sources. The process is reversible, in order to provide bidirectional dependable communications, thus to include remote control commands from SMS to actuators (e.g. visual or audio alarm activation, access lock/unlock, etc.). A demonstration involving mobile and wearable devices to exploit context-awareness will be investigated too, its feasibility depending on the state of development of these SMS features by the end of the project.

*Task 7.2 Voice/Facial Recognition (Task Leader: ETH - Partners: TECNALIA, ISD, S-LAB, SESM, TUC, UNIGE)*

The objective of automatic human recognition is to quantify and demonstrate the efficiency of the automatic recognition of a person using his face and voice. The main goal is to increase the capabilities of biometric based recognition embedded systems in order to fulfil the requirements of modern security application context (strong authentication access control). The algorithms should be capable to identify the most significant features of the face, checking dimensions, proportions and extracting a visual biometric profile that is as much as possible unique for that person. The same approach will be used for the voice. A second part of the algorithm will compare these biometric profiles with the ones stored in the system database, trying to provide a result consisting in the name of a person and the matching percentage for both face and audio contexts. The efficiency and quality of the

system will be assessed from the study of matching results, both in simulated environments and real contexts. This study will be performed by an intelligent embedded system that automatically will examine the results and, evaluating them, will proactively correct and tune system parameters in order to maximize the recognition results.

The automatic human recognition scenario will be focused on the design and development of an application capable to automatically identify a person using biometric parameters: the photos of his face and the audio track of his voice. The application will be used to test the efficiency and quality of the algorithms for face and voice recognition developed in the project. The application, both for face and audio context, will be based on four important concepts: false recognition of positive and negative types, true recognition of positive and negative types. A false positive result happens when the system compares two biometric profiles, belonging to two different persons, and considers them as belonging to the same person. In this case the algorithm associates the real person with wrong biometric profile stored in the system database. A false negative result happens when two biometric profiles of the same person are compared and the system doesn't identify the person. On the other side, a true positive result happens when the biometric profiles of the same person are compared and the system correctly recognizes the person, vice versa a true negative result happens when the system doesn't find the acquired biometric profile in the database and doesn't recognize the person. Using these concepts, two different kinds of tests will be executed: simulation based tests and real tests. In the simulation based tests, we will create a set of synthetic scenarios so we will be able to control a certain set of parameters (resolution, light and noise dependency, exposure time, etc.) containing examples which will cover all types of possible results; in other words, we will stress the system with many biometric profiles some correct and other ones not correct. The test will put in evidence how many errors and correct recognitions will be obtained in a controlled environment. The real test will consists in positioning the acquisition embedded device (the system together with camera and microphone) in a real environment and observe the behaviour of the algorithms in real conditions. The biometric profile of the people that typically are present in the environment will be acquired and stored in the system database and the recognition test will be performed using the images and sound provided by the acquisition devices, independently from the light conditions, images resolutions, dimensions of the face image, images perspective, audio background etc.

*Task 7.3 Dependable Avionic Systems (Task Leader: SG - Partners: ED, HAI, S-LAB, SESM, TUC, UNIGE)*

An Avionic Computers or Avionic System is the principal Embedded System: a modern Avionic Computer/System need to include all the three aspect that are focussed in the nSHIELD project: Security, Privacy and Dependability.

The trend for modern civilian aircrafts is to support aircraft application with an Integrated Modular Avionic (IMA) platform. Platform that have to include always more functionality, starting from the navigation/mission functionality to the flight control function including also communication functionality.

To implement all the functionalities required therefore the IMA platform should be reconfigurable, reconfigurable means that IMA should be able to change the configuration of the avionic platform by moving application hosted on a faulty computing module to spare or other computing elements.

Re-configuration should therefore improve the operational reliability of the aircraft while preserving (or improve) current levels of safety (aircraft systems have to enforce stringent safety requirements that address the effects of failures on the life of passengers). Operational

reliability strong addresses the effect of failures on economical aspects of flight operations (i.e. the number of flight delays or cancellations caused by faulty computing have to decrease).

All the above it will be always more applicable to the Unmanned Aerial Vehicles (UAVs) that in the very near future they will have to share the same civil aerospace with private and commercial aircraft. It is only a matter of time, but UAV will take place in the civilian air space, in roles ranging from surveillance of terrorist and criminal activity to search and rescue to many other applications.

Avionics systems rely on computing platforms, and these platforms must be designed to provide the required levels of safety to passengers, crew, and maintenance staff and obviously for the overall flight functions (flight management (mission and navigation), vehicle management, flight management). The avionics functions must be sustained appropriately in order to ensure a safe flight, yet the hardware components on aircraft operate in a hazardous environment while running software that itself might contain defects.

Many techniques have evolved for constructing dependable computer platforms for avionics systems. Architectures have been developed that use various forms of redundancy and reconfiguration to allow continued operation when components fail. In addition, in many cases replicated components are separated within an airframe to prevent their simultaneous loss in the event that there is damage to the airframe. Various techniques are employed to aid in the correct construction of software, and software development is required to follow a rigorous process. Finally, various analysis techniques can be used to estimate some of the important probabilities related to dependability of computing platforms.

A dependable avionics system, therefore, is one that can be trusted to support safe aircraft operation.

A dependable avionics system need to include the following attribute:
  ➢ Reliability
  ➢ Availability
  ➢ Safety
  ➢ Confidentiality
  ➢ Integrity
  ➢ Maintainability.

In practice, the general dependability requirement for an avionics system or any of its components has to be refined and elaborated, finally being stated in terms of these six attributes.

With the IMA architecture (or distributed architecture) an avionics computer that implement flight management or flight control functions, needs to take in considerations also data confidentiality and data integrity, that are becoming increasingly important with increasing interconnectedness of dependable systems (i.e. also the communication control function: wide/narrow data link management system)

Either in an IMA or distributed architecture the fundamental components of avionics system architecture are computers (i.e. HW), data busses (i.e. Network) and the application (i.e. SW).

These components may be configured in various computing system architectures, where the purpose of an architecture is to meet the functional demands of the computing platform and the dependability requirements.

By using the nSHIELD framework, methods for dependable design and implementation will be provided, in order to make possible a high "functionality" integration that will make use of common resources for all the functions. Methods to be also shared with the other applications in order to come to a common method. Secure communications are a common problem for all the applications.

*Task 7.4 Social Mobility (Task Leader: MAS/THYIA - Partners: ED, ESIS, HAI, ISD, MAS, NOOM, S-LAB, TELC, TUC)*

Figure 3.3-3 provides the scenario for social mobility, where the SPD related aspects are:

- **Security:** Users need to be ensured that their data from embedded systems are securely handled.
- **Privacy:** Users will only share their data with people they trust, and in certain situations they will prefer to be anonymous.
- **Dependability:** The handling of data from embedded system depends on the user preferences, the situation or context and the desired goal.

All these aspects will be demonstrated in the social mobility scenario, through the introduction of context-aware trust networks. The social aspects *"it is fun", "we enjoy traveling together"* of the social mobility scenario are addressed through the *socialtainment equipment* in the vehicle, linking together yourself and your friends and colleagues from your trust network. This type of equipment is expected to be the *"Web 3.0"* in the future vehicle, and seen as being as substantial as navigation systems are today.



**Figure 3.3-3 - Social Mobility, adding socialtainment[102] to commuting and travelling**

First of all, the **detailed requirements** & **specifications** will be developed for SMN scenario **PPTMs** play an important role in social life of people. For example, bus, tram, trains, ships, cruisers, aircrafts, etc., are place that an individual can interact with other people and surrounding environments. The same when an individual is using his/her bicycle, motorcycle, car, camions, boats/yachts, etc. For example, the railways scenario e easily integrated in SMN scenario. Second, the future **ITH** is one of the most important areas of research in FP7.  Additionally, internet based social networking services have experienced an enormous growth over the past years. Simultaneously to the social networking services' triumphant advance, mobile devices in general and smart phones in particular have rapidly

---

[102] Socialtainment: The social act of communication and commuting with your friends and colleagues

penetrated the consumer market. Recent phones do not only exhibit considerable computing resources but also feature means for Internet access as well as wireless short distance communication such as Bluetooth, Wi-Fi, 60 GHz Radio. They seem to be the perfect platform to combine the market potential of traditional social networking services and the success story of mobile devices. **U&PC** devices are very tiny - even invisible - devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods - all communicating through increasingly interconnected networks. **SBLs** will have impact on streets and building lighting, since it is a European directive acting as new European standard.  In this project we are aiming to use a national initiative in Slovenian in city of Kostanjevica. Using electrical grid and combining it with possibility not only to manage intelligently the street lights, but also to communicate over different access technology (optical, radio and PLC) what is proved in OMEGA project http://www.ict-omega.eu/ represent an important technology breakthrough toward an implementation of SMN scenarios during this project and thus prove the concept. The SMN scenario to be proved includes: 1) SPD concept, 2) intelligent applications built on the nSHIELD system architecture, and 3) new street lights with LED or other solid state lighting technologies.
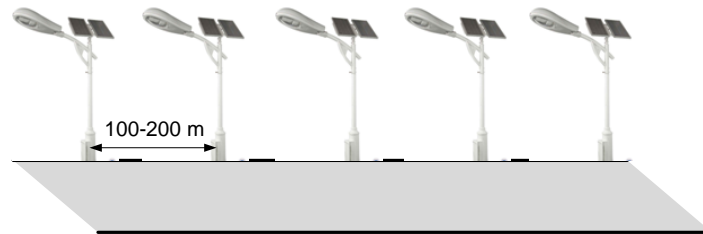


**The street lights with solid state technologies and solar panel.**

For this scenarios objective lie in ecodesign, embedded systems and SPD that contribute not only for social interactions of humans, but also in sense significant carbon dioxide reduction, significant energy savings, safety regulation, and SPD aspects. The scenarios will be demonstrated inside a big meeting room (indoor), or on the street in a village (outdoor). The lights will provide wireless optical down link.  The user will have different possibility for access technologies in up-link. For example UMTS, or short range 60 GHz radio communication link. Each lamp is connected on power electricity grid and provides down-link up to 1 Gbit/s. Additionally, on the street light will be installed two possible alternatives, 60 Ghz radio for communication during daylight. Combining with Radio over Fiber technology, which means connecting the street lights with fiber to the Central Station, and placing an inexpensive Remote Base Station (60 GHz radio link toward mobile users) on each street light it becomes a powerful infrastructure for social networking and accessing internet along the city roads.  An experimental, set-up will be used for demonstrator. This demonstrator will provide a platform for testing some applications and SPD issues over heterogeneous network.

**Deliverables**

*Public*

D7.5    Railways security demonstrator - integration report (M34)

D7.6    Voice/Facial Recognition demonstrator - integration report (M34)

D7.7    Dependable Avionic Systems demonstrator - integration report (M34)

D7.8    Social Mobility and Networking demonstrator - integration report (M34)

D7.9    Railways security demonstrator - validation and verification report (M36)

D7.10   Voice/Facial Recognition demonstrator - validation and verification report (M36)

D7.11   Dependable Avionic Systems demonstrator - validation and verification report (M36)

D7.12   Social Mobility and Networking demonstrator - validation and verification report (M36)

*Internal*

D7.1    Railways security demonstrator - integration and validation plan (M22)

D7.2    Voice/Facial Recognition demonstrator - integration and validation plan (M22)

D7.3    Dependable Avionic Systems demonstrator - integration and validation plan (M22)

D7.4    Social Mobility and Networking demonstrator - integration and validation plan (M22)

**Milestones**

M8      Final integrated platform and applications specific demonstrators (M34)

| Work package number | WP8 | 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 | SG | ASTS | AT | ATHENA | --- | ED | TECNALIA | ESIS |
| Person-months per participant | 10 | 3 | 4 | 4 | 0 | 0 | 8 | 1 |
| Participant no. | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Participant short name | ETH | HAI | ISL | ISD | MAS | MGEP | NOOM | SCOM |
| Person-months per participant | 1 | 6 | 14 | 0 | 3 | 11 | 0 | 3 |
| Participant no. | 17 | 18 | 19 | 20 | 21 | 22 | 23 | |
| Participant short name | S-LAB | SESM | SICS | T2D | TELC | THYIA | TUC | |
| Person-months per participant | 5 | 0 | 0 | 0 | 0 | 5 | 4 | |
| Participant no. | 24 | 25 | 26 | | | | | |
| Participant short name | UNIGE | UNIUD | UNIROMA1 | | | | | |
| Person-months per participant | 0 | 0 | 0 | | | | | |

**Objectives**

The objectives of WP8 are:

- Industrial Dissemination

- Industrial Standardization of innovative solutions;

- 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 MGEP)

*Task 8.1 Dissemination (Task Leader: MGEP - Partners: SG, ASTS, AT, ATHENA, TECNALIA, ETH, HAI, ISL, SCOM, S-LAB, THYIA, TUC)*

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. Proper dissemination and standardization plans will be internally delivered during the first six months. Dissemination activities will consist in the publication of all important results in well-known conferences and journals. The research issues of the project will be promoted through the organization of special sessions in conferences and workshops on the research topics of the project. The universities will contribute to the dissemination of knowledge by

producing scientific publications, by organizing and participating to dissemination events (international conferences and workshops) and by organizing an international journal special issue on the main research nSHIELD topics. Another important outcome of this task will be the annual delivery of the nSHIELD operational manual.

*Task 8.2 Standardization (Task Leader: SG - Partners: ASTS, AT, ATHENA, TECNALIA, ISL, MAS, THYIA, TUC)*

The standardization task is a key component to increase the impact in the SPD sector. Close interaction with standardization groups to monitor ongoing activities and the preparation of documents and proposals for standardization groups are planned.

As in the project the focus is to deliver missing scientific profound input to extend existing standardization for new intelligent SPD applications. The strong focus on verification, test and validation allows nSHIELD to provide scientific proofed selection guidelines for different technical proposals. This will result in guidelines, quality test procedures and certification rules to cover open needs of end-users.

The standardization activities will be led by the strong industrial partnership of the consortium, influencing new and existing standards and regulations, both at European and international level. Members of the project consortium are already members of standardization groups relevant to nSHIELD as listed in section 4.3.

*Task 8.3 Exploitation (Task Leader: ISL - Partners: ASTS, TECNALIA,  ESIS, HAI, ISL, MAS, THYIA)*

The target of this task is to promote and facilitate the exploitation of the achieved results. The partners, and, in particular, the large industrial companies will elaborate business plans to evaluate and explore the impact of the results on their business scenarios. These plans will be updated, in order to adapt them to the evolution of the project and the changes in the relevant markets. Issues of intellectual property and exploitation rights (including patents) will also be coordinated in this task, including potential synergies among the project partners.

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

To support the exploitation of the project results, two workshops will be organized to present to interested final users, industrial partners and other colleague institutions from the scientific community, the achievements of the project demonstrating the validity of the ideas. The first workshop will be organized once the technology prototypes will be available (month 18), and the second workshop at the end of the project (month 36). During these events, demonstration of nSHIELD abilities and technical lectures will be offered.

**Deliverables**

*Public*

D8.1    Web Site (M2)

D8.4    nSHIELD Operational Manual v1 (M12)

D8.6    nSHIELD Operational Manual v2 (M24)

D8.7    nSHIELD Operational Manual v3 (M36)

D8.9    Standardization Report (M36)

D8.8    Dissemination Report (M36)

D8.10   Final Exploitation Plan (M36)
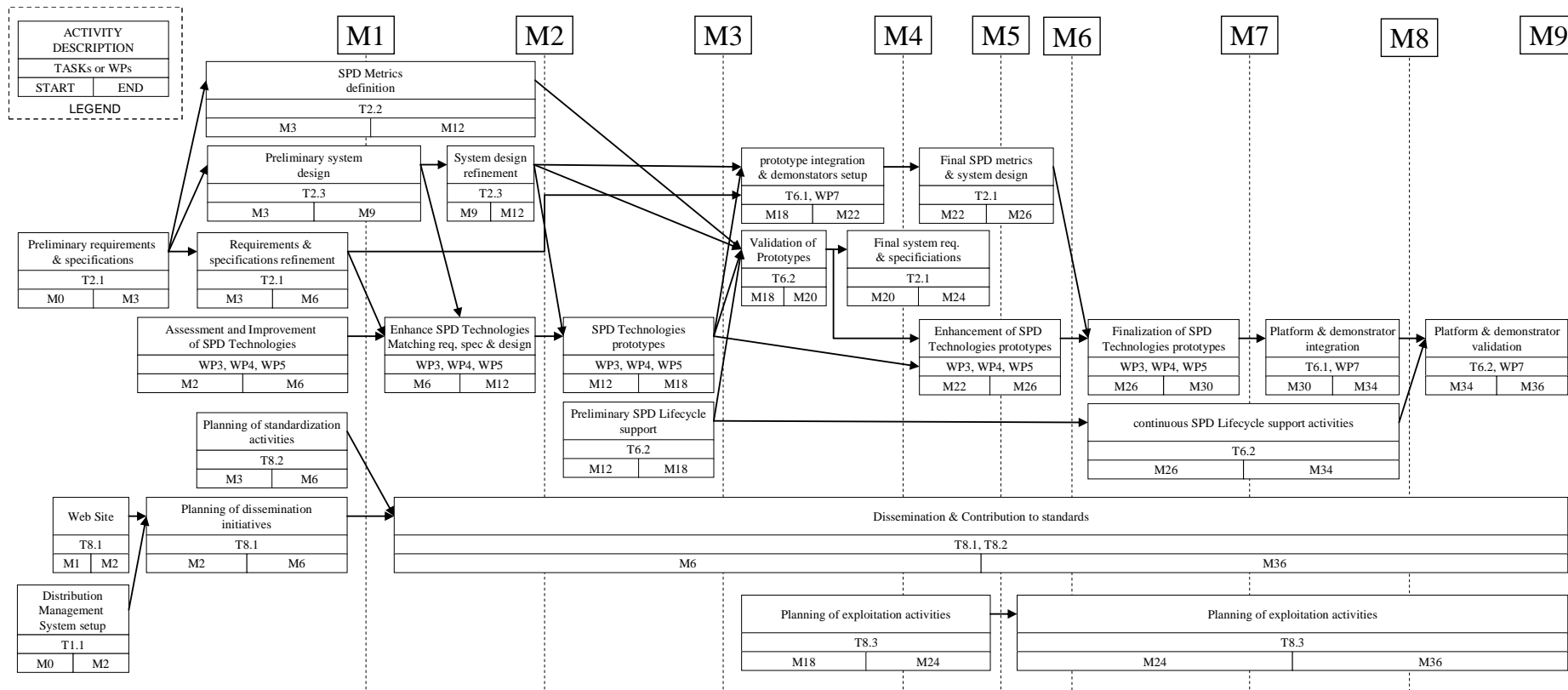
*Internal*

D8.2    Dissemination Plan (M6)

D8.3    Standardization Plan (M6)

D8.5    Preliminary Exploitation Plan (M24)

## Summary of effort

| Partic. No. | Partic. short name | WP1 | WP2 | WP3 | WP4 | WP5 | WP6 | WP7 | WP8 | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | SG | **40** | 10 | 16 | 10 | 10 | 10 | 30 | 10 | 136 |
| 2 | ASTS | 2 | 9 | 0 | 0 | 0 | 6 | 16 | 3 | 36 |
| 3 | AT | 9 | 8 | 22 | 0 | 0 | 19 | 2 | 4 | 64 |
| 4 | ATHENA | 3 | 6 | 8 | 10 | 14 | 21 | 0 | 4 | 66 |
| 5 | --- | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| 6 | ED | 11 | 12 | 0 | 6 | **43** | 17 | 10 | 0 | 99 |
| 7 | TECNALIA | 5 | 12 | 6 | 14 | 20 | 15 | 8 | 8 | 88 |
| 8 | ESIS | 0 | 0 | 0 | 0 | 0 | 4 | 8 | 1 | 13 |
| 9 | ETH | 1 | 2 | **25** | 0 | 0 | 3 | 18 | 1 | 50 |
| 10 | HAI | 15 | 22 | 4 | 15 | 27 | **32** | 23 | 6 | 144 |
| 11 | ISL | 10 | 0 | 0 | 34 | 18 | 24 | 0 | 14 | 100 |
| 12 | ISD | 2 | 0 | 58 | 0 | 0 | 6 | 6 | 0 | 72 |
| 13 | MAS | 0 | 0 | 0 | 0 | 0 | 7 | **8** | 3 | 18 |
| 14 | MGEP | 3 | 0 | 0 | 20 | 8 | 3 | 0 | 11 | 45 |
| 15 | NOOM | 0 | 0 | 0 | 0 | 0 | 1 | 5 | 0 | 6 |
| 16 | SCOM | 12 | 1 | 8 | **78** | 0 | 9 | 0 | 3 | 111 |
| 17 | S-LAB | 0 | 10 | 12 | 0 | 28 | 29 | 24 | 5 | 108 |
| 18 | SESM | 0 | 0 | 15 | 0 | 0 | 0 | 16 | 0 | 31 |
| 19 | SICS | 0 | 6 | 20 | 0 | 0 | 0 | 0 | 0 | 26 |
| 20 | T2D | 0 | 10 | 26 | 0 | 0 | 0 | 0 | 0 | 36 |
| 21 | TELC | 0 | 0 | 6 | 0 | 0 | 0 | 3 | 0 | 9 |
| 22 | THYIA | 13 | **20** | 30 | 12 | 19 | 12 | 32 | 5 | 143 |
| 23 | TUC | 4 | 10 | 30 | 14 | 16 | 10 | 9 | 4 | 97 |
| 24 | UNIGE | 0 | 0 | 30 | 25 | 0 | 0 | 5 | 0 | 60 |
| 25 | UNIUD | 3 | 3 | 12 | 12 | 0 | 6 | 0 | 0 | 36 |
| 26 | UNIROMA1 | 3 | 0 | 0 | 8 | 33 | 4 | 0 | 0 | 48 |
| **Total** | | 136 | 141 | 328 | 258 | 236 | 238 | 223 | 82 | 1642 |

## 3.1.4 - Pert diagrams

| ACTIVITY DESCRIPTION |  |
|---|---|
| TASKs or WPs | |
| START | END |

LEGEND

**M1  M2  M3  M4  M5  M6  M7  M8  M9**

| SPD Metrics definition | |
|---|---|
| T2.2 | |
| M3 | M12 |

| Preliminary system design | |
|---|---|
| T2.3 | |
| M3 | M9 |

| System design refinement | |
|---|---|
| T2.3 | |
| M9 | M12 |

| prototype integration & demonstators setup | |
|---|---|
| T6.1, WP7 | |
| M18 | M22 |

| Final SPD metrics & system design | |
|---|---|
| T2.1 | |
| M22 | M26 |

| Preliminary requirements & specifications | |
|---|---|
| T2.1 | |
| M0 | M3 |

| Requirements & specifications refinement | |
|---|---|
| T2.1 | |
| M3 | M6 |

| Validation of Prototypes | |
|---|---|
| T6.2 | |
| M18 | M20 |

| Final system req. & speciciations | |
|---|---|
| T2.1 | |
| M20 | M24 |

| Assessment and Improvement of SPD Technologies | |
|---|---|
| WP3, WP4, WP5 | |
| M2 | M6 |

| Enhance SPD Technologies Matching req, spec & design | |
|---|---|
| WP3, WP4, WP5 | |
| M6 | M12 |

| SPD Technologies prototypes | |
|---|---|
| WP3, WP4, WP5 | |
| M12 | M18 |

| Enhancement of SPD Technologies prototypes | |
|---|---|
| WP3, WP4, WP5 | |
| M22 | M26 |

| Finalization of SPD Technologies prototypes | |
|---|---|
| WP3, WP4, WP5 | |
| M26 | M30 |

| Platform & demonstrator integration | |
|---|---|
| T6.1, WP7 | |
| M30 | M34 |

| Platform & demonstrator validation | |
|---|---|
| T6.2, WP7 | |
| M34 | M36 |

| Preliminary SPD Lifecycle support | |
|---|---|
| T6.2 | |
| M12 | M18 |

| continuous SPD Lifecycle support activities | |
|---|---|
| T6.2 | |
| M26 | M34 |

| Planning of standardization activities | |
|---|---|
| T8.2 | |
| M3 | M6 |

| Web Site | |
|---|---|
| T8.1 | |
| M1 | M2 |

| Planning of dissemination initiatives | |
|---|---|
| T8.1 | |
| M2 | M6 |

| Dissemination & Contribution to standards | |
|---|---|
| T8.1, T8.2 | |
| M6 | M36 |

| Distribution Management System setup | |
|---|---|
| T1.1 | |
| M0 | M2 |

| Planning of exploitation activities | |
|---|---|
| T8.3 | |
| M18 | M24 |

| Planning of exploitation activities | |
|---|---|
| T8.3 | |
| M24 | M36 |

## Detailed Work Plan description

In order to clarify the timing (Gantt) and the relations (Pert) between the main workpackages and tasks, a detailed work plan organized in workpackages is described in this paragraph.

WP2 - starts on M0 and ends on M26. Task 2.1 starts at the early beginning of the project and releases on M3 a first version of system requirements and specification (D2.1.1). Taking into account the technology assessments done in WP3, WP4 and WP5 and the liaisons plan of WP1, the system requirements and specification are refined in D2.1.2 on M6. Task 2.1 wakes up again on M20, to elaborate a further refinement of system requirements and specification (D2.1.3) on the basis of the results coming from the validation and verification of Task 6.2 (D6.2.1) and the system integration report done in Task 6.1 (D6.1.1) and WP7 (D7.1.1, D7.2.1, D7.3.1 and D7.4.1). Task 2.1 ends on M24. Task 2.2 starts on M4 to identify the preliminary SPD metrics on the base of the preliminary system requirements (D2.1.1) and the SPD functionalities and technologies assessments (D3.1, D4.1 and D5.1) to deliver the D2.2.1 on M12. Task 2.2 starts again on M22 once the integration report (D6.1.1) and the application specific integration plans (D7.1.1, D7.2.1, D7.3.1 and D7.4.1) are available to refine the SPD metrics in D2.2.2 on M26. As for Task 2.2, Task 2.3 starts on M4 analyzing the preliminary system requirements and the available SPD technologies assessments. On M6 the system requirements are available in D2.1.2, thus after 3 months a preliminary architecture design is delivered on M9 (D2.3.1), and, after 3 months, refined in D2.3.2. The system design task starts again on M22 once the integration reports of WP6 and WP7 are available, to finalize the system architecture on M26 (D2.3.2).

WP3, WP4 and WP5 start respectively on M3, M4 and M5 and end on M30. These WPs start with 1MM of delay each other because there is a causality relation between WP3, WP4 and WP5. The node technologies chosen in WP3 will affect the technologies to be developed in WP4. WP3 and WP4 technology solutions will affect the WP5 technologies. In the first 2 months they focus on the assessment of SPD technologies to be selected, enhanced and integrated in the project, so that D3.1, D4.1 and D5.1 are delivered on M4, M5 and M6. Starting from M4 the assessed technologies are selected and improved accordingly with the system requirements provided by Task 2.1 on M3 and M6, with the SPD metrics provided by Task 2.2 on M12 and with the system architecture design provided by task 2.3 on M9 and M12. The tangible results provided by WP3, WP4 and WP5 will be a set of prototypal SPD modules ready to be integrated (D3.2, D4.2, D5.2) provided with the required documentation (D3.3, D4.3, D5.3) on M18. The validation results of the single prototypes will be available two months later (D6.2.1), and a preliminary integration result report will be provided on M22 (D6.1.1). WP7 will deliver the scenario specific integration plans on M22. And WP2 will refine the system requirements and specification, the SPD metrics and the system design on M24 and M26. Taking into account these proceedings the technology workpackages start again their R&D activities on M22 to develop and deliver on M30 an improved version of the prototypes (D3.4, D4.4, D5.4) and relative documentation (D3.5, D4.5, D5.5) solving all the problems raised by the analysis of the previous prototypes.

WP6 starts on M12 and ends on M36. Task 6.1 starts on M18 once the technology prototypes have been released by WP3, WP4 and WP5 and the SPD lifecycle support plan is available. An integration phase and a compliance analysis with the preliminary nSHIELD architecture design provided by WP2 are performed and the results delivered on M22 in D6.1.1. The second integration phase of Task 6.1 starts on M30 once the enhanced versions of the prototypes are ready. After four months, on M34, the final nSHIELD platform integration will

be delivered (D6.1.2) and ready to be validated against the specifications and verified on different application fields. Task 6.2 starts on M18 to validate the prototypes provided in WP3, WP4 and WP5 on the basis of the specification provided by WP2. In two month (M20) the validation report (D6.2.1) is delivered. Task 6.2 starts again on M30 once the second integration phase is terminated and the nSHIELD platform must be validated and verified. On M36 the D6.2.2 is delivered and the task ends. Task 6.3 starts on M12 once the SPD metrics and the reference system design have been released by WP2. After 6 months the lifecycle SPD support plan is delivered (D6.3.1). Once the SPD metrics and the system design are fixed and delivered (D2.2.2 and D2.3.3 on M26) the activities of Task 6.3 starts again to assess the SPD lifecycle during the development of the nSHIELD platform and deliver the final report (D6.3.2) on M30.

WP7 starts on M18 once the technology prototypes developed and documented by WP3, WP4 and WP5 are available and the SPD lifecycle plan has been delivered. From these inputs after four months (M22) each application scenario delivers its own integration plan (D7.1.1, D7.2.1, D7.3.1, D7.4.1) to adapt the general purpose nSHIELD platform to their peculiarities and to select the most appropriate prototypal SPD modules. From M22 to M30 the WP7 tasks follow the WP2, WP3, WP4 and WP5 improvements to ensure they are compliant with their application scenarios. On M30 the new technology prototypes are delivered and in the following four months each application scenario works on the demonstrator setup. On M34 the demonstrator are delivered (D7.1.2, D7.2.2, D7.3.2, D7.4.2) and ready to be validated and verified. From M34 to M36 WP7 activities focus on the preparation of the validation and verification reports (D7.1.3, D7.2.3, D7.3.3, D7.4.3) to be delivered at the end of the project on M36.

WP8 provides all the needed knowledge exchange and industrial validation activities from M0 to M36. Task 8.1 starts on M1 to setup in one month the official project web site (D8.1.1) and to prepare and deliver on M6 a detailed dissemination plan (D8.1.2) based on the information already available on M3: the technologies assessments (D3.1, D4.1, D5.1) and the liaisons plan (1.2.1). Task 8.1 also delivers every 12 months an updated nSHIELD operational manual (see section 4.2) that collects only the essential information from the results of other workpackages (mainly WP2, WP3, WP4 and WP5) to setup a nSHIELD compliant system. Task 8.1 ends on M36 with the delivery of the dissemination report (D8.1.6). Task 8.2 starts on M3 once the technology assessment of the SPD technologies, the preliminary system requirements and the liaisons plan are available. In the next three months a standardization plan (D8.2.1) is delivered. The standardization activity continues till the end of the project (M36) when the standardization report (D8.2.2) is delivered. Task 8.3 starts on M18 once the first tangible results of the project are already available: the technologies prototypes, the system architecture and the SPD lifecycle. The preliminary exploitation plan (D8.3.1) is delivered on M24. In the last year of the project the nSHIELD platform and prototypes are refined and a final, detailed exploitation plan (D8.3.2) can be produced on the base of the achieved results on M36.

## 3.1.5 - Known risks and contingency plan

The known risks in nSHIELD 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.

### 3.1.5.1   Research and technological risks

Due to the high number of SPD technologies that will be developed and integrated in the nSHIELD 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, nSHIELD 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 nSHIELD 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 nSHIELD 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[103]. Moreover the nSHIELD 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.

---

[103] "*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 nSHIELD performances with the minimum effort.

### 3.1.5.2   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 nSHIELD 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 nSHIELD with respect to the standard integrated SPD solution would be covered, or that all the features and functions of nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD infrastructure to the new standard. The nSHIELD components are very modular and composable, and the necessary adaptations may be largely a case of modifying the external interfaces.

### 3.1.5.3   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 nSHIELD, 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. nSHIELD 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.

### 3.1.5.4  *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 nSHIELD 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, nSHIELD 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.

### 3.1.5.5  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 | nSHIELD 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 | nSHIELD impact on the standards would be very low | Adapt the nSHIELD 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

Competition in the market sector
The market sector envisaged by nSHIELD is typically covered by the providers of management platforms for embedded systems. These providers such as ABB, SIEMENS, GE, IBM, Telenor Objects and many others concentrate on the industrial roll-out of sensors, providing sensor platforms for access of the sensors.
Their focus is on access, and the only security is based on access authentication, usually through token or password-based access.

Research in security, privacy and dependability has taken place in many research projects, but their market access has often been hampered through a non-integrative approach. Industrial partners involved in the nSHIELD project were invited for demonstration of the capabilities, and not for dissemination of the results.
The goals of nSHIELD in providing security, privacy and dependability are advanced with respect to the sensor platform providers. We expect that our concepts will be launched together with our partners, thus providing us with a competitive advantage

The demand for security systems is growing more and more each year and respond to that question is often required to develop a fully integrated system, particularly in urban centers

It is expected that the results obtained with nSHIELD, applied to systems for monitoring and protection (railway and urban transport infrastructure, voice and facial recognition, social mobility and surveillance avionic system), will allow a reduction of costs and development time and an improvement in meeting the requirements of the SPD and the level of integration between heterogeneous elements

In addition, the project will probably have an additional advantage to higher system reliability and a lower time-to-market than competing products, with a consequent increase in sales

Only for the railway and urban transport infrastructure (ASTS information) the benefits in the period 2014-2018, can be estimated at approximately € 4-5 M € of incremental revenue on products and services that will benefit from innovation brought by the project. At this estimation should be added the value of orders dedicated to the security. In fact solutions dedicated to a better or integrate security is often a prerequisite for the acquisition of much larger orders.

nSHIELD technology platform acceptance from standardisation bodies
nSHIELD focusses on the strong interaction with industry and the related standardisation. The industrial partners in the following chapter have provided an own exploitation plan.

The main input for standardisation it towards strong partnership with industrial actors. The most successful standards have been created in the Telecom industry, where more than 5 billion people are connected towards mobile networks, and all of them heading towards LTE as a common standard.

nSHIELD partners will prolong the standardisation through a tight collaboration with selected Telecom partners and contribute to ETSI.

The approach that nSHIELD will adopt will be based on metrics that will be uniformed on all the three SPD layers (node, network, middleware) that form the nSHIELD system, in order to define a single level of SPD assurance for the whole system.

In this respect the process that leads to the definition of the level of SPD, could be seen as a process of evaluating a system in order to verify whether or not it meets the assumptions made in the definition (or development) stage. Of course, the rules have to be extracted from an existing catalogue and that the procedures for verify are well defined, in this case nSHIELD will define a standard that would lead a generic system embedded obtaining certification of a hypothetical "SHIELD compliant".

This approach has been derived in part from a globally recognized standard (ISO15408), so any system SHIELD compliant with minimal effort might conform to that standard.

In addition Telenor Objects is associated partner in nSHIELD, and provides their M2M platform for interoperability testing. The Norwegian partners have already access to the platform, and collaborate with Telenor on potential extensions.

In ETSI the functional architecture of an interoperable platform is defined through TS102.690, where Telenor directly contributes. Movation, as being an ETSI member, will join forces with Telenor and suggest extensions in the TS102.690 follow-up activities.

The Europe-wide spreading of partners in nSHIELD opens for national standardisation, where the platform components developed by nSHIELD will be made available for cooperation. In Norway the nSHIELD partners are presented in the steering board of the Norwegian Mobile Association, where we identify national test-beds.

As last Ansaldo STS has for years been involved in several international committees to standardize the process and / or product (CENELEC, UIC, etc..), therefore by participating in these committees ASTS will present the typical characteristics of the nSHIELD architecture and will support its adoption in terms of specific standards and guidelines.

## *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 nSHIELD 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 nSHIELD, will be highlighted in order to show the overall market potential of the nSHIELD 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

nSHIELD 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 nSHIELD 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[104] 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 nSHIELD is so necessary. Moreover, the growing number of breaches[105,106,107,108] 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.

nSHIELD 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.

For instance, trusted platform modules (TPM) are already used in many modern computing systems (laptops, etc.): but many people continue to consider risky to use such devices for

---

[104] see ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402464encfull.pdf
[105] 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
[106] keeloq crack - http://www.wired.com/threatlevel/2007/08/researchers-cra/
or http://hackedgadgets.com/2007/09/08/keeloq-remote-vehicle-entry-system-cracked/
[107] Dutch passport readout - http://www.rfid-nSHIELD.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.
[108] iPhone SMS bug
http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html

their private sensible information. The complete acceptance and trustiness in TPM can bring great benefits to all the people using such devices. nSHIELD activities aimed at integrating TPM in embedded systems is expected to produce new architectures for the use of TPM and to address performance and security issues.

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. nSHIELD 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 nSHIELD 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 nSHIELD 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.**

nSHIELD 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 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. An example will be Selex Communication (SCOM). Taking advantage from nSHIELD framework, the TETRA[109] 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 nSHIELD technologies will be addressed. Moreover, such an approach will allow nSHIELD-oriented TETRA technology to broaden market perspectives and applications towards the development of innovative, secure, dependable and privacy-oriented transmission/communication modules.

---

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

The innovative nSHIELD 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 nSHIELD will concentrate mainly in achieving a common framework for SPD accounting new composability mechanisms. In this respect nSHIELD fully address these topics in WP2 (Task 2.1 and Task 2.3) where the requirements, specification and design of nSHIELD conceptual framework are 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 nSHIELD 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 nSHIELD consortium can be used in the Common Criteria (CC, ISO/IES 15408) evaluation and certification process (CEM, ISO/IES 18045). nSHIELD consortium will, furthermore, provide contributions from the project results to (1) 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 nSHIELD 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: AT 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).**

nSHIELD 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*

WP7 (SPD applications) set-up four demonstrators 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

nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD-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 nSHIELD 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 nSHIELD 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 result 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 nSHIELD 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.

nSHIELD 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 nSHIELD SPD requirements to CC security functional and assurance requirements, while evaluators will be able to use checklists issued by nSHIELD to verify security claims, and the automated tools developed by the nSHIELD consortium will produce the necessary evidence for these claims. In this respect nSHIELD 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 ...).*

nSHIELD 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 application could stress particular aspect of SPD by using the nSHIELD framework specialized with opportune nSHIELD 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.

nSHIELD 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

nSHIELD 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 raises several unique and challenging SPD issues to be explored highlighting the composable and modular aspects of the solution.

nSHIELD 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[110,111,112,4]) the nSHIELD 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

---

[110] "Semiconductor Trends and Opportunities for Europe", March 2009.
  http://www.semi.org/cms/groups/public/documents/web_content/ctr_029000.pdf
[111] "*ESIA 2008 Competitiveness report*", EECA, 2008.
  http://www.eeca.eu/data/File/ESIA_Broch_CompReport_Total.pdf
[112] "*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

account similar experiences in software engineering[113], we can estimate a time-to-market reduction up to 40% adopting the nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD, 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.

- nSHIELD 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, recognition, avionics and social mobility; 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.

  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 nSHIELD 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 nSHIELD 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 nSHIELD to validate the project results, could be given in order to show the overall market potential of the nSHIELD solutions after implementation in the pilot scenarios:

*Example 1 –The Railways Security Scenario*

---

[113] 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.

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 nSHIELD objectives and scope of work, both vital and no-vital railway systems must fulfil 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 – Social Mobility and Networking*

Why social mobility? SAP reports in the 2009 sustainability report that the carbon dioxide footprint is reduced by 15 %, but that the total commuting and travelling part accounts to 45% [SAP, 2009]. The commuting amount of 6 % as presented in figure is underrepresented, as the use of corporate cars with 33 % includes a substantial part of commuting. The Environmental Protection Agency (EPA) published various scenarios, indication that a vehicle emission reduction of 27 % is suitable within 2030, looking primary on technology advances.
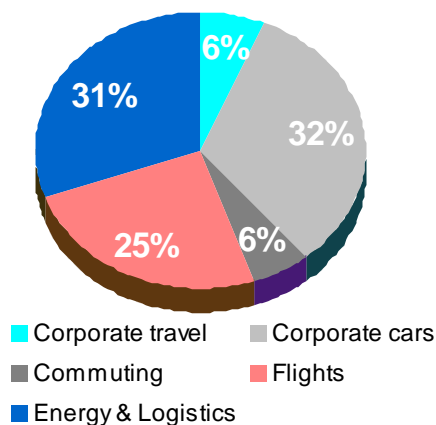


**Figure 4-1 - SAP carbon dioxide footprint, segment usage [SAP, 2009]**

We believe that another 8% of $CO_2$ can be reduced through a change of attitude and behaviour of people, thus 'social mobility'. The principles are outlined in Figure 3.8 (see section 3), where emphasis is put on making a travel becomes a social event, with people communicating with people of their trust network.

The potential of social mobility accounts for 1.2 billion Euro (for Norway), which is further elaborated in the business section. For the use-case we envisage an advanced city trying to become $CO_2$ neutral will adopt the nSHIELD results. With more than 20 % of public employees the city has plans to substantially reduce the travel-related $CO_2$ budget, looking for advanced solutions.

Sustainability is the holistic management of societal, environmental, and economic risks and opportunities for increased short- and long-term profitability. The sociality mobility scenario with its innovative transport pooling system contributes to every aspect of sustainability. It

advocates a change in mind set and overall behavioural shift towards sharing resources. By doing this, the scenario also has the potential to contribute in enhancing social interaction and bondage. The sharing of resources has significant environmental impact through the reduction of Greenhouse Gas (GHG) emission. Transport sector has been seen as one of the contributors of GHG emission. The contribution of transport in total EU GHG emission rose from 17% to 24% in 2004 and in the world transport sector accounted for 13.5% of GHG emissions in 2005. Another study found that shifting towards renewable and low-carbon energy can contribute little in comparison to bringing efficiency in energy usage management in the reduction of GHG emission. The report said efficiency in energy usage contributes the most (up to 74%) in the reduction of CO2 emission while it is only 14% by shifting from oil to natural gas and 12% by strongly introducing renewable energy. The social mobility scenario has economic impact as it contributes by lowering cost and increasing savings. All these can bring competitive advantage to businesses, enterprises and organizations that ultimately lead to sustainability.

*References*

[SAP, 2009] SAP Sustainability Report,

http://www.sapsustainabilityreport.com/, [assessed 25.8.2010]

[EPA, 2010] EPA Analysis of the Transportation Sector: Greenhouse Gas and Oil Reduction Scenario, Environmental Protection Agency, March 2010, www.epa.gov/oms/climate/ GHGtransportation- analysis03-18-2010.pdf, [assessed 23.8.2010]

### 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, nSHIELD based, in the pilot application scenarios:

*Railway market impact - reduction of costs*
As mentioned in the exploitation plan, Ansaldo STS aims at exploiting nSHIELD 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 nSHIELD 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 availability of inexpensive hardware support of ECC will also enhance the quality of service in railway communications infrastructure, allowing wider bands and more secure access procedures. 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 nSHIELD 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 nSHIELD 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 nSHIELD to other types of ES developed by Ansaldo STS.


Voice/Facial Recognition *market impact*
One of the reference market segments related to SPD application for WP7 of nShield project is "Voice and Facial recognition". This is a part of a wider market scenario that is the Area Access Control and Identification. Eurotech Group is interested in this market in terms of providing new solutions, new smart technologies and integration with existing devices. The spread of such systems currently affects a limited number of areas for which, however, are already characterized by rising market expansion. At the moment the human identification and access control is mostly entrusted to specialized personnel that require training and regular updates for new procedures. Then it has to be considered the amount of costs related to integrate the human recognition procedures with other features such as the area access policies application, access permissions identification, tracking movement of people in a building or in a set of buildings. Eurotech is interested in creating and developing an innovative products line of embedded systems for secure access control and dependable identification that reduces the use of human resources, allowing the automation of these kinds of operations, offers an integrated management of services, processes and resources required for the proper access of buildings and resources such as military area, airports, bank agencies and public administration offices, and it could be extended to other relevant services not explicitly related to the military and public sectors. Moreover, this new set of solutions is open to be integrated with existing devices by customer. The nShield project offers a chance to explore the developing possibilities of this market scenario, using the SPD architecture as a starting point, where Security, Privacy and Dependability are "built in" functionalities. This could lead to a considerable reduction in terms of integration of embedded systems, providing opportunities for easy management of privacy and data security.


*Dependable Avionic Systems market impact*

Avionic computer represents one of the cores of Selex Galileo products, therefore the technological plan strategy is always focussed to keep them up technological evolution.

With the implementation of the nSHIELD concepts in the avionic computers based on IMA platform allow a cost reduction in development, due to the share activities. Emphasis is placed on the development of key sensor and processing technologies (both HW and SW) to support a fully integrated open architecture sensor/processing package

The actual definition of the functional requirements is very much work in progress and will vary depending on whether the platform is at the safety or non safety level.

Related investment in all the LoBs (Line of Business) in Selex Galileo will take benefit from the nSHIELD project.

Widespread use of open systems and architecture joined with the nSHIELD architecture will facilitate the rapid cost-effective introduction of always new technologies into avionic computer.


*Social Mobility market impact - new products*

Through Social Mobility scenario, the implementation of nSHIELD project has the potential to bring new service to market. The scenario can bring in significant economic benefit by reducing cost in the transport sector. According to the following figure, in Norway road transport contributed about 87% of the total available transport modes including road, railway, water and air transport in 2007. Despite measures taken by the states to the reduce number of private cars, 88% of the road transportation is private cars.
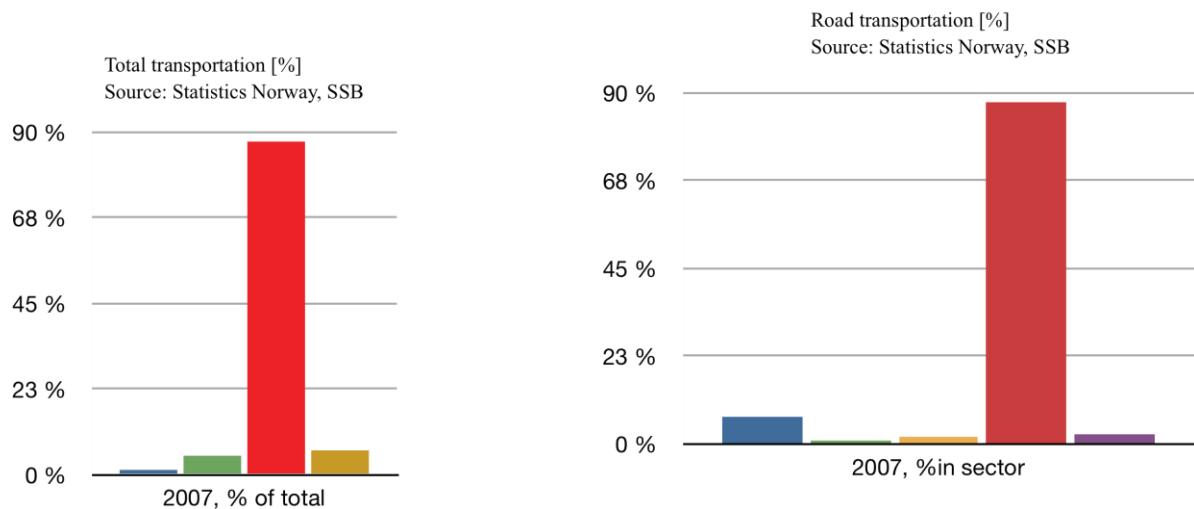


The technological advancement in transport sector (e.g. smart vehicle) may account for up to 27% reduction of transportation cost[114]. Social Mobility scenario has the potential to bring behavioural changes and that can contribute up to 8% of the reduction of private car usage. The following table estimates the overall cost reduction Social Mobility scenario can contribute in the transport sector of Norway. It has been estimated at 1.2 billion Euro according to the commuters number in 2007. This can be a significant business prospect not only in Norway but also all over Europe especially when the primary energy source of transport sector is depleting and its cost is rising.

| | Total commuters with private cars or motorcycle [MPersonKm] | Work related commuters (80% of total) [MPersonKm] | Technical reduction (~27%) [MPersonKm] | Behaviour change (~8%) [MPersonKm] | total reduction [MPersonKm] |
|---|---|---|---|---|---|
| | 54,639 | 43,711.2 | 11,802 | 3,497 | 15,298.92 |

| | | | | | |
|---|---|---|---|---|---|
| costs (1 km = 3 NOK) MNOK | | 131,134 | 35,406 | 10,491 | 45,897 |
| costs (1Euro=8.1 NOK) MEuro | | 16,189 | 4,371 | 1,295 | 5,666 |

---

[114] Analysis of the Transportation Sector: Greenhouse Gas and Oil Reduction Scenarios, the Environemental Protection Agency, February 10, 2010.

## 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 nSHIELD innovative approach to the design of SPD-based ESs. European industrial leaders in the field of ESs, <u>which are represented in large part within the nSHIELD consortium,</u> will assure a proper development and exploitation of nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD 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, nSHIELD 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 nSHIELD 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, nSHIELD "built in" platform can be easily exploited in order to enhance security, privacy and dependability features.

Moreover, the adoption of nSHIELD 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, nSHIELD'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 nSHIELD 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*

**nSHIELD 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 nSHIELD consortium plans in terms of *exploitation, dissemination* and *patents*.

### 4.2.1 - Dissemination plan

nSHIELD *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 nSHIELD 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.

***Workshops and seminars***: participation to IST cluster events and European concertation meetings (ARTEMIS), participation in workshops and conferences organized by IST, and other important international organization like IEEE will represent another key dissemination activity for nSHIELD partners. Moreover, each academic partner, by means of publications of obtained innovative scientific results, will promote and spread nSHIELD SPD features through the organization of seminars in their respective university. As well, every year, a nSHIELD workshop will be organized by coordinating institution and partners in order to share with the scientific community and with ESs stakeholders achieved results. Nevertheless, such a sharing of innovative strategies in the design of ESs will lead to a continuous refinement of nSHIELD implementation influencing the development of the proposed architecture both at market innovation and market impact level.

*Workshops*

- Workshop on Cryptographic Hardware and Embedded Systems (CHES[115]);
- Workshop on RFID Security (RFIDSEC[116])

---

[115] http://www.chesworkshop.org/
[116] http://www.cosic.esat.kuleuven.be/rfidsec09/

***Publications:*** project results will be disseminated by paper submissions to major European and worldwide journals and reviews. The nSHIELD 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);

- IEEE International Symposium on Circuits and Systems (ISCAS)

- Embedded System Conferences (ESC)

- IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)

- IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)

- 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

- IEEE Transactions on Computer

- IEEE Transactions on Reliability

- IEEE Embedded Systems Letters

- ACM Transactions in Embedded Computing Systems (TECS)

- IEEE Transactions on Signal Processing

- IEEE Signal Processing Letters

***nSHIELD Operational Manual:*** nSHIELD partners will prepare and spread a nSHIELD operational manual. This manual will be made available in six languages: Italian, Spanish, German, and Czech as nSHIELD consortium most represented languages and English and French as European Community official languages. The operational manual will represent an easy and effective dissemination of the project strategy not only towards ARTEMIS community (each ARTEMIS member will receive a copy of it) but also at local, regional and national level. In fact, each partner will be invited to spread the operational manual within its national borders both and institutional and industrial level aiming at disseminating the good practices and relevant results obtained by nSHIELD. Thus activity will promote the development of new nSHIELD-based or nSHIELD-oriented ESs applications by industries

not involved in the project as well as the definition of SPD-oriented policies in the design of ESs from local, regional and national authorities.

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

Moreover, nSHIELD 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 nSHIELD Italian partners. nSHIELD goal will be to reinforce and enlarge such working groups involving new stakeholders, also coming from other member states and in particular from nSHIELD'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 nSHIELD 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.
nSHIELD 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   *Individual industrial exploitation plans*

<u>*SELEX GALILEO:*</u> the results of the nSHIELD project will be used to enhance the Selex Galileo innovation activities with the purpose of developing prototypes and products and enabling the enhanced of a the avionic family computer to be proposed on national and international markets. Furthermore Selex Galileo 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.

<u>*Ansaldo STS:*</u> The results provided by the application of the nSHIELD 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, nSHIELD 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, nSHIELD 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 nSHIELD 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 nSHIELD 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.

*Acorde Technologies:* 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 nSHIELD 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.

*Elsag Datamat:* the results of the nSHIELD 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.

*Fundacíon Tecnalia Research & Innovation:* TECNALIA will use the knowledge and results generated in nSHIELD 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

exploitnSHIELD 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.

TECNALIACenter 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 TECNALIACenter 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 nSHIELD 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 nSHIELD 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 nSHIELD results | 150 | 400 | 900 |
| SMEs using nSHIELD results | 10 | 40 | 60 |
| Expected Economical income for TECNALIA from nSHIELD 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 nSHIELD | 2 | 5 | 8 |

_Eurotech:_ Eurotech will promote project results following nSHIELD 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 nSHIELD 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 nSHIELD topics, both in Europe and world-

wide. nSHIELD 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. nSHIELD 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, nSHIELD's results will be used by ETH Lab in further research activities referring to the mentioned areas of scientific interest.

*ESIS Norge* will exploit the outcome of the SHIELD project through its electrical motorbike that is a part of the Social Mobility scenario of this project.  The motorbike is fitted with several sensors and an on-board PC. When the motorbike has its own IP address and can be discoverable through Internet, privacy can be a concern. ESIS is specifically interested to the SPD nodes and the integration to middleware outcomes of the SHIELD. The exploitation will make the European market aware of the competence of Norwegian competence in low-footprint energy in transport as well. This may involve new partners for the commercialization of low-footprint transport communication systems

*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 nSHIELD 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 nSHIELD 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 nSHIELD findings and market changes. Currently HAI has particular interest in exploiting the technologies developed by nSHIELD in the areas of ad-hoc networks, sensor networks, services over dynamic networks, systems integration and lifecycle support.

*Indra*:
Indra is the premier IT company in Spain and a leading IT multinational in Europe. Indra Software Labs is the network of Software Labs of Indra that develops customized software solutions for Indra's markets including: Transport and Traffic, Energy and Industry, Public Administration and Healthcare, Financial Services, Security and Defence and Telecom and Media.
Direct exploitation of project results will consist on applying the nSHIELD concepts and methodology to Indra's product lines, in particular in industrial sectors with European leadership. Indirect exploitation will build on the huge knowledge developed by the project to be then re-used in education materials, trainings, technology transfer, spin-off activities, consultancy services, follow-up project, IP revenues, etc. With nSHIELD results Indra will be

able to improve its products and build embedded solutions that take into account security, privacy and dependability issues in applications, networks and services.

ISL will use the results of the project in several ways.

**Market position:** Increase in the activities of ISL in the field of security and in particular embedded security.

The aids received for this project will significantly increase the knowledge of ISL in the security domain and therefore will increase the activity of the company in this area. Through the participation in this project the company will boost the viability of such activities whilst improving the technological capacities of the company.

The involvement of ISL in ARTEMIS projects seeks to significantly increase the integration and exploitation of embedded systems in the different business lines of Indra's group. All the main business lines of Indra (Infrastructures, Transport, Energy, Defence, Water and Urban and Environmental Services) can benefit from a more intensive use of secure embedded systems, which can provide a technological added value to these business lines and help to achieve a market differentiation from all of our competitors.

In this sense Indra, through its ICT research group, has been carrying out several research activities in the embedded systems domain, so the aids received for this project will help us to consolidate the efforts and resources committed to this particular technological field.

**Competitiveness:** Increase in the market capacities of ISL in the embedded security sector

With the results obtained from the project ISL and as a consequence Indra will be able to only obtain new products and increase our market capacities in the embedded security sector. In addition ISL will be able to achieve major advances in the scientific and technological foundations that support such products and market capacities.

*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.

*MOVATION AS:* is a Norwegian platform for open innovation. Movation will exploit the results of SHIELD for ensuring secure and dependable operations of the Norwegian Railway administration through the Railway scenario of this project. In this regard, Movation will specifically make use of the SPD nodes, Integration to middleware and SPD application outcomes of the SHIELD project.

Movation through its industrial alliances will exploit the results for developing innovative use cases in different areas that will make significant impact on creating new business avenues for industries. The inner circle members of Movation, 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 technological advancements and outcomes of SHIELD, and will bring it into one of these companies.

*NOOM AS* has communication interfaces to services. The results of SHIELD will contribute to enhancing NOOM's capabilities by enabling the communication to Internet of Things. Thereby NOOM can expand its product portfolios

*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 nSHIELD 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. nSHIELD results will be used within Selex-Communications further research activities.

*SESM*: will exploit the nSHIELD 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.

*T2Data*
T2Data aims to use the nSHIELD secure boot and software management routines in their product offerings. The final nSHIELD architecture will be evaluated and discussed with large end customers. Especially, the routines for secure product life cycle management are foreseen important in future products.

*TELCRED*
Telcred aims to use the secure firmware installation and upgrade technologies in their future access control products. Similar the novel cryptographic solutions will be evaluated for constrained embedded lock units.

*THYIA:*

is aiming to explore embedded technology and SPD approach that are key technologies for SMN scenario. An indoor and outdoor demonstrator will be developed in which a heterogeneous network infrastructure will be used for proof of the concept for these scenarios. The short range communication will be achieved by 60 GHz radio, optical fiber technology, and power electrical grid that allow continuity of services over different access technologies. Exploring new SPD technologies for such complex system infrastructure is a primary aim of THYIA in this project. For testing some sensor technologies (e.g., smart dust and video surveillance) the use micro and nonoelectronics that required 3D integration is required.

The table below gives some motivations why 3D integration for embedded system design is important.

| 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**

Thus, the main interest of THYIA in the exploitation plan lies in testing SMN scenarios, and the use of specific sensor platform, and other devices that will be delivered in the market after the termination of the project.

### 4.2.2.2  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.


_Swedish Institute of Computer Science_
Swedish Institute of Computer Science will make publication in highly ranked conferences on new protection mechanism in constrained embedded systems. In particular, we expect novel results with respect to hypervisor protected embedded systems and TPM based secure boot as well as platform software protection. The demonstration system developed within nSHIELD will be showed at large national and international events as well as to the SICS Swedish industry partners


_Technical University of Crete:_ will exploit the results in numerous ways. Firstly it will publish them in the relevant conferences and journals. Secondly, TUC is the co-ordinator of a national network of research institutes and companies working on networking; therefore, the

lessons learnt within this project, as well as the particular skills, will be disseminated nationally within the framework of the seminars and workshops organized by TUC. Moreover, the specific topics of nSHEILD and the experience gained from it will be parts of a number of graduate courses taught at Technical University of Crete; in this way the experience gained will be disseminated to all the M.Sc. and Ph.D. students of the department. Furthermore, TUC will exploit the achieved results and use them within new research projects in the FP7 framework. The institute will use the obtained know how, to investigate further new concepts like visual sensor nodes, location problems, streaming in a sensor environment, etc. So although exploitation in the context of an academic partner must be understood in a more broad sense, the importance and commitment are comparable to that of the industrial partners. This project will also facilitate the relationship between TUC and the industries and universities at a European level, providing an optimum framework for future collaborations. Finally, the skills gained within nSHIELD will be utilized in the numerous consulting tasks that TUC already takes up, for National and European Large Companies and SMEs.

*Università di Genova:* will publish obtained results in referred International conferences and journals focusing particularly: 1) 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; 2) on advanced research on embedded cryptographic platforms. Moreover, the University of Genoa research groups, 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 nSHIELD developed solutions. Finally, relevant effort will be devoted to the creation of the nSHIELD Manual, particularly concerning the SPD metrics description and to the institution of specific seminars concerning part of nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD 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 nSHIELD a strong expertise in patents production: this is the case, for example, of University of Rome or Integrated Systems Development. In fact their

key personnel involved in the project hold more than 10 patents in SPD related fields. As detailed in section 5.2, the consortium members account skilled people in standardization activities.

## *4.3 - Contribution to standards and regulations*

The research challenges raised by the nSHIELD 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 nSHIELD project is expected to raise in the current standards.

Some partners of the nSHIELD 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)
- → nSHIELD 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
- → nSHIELD 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)
- → nSHIELD 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) (SG)

→ Dissemination of nSHIELD 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 nSHIELD 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.

→ nSHIELD 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.

→ nSHIELD 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. nSHIELD 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 nSHIELD addresses issues dealing with trusted computing building blocks and software interfaces across multiple platforms, contributions to TCG will arise. In particular nSHIELD 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.

→ nSHIELD 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 nSHIELD partners participate in *Secure Simple Pairing* and *Ultra Low power* white paper groups.

→ About Secure Simple Pairing, nSHIELD 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, nSHIELD 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.

→ nSHIELD 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 assess 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.

→ nSHIELD 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, scalable approaches to produce technologically appropriate solutions that meet societal needs.

→ nSHIELD 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 nSHIELD 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.

→ nSHIELD 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.

→ nSHIELD 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.

→ nSHIELD 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.

→ nSHIELD 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 nSHIELD 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.

→ nSHIELD 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.

→ nSHIELD could help standards development and certification

## 4.3.4 - Other standardization activities

Up to now, potential activities among standardization organizations or industrial fora where nSHIELD partners can act directly have been described. Other related activities could be suggested among different organizations.

This is the case of nSHIELD Results from WP2 - *SPD Metric, requirements and system design*, WP6 - *Platform integration, validation & demonstration*. In fact techniques and methods developed by the nSHIELD 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 nSHIELD security requirements to CC security functional and assurance requirements, while evaluators will be able to use checklists issued by nSHIELD to verify security claims, and the automated tools developed by the nSHIELD consortium will produce the necessary evidence for these claims. In this respect nSHIELD 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'*, nSHIELD 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 nSHIELD will look after.

## *4.4 - Management of intellectual property*

Due to the innovative aspects of nSHIELD, 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 nSHIELD result is the prototypes implementation of the developed system architecture for multi-layer secure and dependable solutions for embedded systems for heterogeneous application fields (railways, recognition, avionics, social mobility). 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 nSHIELD 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 4-2 - 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 nSHIELD 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 nSHIELD 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 nSHIELD 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:
  - o industrial and market impact
  - o contingency of manufacturing and business risks ,
  - o ARTEMIS target's convergence
  - o liaison with other R&D projects (especially the ones already funded by ARTEMIS and the ones that will be funded during the nSHIELD 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 project co-ordination will be taken by SG, the Italian leader in Avionics, Sensors and Airborne Systems, and system integration with an organization with remarkable expertise in managing European and National R&D projects; SG will express the Project Manager and will represent the single point of contact with the JU for all matters.

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.
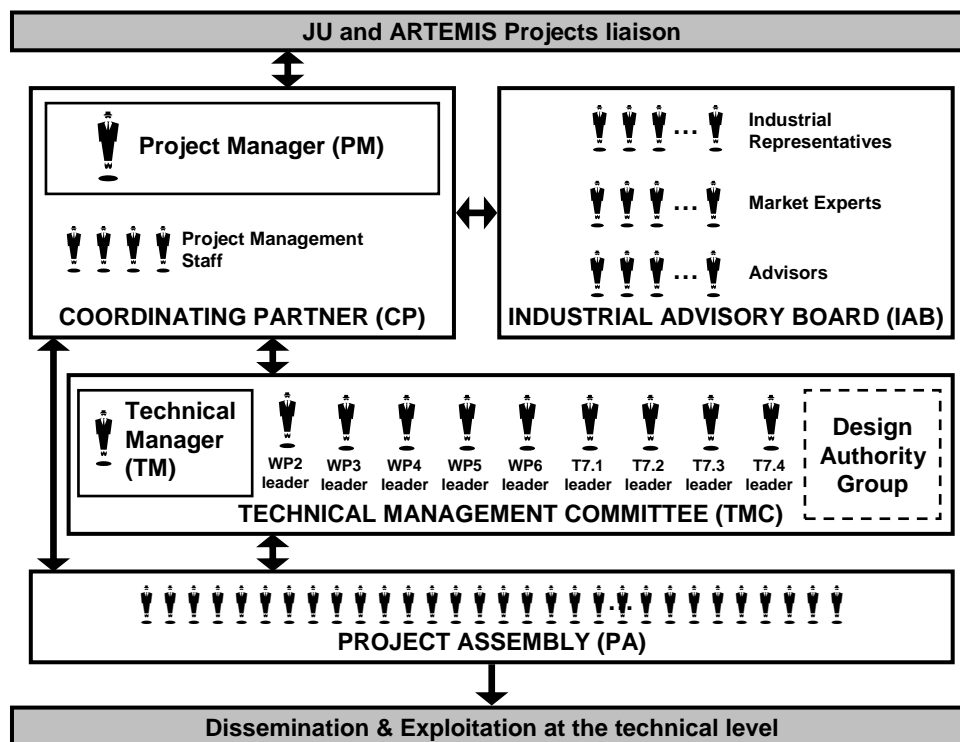


**Figure 5-1 - Organization Structure**

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. Luigi Trono (see SG 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) and the four applications Task leader (each representing the different pilot application in the WP7). 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 General Assembly and the Project 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.
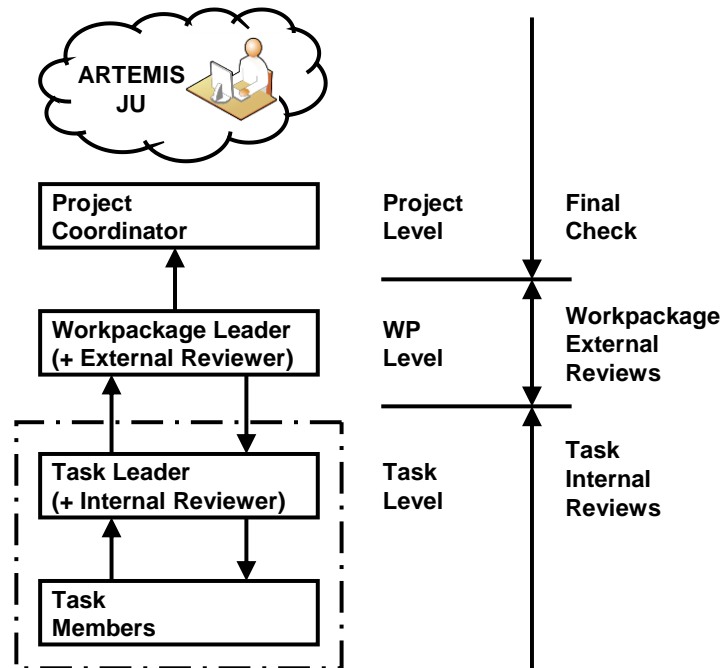


**Figure 5-2 - Project internal review process**

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.
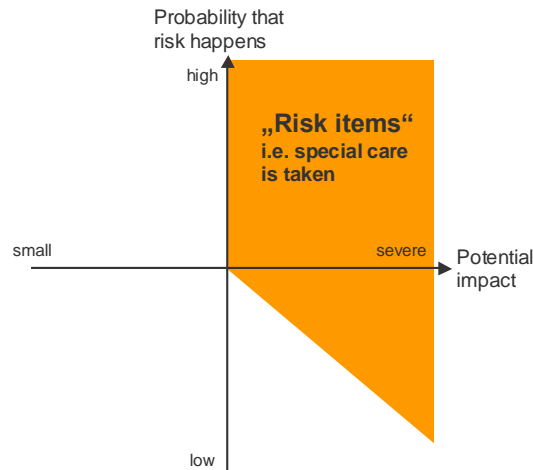


**Figure 5-3 - Risks classification**

- 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 nSHIELD 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 nSHIELD 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. Following this nSHIELD partners list, a brief description of external sponsor of the initiative will be depicted.

## 5.2.1 - nSHIELD Consortium Partners

| Organization | Selex Galileo - FINMECCANICA | Short Name | SG | Partner # | 1 |
|---|---|---|---|---|---|
| Country | Italy | Logo | | | |
| Type | Industry | | | | |

| | |
|---|---|
| **Description** | Selex Galileo, a Finmeccanica Company with 7.000 employees, is the Italian leader in Avionics, Sensors and Airborne Systems. Selex Galileo designs, develops and produces both stand-alone equipment (displays, computers, *etc.*) and on-board systems and sensors (navigation, surveillance, mission management, radar, IR) together with the related operational and logistic support. The company is also involved in the development of unmanned air vehicles. Selex Galileo has a primary role in several leading European and international cooperative aircraft programmes: *e.g.* Typhoon, EH-101, NH90, JSF, AGS; and national programmes: *e.g.* M346. The Company is member of the AIAD (national) and ASD (European) associations. Selex Galileo has been involved in the ACARE (Advisory Council for Aeronautics Research in Europe) activities for the preparation of the SRA (Strategic Research Agenda) including SRA2/FP7 Collaborative Research and Clean Sky JTI. Since 1994 Selex Galileo has been involved in EC-funded projects with the Framework Programme 4 (AFMS and AATMS projects) leading the Surveillance (ADS) function development. In FP5 Selex Galileo was involved in two Integrated Projects: MA-AFAS and AFAS. In FP6 Selex Galileo was involved in six FP6 Projects (5 IP and 1 STREP): SAFEE, TATEM, FLYSAFE, HILAS, NICE TRIP and SOFIA, and for the FP7 the Company is involved in several Projects : Daphne, SCARLETT. For ARTEMIS, Selex Galileo is involved also in the following project: CAMMI and iFEST. |
| **Qualification of the key personnel** | **Mr. Luigi Trono** obtained his Master degree in Electronic Engineering from the Polytechnic University of Turin (Italy) in 2000. He got a certification of Fundamental Avionics from the University of Kansas in 2003. Member of the Italian Engineer Association with ten years of experience in Aeronautical Defense Industry. Worked for 7 years in Lockheed Martin for an international multibillion dollar program (Joint Strike Fighter) in Fort Worth, Texas. From 2007 to 2011 was the Information System Lead for the Support Equipment Business Operations. He was the responsible for managing business requirements across functional Teams (Engineering, Finance, Operations, Planning, Contracting, Procurement, Global Sustainment etc.). Led Value Stream Mapping efforts and key member of Kaizen event for corporate procedures. Developed cost models and handled budgets for multiple WP in the SE. From 2004 to 2007 was the Software/System Integration Lead for the testing and the integration of different JSF software products (Vehicle and Mission Systems). From 2001 to 2004 held the position of System Software Test Engineer in Selex Galileo in Turin and was the responsible for testing the Operational Flight Program (OFP) which is an executable program hosted on the Mission Computer. This software manages (by receiving, processing and transmitting) all the messages from/to radio (UFCP), displays (Head Up Display and Multi Function Display) and |

|  | sensors. |
|--|----------|
|  | **Mr. Michele Genisio:** He works in the Chief Technical Office (CTO) and covers the role of Head of European/International Projects. Has been directly involved in various Research Projects in the area of Security. |

| Organization | Ansaldo STS | Short Name | ASTS | Partner # | 2 |
|---|---|---|---|---|---|
| Country | Italy | **Logo** | | | |
| 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.<br><br>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*.<br><br>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.<br>**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 | **Acorde Technologies S.A.** | Short Name | AT | Partner # | 3 |
|---|---|---|---|---|---|
| Country | Spain | Logo | | | |
| Type | Medium Enterprise | | | | |

| | |
|---|---|
| **Description** | ACORDE TECHNOLOGIES S.A activities are focused on high technology subsystems and components for Space, Telecommunications and Defence Sectors. The company was created in 1999 and nowadays has business in Europe, Asia, Middle East and Latin America. The core activities are system engineering, industrial prototype development and manufacturing of small and medium series. ACORDE is specialized also in design and development of custom articles, such us a light weight X-band Manpack Terminal, Radio over Fiber systems for UMTS, and Satellite Antenna System to provide INTERNET to High Speed Trains. The wide and specialized staff and modern laboratory facilities allow ACORDE to work in a wide variety of different products from DC up to Ka band, power supplies, control cards, transceivers, frequency converters, amplifiers, filters, oscillators, synthesizers. ACORDE has obtained the ISO 9001:2000 and ISO 14001, as well as the NATO AQAP 2110 certifications.<br><br>ACORDE has also long experience in R&D projects at national and European level since its origin. ACORDE's involvement in European collaborative projects could be sampled as: WISE (IST): design, manufacture and integration of wireless sensors network mounted on aircrafts; Magnet/Magnet Beyond (IST): design and development of WPAN Low Date Rate MMICs and High Data rate RF platforms; GREAT and GRAMMAR (FP6 and FP7 GALILEO): RF MMICs developments for multiband GNSS receiver; CHOSEN (FP7) integration of smart wireless sensor networks (both HW and SW) in large-scale, performance-critical application fields like the automotive and the aeronautic scenarios. Besides, ACORDE has a long expertise in R&D internal activities aimed at developing new products and solutions, and creating custom systems for specific customers, focused on perimeter security, distributed monitoring, and secure networks |
| **Qualification of the key personnel** | **Álvaro ÁLVAREZ VÁZQUEZ** was born in Oviedo, Spain, in 1978. In 2002 he obtained his degree in Telecommunications Engineering at the University of Cantabria. He worked in the Department of Communications Engineering (DICOM) of the University of Cantabria from 2000 to 2001, developing radar technologies and push-push oscillators. In 2001 he finished his Master Thesis at the Information & Telecommunication Technology Center of the University of Kansas, working in UWB signal processing simulations, under the supervision of K. Sam Shanmugan, Southwestern Bell Distinguished Professor. Mr Álvarez joined Acorde in May 2002, as Project Manager. Actually he is working in different fields of UWB technologies, from system simulation and hardware design to radio-channel characterisation. Now he has also joined the University of Cantabria as PhD student and Assistant Professor in the field of signal theory and electronic circuit's simulation.<br>**Beatriz QUIJANO RUIZ** was born in Santander, Spain, in 1978. She obtained her degree in Telecommunications Engineering at the University of Cantabria, in 2003. Her works on coexistence between UWB and legacy radio services started in 2002, while performing her Master Thesis at the Information & Telecommunication Technology Center of the University of Kansas, under the supervision of K. Sam Shanmugan, Southwestern Bell Distinguished Professor. She worked then for Accenture (consulting) in the fields of technological consultancy. Mrs Quijano joined the Communications Engineering Department (DICOM) of the University of Cantabria in 2003 performing interference studies to analyse the influence of UWB |

|  | and GSM. In January 2004 she joined ACORDE, where has performed studies on coexistence between UWB and UMTS or WLAN. She is currently in active collaboration with TG3 of ETSI and UWB Cluster of the IST FP6 from the EU, dealing with UWB regulation in Europe. She has worked in research activities within projects under the European Commission FP5 and FP6 such as UCAN, PULSERS, MAGNET, WISE, and ESA projects like POSIRIS. She has authored several publications in the IWUWBS 2003, IST Wireless Summits 2004 and 2005, IEEE ICU 2005, IWS 2005, among other international conferences and workshops. She has also joined the University of Cantabria as PhD student. |
|---|---|

| Organization | **ATHENA RC/ Industrial Systems Institute** | **Short Name** | **ATHENA** | **Partner #** | **4** |
|---|---|---|---|---|---|
| **Country** | Greece | **Logo** | | | |
| **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.<br><br>**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.<br><br>**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. |

Page intentinally left blank

| Organization | Elsag Datamat S.p.A. | Short Name | ED | Partner # | 6 |
|---|---|---|---|---|---|
| Country | Italy | Logo | | | |
| 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 | **Fundacíon Tecnalia Research & Innovation** | **Short Name** | **TECNALIA** | **Partner #** | **7** |
|---|---|---|---|---|---|
| **Country** | Spain | **Logo** | | | |
| **Type** | Medium Enterprise | | | | |

| | |
|---|---|
| **Description** | Fundación Tecnalia Research & Innovation (Tecnalia) the leading private and independent research and technology entity in Spain and the fifth largest in Europe. Tecnalia in 2010 employed 1,437 people (164 PhDs), had a turnover of 121 M€, filed 53 patents, had 3800 clients and created 8 spin-offs. Tecnalia is very active in the Seventh Framework Programme (FP7) having already gained 169 projects, and coordinating 34 of them.<br><br>The European Software Institute (ESI-Tecnalia) is the ICT division in Tecnalia in charge of this project. It was launched in 1993 by an initiative from the European Commission and with the support of leading European companies and the Basque Government with the objective to contribute to developing the Information Society and to increasing industry competitiveness by means of knowledge, innovation, continuous improvement, and the promotion and dissemination of Information Technology. Moreover, ESI- Tecnalia has been an active player of the ARTEMIS and NESSI ETP and their equivalent Spanish platform PROMETEO and INES, as well as the FIA research community regarding the Internet of the Future. ESI-Tecnalia has an extensive experience on EC Framework Programmes, and Eureka international projects, in particular, in ITEA, MEDEA and CELTIC clusters. Recent outstanding European projects where TECNALIA has participated are SHAPE, with TECNALIA's participation in the development of the OMG standard model for SoA (SoaML), NEXOF initiative where the foundations for a reference service architecture (NEXOF-RA) are being laid and COIN, an IP intended to overcome interoperability and cooperation challenges of IT industry. |
| **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.<br><br>He is studying for his Ph. D. in 'R&D Management' at E.T.S Ingenieros Industriales y Telecomunicaciones de Bilbao (UPV/EHU). He obtained his degree in Computer Science from Deusto University and Lund University and his degree in Industrial engineering at Deusto University.<br><br>**Ms. Erkuden Rios** is research engineer in the 'Trust, Security & Dependability' department within 'R&D Project Area' atTecnalia. Before joining TECNALIA in 2003,she worked in Ericsson Spain for 6 years, in the R&D of mobile radio equipment manufacturing. She is specialized in trust and security engineering technologies, and has also a great experience in Model Driven Architectures and their industrial applicability for the improvement of software development process. She has worked in several large European and Spanish national projects related to security and modeling techniques such as nSHIELDS, MODELWARE, MODELPLEX, and MODEM. She obtained her bachelor in Telecommunication Engineering at University of Basque Country (Spain) and currently she is studying for her Ph.D in Information and Communication Technologies in Mobile Networks at the Engineering High Technical School (ETSI) of University of Basque Country (UPV/EHU). |

| Organization | ESIS Norge AS | Short Name | ESIS | Partner # | 8 |
|---|---|---|---|---|---|
| Country | Norway | Logo | | | |
| Type | SME | | | | |

| | |
|---|---|
| **Description** | ESIS Norge AS is an independent company directed towards the implementation and application of future-oriented, innovative and green technologies. The company focus is on the application of artificial intelligence techniques in and for green transport. The company has a track-record on information and knowledge-intensive computing systems, applied in a range of different applications (from electric motorcycles to modern museums). ESIS Norge AS has produced a road-legal prototype electric motorcycle in cooperation with the Norwegian government and the seed-funds of Campus Kjeller (Norway). The company is seeking international cooperation to test, evaluate and further develop the communication and control systems for the vehicle, abstracting it to be used for all types of electric transport. These control, communication and information systems shall be subject of development and evaluation in the nSHIELD project. |
| **Qualification of the key personnel** | **Dr. Robert H.P. Engels** is the founder of ESIS Norge AS, an independent company directed towards the implementation and application of future-oriented, innovative and green technologies. He is appointed Associate Professor at the Western Norway Research Institute in Sogndal. His areas of competence include Business Development and Product design within the areas of semantic annotation strategies for multimedia, information access, AI/ML and computer linguistics. Holding a PhD from the Business Economics Department of the University of Karlsruhe, Germany, Dr Engels conducted research in the area of Knowledge Discovery and Data Mining. He studied Artificial Intelligence, Psychology and Computer Science at the University of Amsterdam, NL and conducted his Msc thesis on applications of Inductive Logic Programming at the University of Stockholm, Sweden. Dr. Engels (co-)authored several papers Knowledge Discovery in Databases, Computational Linguistics and Semantic Web. He organised several international and local (german) workshops on Semantic Web and practical applications of Data Mining. Robert has a.o. worked as consultant at DaimlerChrysler AG, Deutsche Telekom AG, CognIT a.s., Movation AS, Computas AS & the Norwegian Broadcasting Cooperation (NRK). |

| Organization | **Eurotech Security (I.P.S.)** | Short Name | **ETH** | Partner # | **9** |
|---|---|---|---|---|---|
| **Country** | Italy | **Logo** | | | |
| **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. nSHIELD 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 nSHIELD and the project will provide important SPD guidelines to drive and suggest the evolution of Eurotech products in many technology markets. nSHIELD 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** | | | |
| 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 nSHIELD 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. <br><br> **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 | **Indra Software Labs** | Short Name | **INDRA** | Partner # | **11** |
|---|---|---|---|---|---|
| **Country** | Spain | **Logo** | | | |
| **Type** | Industry | | | | |

| | |
|---|---|
| **Description** | Indra is a global company of technology, innovation, and talent, leader in high value-added solutions and services for the Transport and Traffic**,** Energy and Industry**,** Public Administration and Healthcare**,** Finance**,** Insurance**,** Security and Defence**,** and Telecom and Media sectors. Indra operates in over 100 countries and has 29,000 employees worldwide who share their knowledge of different sectors and countries to find innovative solutions to the challenges that clients face. Indra is the European company that most invests in R&D in its sector.<br><br>Indra is quoted in the stock exchange of Madrid, Spain (IBEX: IDR), and it is in the Dow Jones Sustainability World Index (DJSWI) and the Dow Jones SOXX Sustainability Index (DJSI STOXX) for IT and Internet services.<br><br>It is currently the second largest European company by market capitalization in its sector.<br><br>Indra Software Labs (ISL) is the network of Software Labs of Indra that develops customized software solutions for Indra's markets. ISL comprises 20 centres around the world with 4.000 professionals.<br><br>At national level, Indra is part of the management committee of the PROMETEO platform (intelligent embedded systems). member of the management committee of the eSEC platform (security). ISL is member of the INES national platform (software and services) and of the NESSI platform (Networked European Software and Services Initiative) |
| **Qualification of the key personnel** | **Juan Carlos Cavero Torrejón** was born in Madrid in 1967 and has a Telecommunication Engineer degree in Electronic Equipment from the Universidad Autónoma de Madrid in 1994. He has developed several projects in the area of Utilities such as the Open SGC (Market Trading System for electric / gas), Open SGT (job management system for utilities company), Architecture for projects of Union Fenosa ( ARQv10, ARQw10), Sonar Simulator LWHP53 project for the frigate F-115, maintaining the website of the Ministry of Environment (SAIH project), iDBM project in ATM (Air Traffic Management) for the client NATS and DFS. Currently working on the project of Voice Control System (VCS) in ATM customer AENA, as head of development.<br><br>**Jorge Sánchez Uríen** was born in Bilbao in 1971 and has a technical degree in computer science from the School of Computer Systems of Madrid won in 1995. He also has a certification as java/j2ee programming from Sun Microsystems. He started working for a small multimedia company developing videogames in C/C++, until 1998 when he joined Union Fenosa International Software Factory. There, he was involved in different projects for the utilities sector as a java developer. Since 2008 he belongs to Indra Software Labs Defense and Space department , where he's been working as a senior software engineer in GALILEO project for the European Space Agency and currently, LWHP53 Sonar project for the F-105 frigate of the Spanish Navy. |

| Organization | **Integrated Systems Development S.A.** | **Short Name** | **ISD** | **Partner #** | **12** |
|---|---|---|---|---|---|
| **Country** | Greece | **Logo** | | | |
| **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.<br><br>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.<br><br>**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.<br><br>**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 # | 13 |
|---|---|---|---|---|---|
| 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.<br><br>In nSHIELD 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 nSHIELD 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.<br>Truls is the author of the book: Information Sea - a survival guide for tomorrow's knowledge workers.<br><br>**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 | | | |
| 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 nSHIELD 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 | **Noom AS Scandinavian Mobile Technology** | **Short Name** | **NOOM** | **Partner #** | **15** |
|---|---|---|---|---|---|
| **Country** | Sweden | **Logo** | | | |
| **Type** | Medium Enterprise | | | | |

| | |
|---|---|
| **Description** | Scandinavian Mobile Technology was found in 2005 following the idea of "you don't call a number, you call a name". The company successfully implemented services like "call taxi", which connects you to the closest free taxi driver and "key return", providing anonymous communication for the founder of your lost keys. In nSHIELD the company will use their dedicated communication platform to communicate with embedded objects, allowing all kinds of mobile and fixed communication channels. Ideas for such communication are informations from vehicles or members of the trust-network. Scandinavian Mobile Technology will be represented by Per Lasse Hauglum. |
| **Qualification of the key personnel** | **Per Lasse Hauglum** is founder of Scandinavian Mobile Technology, and holder of multiple patents related to "call-a-name". The suggested identification system addressing embedded objects in the Internet of Things are personal identifiers, related to the owner or user of the devices. He is a system engineer and IT specialist with long experience in sales and marketing. He started Internett Partner in 1995 and was a pioneer building an Internet shop for Interflora. Founder of a patended mobile system where you can make mobile calls by names instead of numbers |

| Organization | **SELEX Communications S.p.A.** | **Short Name** | **SCOM** | **Partner #** | **16** |
|---|---|---|---|---|---|
| **Country** | Italy | **Logo** | | | |
| **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. <br><br> 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** | **Ing. Carlo Gugliemini**, Graduated in Electronics/Communications at the Genoa University in 1981, he joined the Company in 1982 <br><br> Head of System Innovation – Military and Satellite Business Unit of SELEX Communications, the leading company for defence communications in the Finmeccanica Group, has the responsibility of the innovation of systems and solutions for the defence market. <br><br> Involved for more than twenty five years in system design and engineering, he has been responsible of major projects for the implementation of both Strategic Networks and C4I tactical systems for the Italian MoD, NATO and other allied nations. <br><br> Director for NCW projects (2004), he participated as Technical Team Leader in the "NCW/NEC Architectural Study" developed for the Italian MoD by Finmeccanica. <br><br> He had the responsibility of the customer solutions for defence market (VP Proposal Engineering Network Centric Operations, Land & Satellite Systems - 2006) and of exploring and developing system innovation in line with technology innovation (VP System Development Infrastructural, Naval and NCO&W - 2008). <br><br> In the current position (2009), he leads engineering groups in the NEC architecture, Networking & Information Infrastructure, Wireless, Satellite, Core & Application Services and Network Modelling & Simulation areas with the responsibility of the system innovation and the development of NCO&W solutions <br><br> **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. <br><br> 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).

**Ing. Alessandro Ambrosetti** graduated in RF Engineering at Politecnico of Turin in 1986 and begins his career in Marconi spa as RF engineer in Research and Development of Radio frequency products for Data Link System.

From 1992 to 2000 he is System Manager at Esaote Spa for study and realization projects in the health sector field, particularly referring to projects supporting tenders on a contract work basis.

In 2000 rejoins former Marconi Mobile spa (now Selex Communications spa) as Program Manager for the supply & commissioning of telecommunication systems used in public and private mobile application.

| Organization | **SEARCH-LAB Security Evaluation Analysis and Research Laboratory Ltd** | Short Name | **S-LAB** | Partner # | **17** |
|---|---|---|---|---|---|
| **Country** | Hungary | **Logo** | | | |
| **Type** | SME | | | | |

| | |
|---|---|
| **Description** | SEARCH Laboratory was established in 1999 at the Budapest University of Technology and Economics, Hungary, with a focus on security research and development. In 2002 the leaders of the laboratory founded SEARCH-LAB Ltd as a spin-off company to provide the legal and infrastructural background for dependable professional services. <br><br> The cooperation of the university laboratory and the professional dedicated company provides an incomparable combination that can successfully face challenges in the wide area from research through development to high-level services. We have a strong expertise and high respect on the market, with a unique experience in the area of security of embedded devices, and having market leading mobile phone and set-top-box manufacturers among our customers. Besides human intelligence driven black- and white-box testing (following our own methodology called MEFORMA), we also use our automated security testing tool named FLINDER for evaluation of APIs, protocol implementations and pieces of software in general. |
| **Qualification of the key personnel** | **Zoltán Hornák** completed his degree at the Budapest University of Technology and Economics as an engineer of informatics. After spending eight years in the anti-virus industry as the development director of VirusBuster and working two-and-a-half years as a security consultant, he returned back to research and established the SEARCH Laboratory. He took part in the organization of several scientific conferences as a PC member, and recently he is also involved as the member of the International Board of Advisors in the Software Assurance Forum for Excellence in Code (SAFECode) initiative established by large software vendor companies like Microsoft, SAP and Nokia. <br><br> **Ernő Jeges** has been working in the area of security for nearly fifteen years. During this period he was involved in a number of activities in different areas of security. His areas of interest include the convergence of logical and physical security, data hiding, technological aspects of digital rights, remote biometrics and intelligent video surveillance. He has several innovations in the area of ear-based human identification, integration of fingerprint biometrics with cryptosystems, computer vision, and software watermarking. |

| Organization | **SESM - FINMECCANICA** | Short Name | **SESM** | Partner # | **18** |
|---|---|---|---|---|---|
| **Country** | Italy | **Logo** | | | |
| **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.<br>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.<br><br>**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 | **Swedish Institute of Computer Science** | Short Name | SICS | Partner # | 19 |
|---|---|---|---|---|---|
| **Country** | Sweden | **Logo** | | | |
| **Type** | Public research Institute | | | | |

| | |
|---|---|
| **Description** | Swedish Institute of Computer Science (SICS) is a part of Swedish ICT Research AB, a nonprofit research organization owned by the Swedish government (60%) and industry (40%). SICS' mission is to contribute to the competitive strength of Swedish industry by conducting advanced and focused research in strategic areas of computer science, and actively<br>promoting uptake of new research ideas and results in industry and society at large. SICS works in a close collaboration with industry and the national and international research community.<br>SICS focuses on distributed and networked interactive real-time systems and applications, spanning from infrastructural issues to software methodologies to human-computer interaction. In December 2008 SICS had a research staff of 85, thereof 46 PhDs. SICS publish approximately 70 refereed papers and articles in international journals and conferences per year. SICS is an active participant in collaborative national, European, and other international R&D programs.<br>The secure systems group at SICS work with security in embedded systems such as secure hypervisor design, formal verification and trusted computing technologies. The group currently has five active researchers. |
| **Qualification of the key personnel** | **Christian Gehrmann** has been working with security research since 1992. He joined SICS in 2009 as lab manager. His research covers cryptography, authentication theory, security in cellular networks and in the Internet, security for ad hoc wireless networks, mobile platform security and security in surveillance networks. Christian Gehrmann is the main architect and<br>the editor of the new global network video industry standard ONVIF. He has published over 25 scientific security papers at international conferences and in journals and around 50 different patent applications. Christian holds a M.Sc. in electrical engineering and a Ph.D. in Information Theory, both from the Lund Institute of Technology. Christian is since 2007 associated professor in Information Theory at Lund Institute of Technology. |

| Organization | T2Data | Short Name | T2D | Partner # | 20 |
|---|---|---|---|---|---|
| Country | Sweden | Logo | | | |
| Type | Small Enterprise | | | | |

| | |
|---|---|
| **Description** | T2 Data is an independent IT consulting firm started in 1990. The company is located in KISTA, in Stockholm.  2 Data is specialized in systems development with the following areas of expertise:<br>• Advanced Real-Time Systems.<br>• Embedded Systems.<br>• Electronic Design.<br>• Object Oriented Systems.<br>www.t2data.se<br><br> The average employee of T2 Data has 15 years of work experience and about 60% of the consultants hold an MSc degree in engineering. Annual turnover is approx 60 MSEK. |
| **Qualification of the key personnel** | **Hans Thorsen**  born in Sweden 1959. He holds a Master of Sciene Electronic Engineering Department from Lunds Institute of technology.  He spent two years with Silicon Graphics as system engineer. As a freelance consulting 1990 – 2003 he have been engaged by Ericsson in projects resulting in the OSGI initiative.  Hans holds several patents in the area of security applications.  The key deployment of Assa Abloys ARX product series is covered by patents invented by Hans.  Currently Hans is engaged by T2Data as a CTO. |

| Organization | **Telcred AB** | **Short Name** | **TELC** | **Partner #** | **21** |
|---|---|---|---|---|---|
| **Country** | Sweden | **Logo** | | | |
| **Type** | Small Enterprise | | | | |

| | |
|---|---|
| **Description** | Telcred is a research based startup company that develops access control systems based on NFC and state-of-the-art IT-security methods. These will allow NFC devices, including mobile phones, to be used for access control instead of, or in addition to, traditional keys and smart cards. In particular, Telcred develops novel embedded systems for access control working also in remote off line locations |
| **Qualification of the key personnel** | **Carlo Pompili, CEO.** Carlo has close to 15 years experience from working with innovation and new business development in IT and Telecommunications. His experience includes being a co-founder of, and partner in, an incubator focusing on mobile Internet services. Prior to co-founding and becoming the CEO of Telcred, he was responsible for product management at a niche mobile operator in Sweden, and before that he was responsible for business development at SICS.<br><br>**Adrian Slabbert** has been working as researcher between 2007-2009. He has performed both theoretical security analysis and implemented access control solutions as software developer. Adrian has published papers in computer network security and factory automation and he has given talks at several internal conferences and workshops. He holds a B.Sc. from University of Stellenbosch, South Africa and a M.Sc. from Royal Institute of Technology in Stockholm. Adrian is currently the main software and hardware architect an Telcred. |

| Organization | THYIA d.o.o. | Short Name | THYIA | Partner # | 22 |
|---|---|---|---|---|---|
| Country | Slovenia | Logo | | | |
| Type | Small 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 (FP7-OMEGA), civil (FP7-IMSK) and military sensor networks with huge number of nodes (EDA-WINEA), and TITRES a national project in Slovenia lead by THYIA. This thatbackground represents an important technology breakthrough for nSHILED project that will be used for surveillance and other military applicationsdifferent scenarios and applications. Therefore, THYIA interest is in various fields related to the Wireless Radio Communicationsheterogeneous networks and sensors, RFID, UWB and sensor networks (. GPRS/UMTS, WiFI, WiMAX, 60 GHz radio, Flexible Radio & SDR, Cognitive Radio (CR)). Additinally, SPD technologies, , 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 nSHIELD 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, TPMs, 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 and Utility sectors. In particular for nSHIELD he will contribute as architect for SMN scenarios and in different security areas related to sensor, sensor networks, wireless technology, interoperability aspects, SW & HW architecture, system requirements, specifications, and business models. For overall nSHIELD R&D activities he will assist the partners with expertise in wireless systems and networks and new multi-technology security solutions for embedded devices.<br><br>**Dr. Gordna Mijic** is CTO of THYIA working in the fields of 3G & 4G technologies, microwave technologies, Wireless Grid, WiFi, WiMAX, UWB, SDR, MIMO, RoF and 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 | **Technical University of Crete** | Short Name | TUC | Partner # | 23 |
|---|---|---|---|---|---|
| Country | Greece | Logo | | | |
| Type | Public research Institute | | | | |

| | |
|---|---|
| **Description** | Technical University of Crete (TUC), has participated in many projects in the ESPRIT, ICT, ACTS, Telematics, and other programmes. TUC has also adopted a strategy of promoting the commercial exploitation of R&D results, by providing services (e.g. consulting) and contracting with industrial partners for specific products. <br><br> TUC is the younger of the two technical universities in Greece. The purpose of TUC is to offer advanced high-quality education and research in modern Engineering specialties. TUC has five departments. The Department of Electronic and Computer Engineering (ECE) has been accepting students since 1990. The department has a modern program of undergraduate and postgraduate studies aimed at educating engineers in MHL (Microprocessor and Hardware Laboratory), which is one of the laboratories of the ECE, and will be the main contributor to the nSHIELD project. The laboratory conducts research and development in the architecture, design and implementation of both fixed and reconfigurable computer and communication systems, and in their implementation, at the IC, board, and system level. It is also involved in a number of projects targeting secure networking. |
| **Qualification of the key personnel** | **Prof. Ioannis Papaefstathiou** is an Assistant Professor at the Department of Electronic and Computer Engineering at the Technical University of Crete. He is working in the design and implementation methodologies for networking systems with tightly coupled design parameters and highly constrained resources. He was granted a PhD degree in computer science at the University of Cambridge UK, in 2001, an M.Sc. degree (Ranked 1st) from Harvard University, Cambridge, MA, in 1996 and a B.Sc. degree (Ranked 2nd) from the University of Crete, Greece in 1996. From 1994-1996 he was a VLSI systems engineer at ICS-FORTH, and from 1997-2000 he was a Research Associate at the Systems Research Group, Computer Laboratory, University of Cambridge. From 2001-2005 he was the manager of the Crete R&D department of Ellemedia Technologies, a closely affiliated to Lucent's Bell Labs microelectronics company. He has published more than 40 papers in IEEE-sponsored journals and conferences. He has been the prime Guest Editor for an issue of IEEE Micro Magazine and for one in IEEE Design & Test Magazine. He has served as a evaluator for the Commission of the European Communities, as well as for the Greek General Secretariat for Research and Technology. He has participated in many European R&D Programmes, ACTS (ARCHES), ESPRIT(Telegraphos, ASICCOM), IST(Pegasus, PRO3, ADAMAS, MobileIN). <br><br> **Prof. Charalampos Manifavas** is an Assistant Professor at the Technological Educational Institute of Crete. His expertise lies in the area of Network and Information Systems Security. He received his Ph.D. in Computer and Communications Security from the University of Cambridge, UK, in 2002, his M.Sc. in Communication Systems Engineering from the University of KENT, UK, in 1994, and his B.Sc. in Computer Science from the University of Crete, Greece, in 1993. From 1995 to 1998 he worked as a Research Assistant at the Computer Lab, University of Cambridge, on electronic payment protocols, digital certification infrastructures and copyright protection. From 2000 to 2003 he worked as a security engineer for Barclays Capital, an investment bank in London, where he was responsible for the productionisazion of several security technologies like Public Key Infrastructures (PKI), Intrusion Detection Systems (IDS), Identity Management Systems (IMS), Anti-virus Management, Active Content Protection και Secure |

Instant Messaging. From 2004 to present he has been lecturing on Information Systems and Network Security. From 2007 to 2008 he worked as a security engineer & consultant with Virtual Trip, Ltd. and with ICS-FORTH (Institute of Computer Science, Foundation of Research & Technology – Hellas) on security projects serving the private and public sector respectively (some of them funded by GSRT, the General Secretariat for Research and Technology of the Greek Ministry of Development). He has also co-operated with ENISA (European Network and Information Security Agency) for the writing of two position papers aiming to increase information security awareness among European SMEs. Dr Manifavas is the author or co-author of several research papers and a book, all in the area of information security.

**Prof. Konstantinos Rantos** is an Assistant Professor at the Technological Educational Institute of Kavala working on Cryptography and Network Security. He received his Diploma in Computer Engineering and Informatics from the University of Patras, Greece, and both his M.Sc. (1997) and Ph.D. (2001) in Information Security (sponsored by Marie Curie Research and Training Grant) from Royal Holloway, University of London. Between 1997 and 1999 he was involved in an EU ACTS project concerning security for third generation mobile communications. Following his appointment as a smart card security architect at Datacard Group he joined Encode S.A. as a security consultant contributing to a number of security related projects. He has worked as an assistant professor at the Technological Educational Institute of Kavala and as a lecturer at the Democritus University of Thrace (Department of Electrical and Computer Engineering) and at the University of Central Greece (Department of Informatics with Appliances in Biomedicine). He worked as a scientific officer at the Hellenic Ministry of Interior where he managed and contributed to the development of large-scale production and EU-level pilot projects (SPOCS, STORK). He is a reviewer to a number of scientific journals and conferences.

| Organization | Università di Genova – Dipartimento di Ingegneria Biofisica ed Elettronica | Short Name | UNIGE | Partner # | 24 |
|---|---|---|---|---|---|
| Country | Italy | Logo | | | |
| 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 nSHIELD platform at node and network transmission level and the definition of SPD metrics for the analysis of nSHIELD 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. **Prof. 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. **Prof. Rodolfo Zunino** received the "laurea" degree (summa cum laude) in Electronic Engineering from the University of Genoa, in 1985. He is Associate Professor at DIBE since 2000. Since 2005 he coordinates the Smart Embedded Application Laboratory (SEALab) at DIBE. **Prof. Daniele Caviglia** graduated in Electronic Engineering and specialized in Computer Science at the University of Genoa in 1980 and 1982, respectively. In 1983 he is Assistant Professor (1983-1992) and then he is Associate Professor (1992-2000). From 2000 he is Full Professor of Microelectronics at the same University. In October 2002 he has been elected Head of Department. His main interests are now in the field of the VLSI implementation of artificial neural networks and in CMOS |

circuit design for Telecommunications

**Prof. Maurizio Valle** received the Master degree in Electronic Engineering and Computer Science at the University of Genoa in 1985. In 1990 he received the Ph. D. degree in Electronic Engineering and Computer Science from the University of Genoa (curriculum: Microelectronics). In 1992 he became Assistant Professor. His main research and scientific interests are in the areas of mixed mode microelectronic systems (in CMOS technology) for signal processing and ad hoc wireless sensors networks.

**Mr Luca Bixio** 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. His research is mainly focused on software defined radio, cognitive radio and reliable transmission methodologies.

| Organization | **Università degli Studi di Udine** | Short Name | **UNIUD** | **Partner #** | **25** |
|---|---|---|---|---|---|
| Country | Italy | Logo | | | |
| Type | Public research Institute | | | | |
| Description | The University of Udine was founded in 1978 as part of the reconstruction plan of Friuli region after a devastating earthquake in 1976. The purpose was to provide the Friuli's community with an independent centre for advanced training in cultural and scientific studies.<br>The University of Udine has always been settling and following its main targets, i.e. dissemination of culture, knowledge and results of research activities, in order to contribute to the territorial socio-economic development. Since its institution, the University of Udine has rapidly earned a high standing reputation and acquired a position among the leading research universities.<br>The University of Udine is actively engaged in a wide range of research activities, not only internally but also in co-operation with other universities and research institutes at both national and international level.<br>The University's strong research focus has seen it become a centre of excellence in a considerable number of fields.<br>In particular, the DIEGM is a multidisciplinary Department, belonging to the School of Engineering of the University. The only technological Department of the University in the field of Information and Comunication Technologies, the DIEGM incorporates many technological disciplines, from mechanical to electrical and electronics engineering. Specifically, all disciplines that are relevant in the ICT context are represented within the Department by Research Groups of international reputation, namely device physics and microelectronics, system level design, telecommunications, antennas, power electronics, micromechanics and micro-fabrication.<br>Among the different project that have seen the participations of different DIEGM Groups, e.g. the SiNano Network of Excellence, the PullNano IP, the Agave and Wirenet CRAFT the FunFox STREP, IST COLUMBUS, and Omega Projects, and other Italian research projects. The Department includes about fifty academic staff people, with the addition of about thirty Ph.D. students, several Technology Labs among which it is worth to mention, for the purposes of the present project submission, the Pervasive Computing Laboratory. The people involved cover the main technological areas needed to pursue the goals of the Project. In particular, the different individuals have wide expertise in the design integrated circuits, system level design, and digital communications. |
| Qualification of the key personnel | **Antonio Abramo** was born in Bologna, Italy, in 1962.<br>He received the Laurea degree in Electrical Engineering (magna cum laude) from the University of Bologna, Italy, in 1987, and the Ph.D. degree in Electrical Engineering from the same Institution in 1995.<br>His experience includes research periods with the Intel Corporation, Santa Clara (CA), USA (1992), at the Center for Integrated Systems, Stanford University, Stanford (CA), USA (2000). Between October 1993 and December 1994 he was Resident Scientist at the AT&T Bell Laboratories, Murray Hill (NJ), USA, while from 1995 to 1997 he was Post-Doc at the Department of Physics, University of Modena, Italy. Antonio Abramo is co-author of about 70 scientific publications on International Journals and Conferences. In years 2001-02 he has been appointed Member of the "Modeling and Simulation" technical sub-committee of the IEEE |

International Electron Device Meeting (IEDM) Conference, and in year 2003 Chair of the same sub-committee. Presently, he is Associate Professor of Electronics at the University of Udine, Italy. After about ten years of scientific activity in the field of modeling and simulation of carrier transport in electron devices, Antonio Abramo has recently become active in the field of the design of digital circuits for DSP applications on reconfigurable platforms, of neural networks circuits on reconfigurable platform, of distributed computation methodologies on wireless sensor networks, on the system level design of wireless digital systems. These activities have led to the activation of collaborations with industrial partners operating in the field of digital electronics and pervasive computing, and to the activation of research funding projects. Antonio Abramo is Senior Member of the IEEE.

**Roberto Rinaldo** obtained the "Laurea in Ingegneria Elettronica" degree in 1987 from the University of Padova, Padova, Italy. From 1990 to 1992, he was with the University of California at Berkeley, where he received the MS degree in 1992. He received the Doctorate degree in "Ingegneria Elettronica e dell'Informazione" from the University of Padova in 1992. In 1992 he joined the Dipartimento di Elettronica e Informatica of the University of Padova as a "ricercatore". Starting from November 1st 1998, he was associate professor in Communications and Signal Processing in the same Department.
Since November 2001, he was an associate professor in the "Dipartimento di Ingegneria Elettrica, Gestionale e Meccanica" of the University of Udine. Starting December 2003, he is now a professor in the same department. His interests are in the field of multidimensional signal processing, video and image coding, optimal coding for p2p and web applications. Prof. Rinaldo represents the University of Udine in the CNIT (Consorzio Nazionale Interuniversitario Telecomunicazioni). He is the Author of about 100 papers in international journals and conference proceedings. He has served as a reviewer for major International Journals and Conferences.

**Mirko Loghi** is an Assistant Professor at University of Udine.
He received the Laurea Degree in Electrical Engineering from the University La Sapienza of Rome and the Ph.D. degree in Computer Science from the University of Verona. His experience includes a period of research as Visiting Researcher at Sun Microsystem (Menlo Park, (CA)) a Postdoctoral Fellow position at Politecnico di Torino.
His research interests include embedded systems design, and multiprocessor systems on chip development, with particular emphasis on power modeling and optimization of digital systems.

During his research activity, Mirko Loghi has co-authored about twenty scientific papers on International Journals and on Proceedings of International Conferences.

| Organization | Università di Roma – Dipartimento di Informatica e Sistemistica | Short Name | UNIROMA1 | Partner # | 26 |
|---|---|---|---|---|---|
| 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 nSHIELD consortium comprises 7 manufacturers and system integrators (SG, ASTS, ED, ETH, HAI, ISL, SCOM), 7 universities (MGEP, UNIGE, UNIROMA1, UNIUD, TUC, SICS, S-LAB,), 9 SMEs (AT, TECNALIA, ESIS, ISD, MAS, NOOM, T2D, TELC, THYIA) 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 – nSHIELD 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 nSHIELD team.

| Responsibility | Beneficiary |
|---|---|
| Project Coordinator | SELEX GALILEO (SG) |
| Technical Manager | ELSAG DATAMAT (ED) |
| WP 1 – Leader | SELEX GALILEO (SG) |
| WP 2 – Leader | THYIA (THYIA) |
| WP 3 – Leader | THYIA (THYIA) |
| WP 4 – Leader | SELEX-COMMUNICATION (SCOM) |
| WP 5 – Leader | ELSAG DATAMAT (ED) |

| WP 6 – Leader | HELLENIC AEROSPACE INDUSTRY (HAI) |
|---------------|-----------------------------------|
| WP 7 – Leader | MOVATION AS (MAS) |
| WP 8 – Leader | UNIVERSITY OF MONDRAGON (MGEP) |

**Table 5.1 - Responsibilities of nSHIELD beneficiaries**

## 5.3.1 - nSHIELD Consortium analysis

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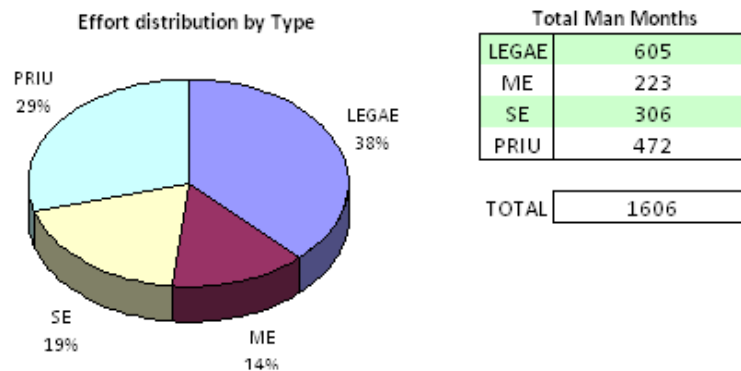


**Table 5.2 – nSHIELD effort distribution by type**

Indeed Table 5.2 shows clearly that the project is leaded by an industrial partnership (70% of the effort) even if an important role is left to the universities and the research centers (30%) in order to bring the needed high innovation. In particular the large industries lead the project with the majority of the effort (38%). 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 (33% of the overall effort) in the development of the new SPD technologies and their integration in the nSHIELD platform.
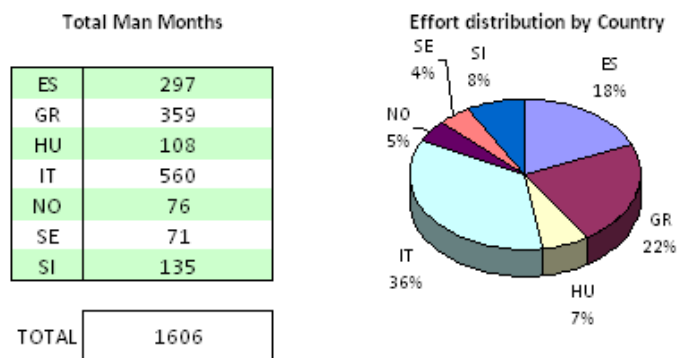


**Table 5.3 – nSHIELD Country involvement**

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 (27% of the total effort), the Norwegian and Slovenian (13%), the Swedish (12%) and the Greek (13%) clusters involved respectively in the railway, recognition, avionics and social mobility application scenarios. Other two clusters from Hungary (7%) and Spain (18%) are

more focused on the development of the SPD technologies and methodologies and on their integration in the nSHIELD platform.

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

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 nSHIELD 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 nSHIELD 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 (33% of the overall effort, see Table 5.2) covering most of the challenging research aspects of nSHIELD and guaranteeing a high level of complementariness.

More in detail the following research topics will be investigates: SPD middleware functionalities and interfaces (ISD, THYIA, ESIS), cross-layer security (THYIA), SPD data distribution system (T2D), SPD metric definition and tracing (TECNALIA), intelligent nodes and smart transmission design and development (AT, TELC, NOOM, MAS).

## 5.3.3 - Complementarities

The nSHIELD 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 nSHIELD project, from the design to the demonstration and to cover all the SPD challenges in the world of ES. The features and technologies that have been described in section 2.2 and that will be improved and developed in the project (see the WP3, WP4 and WP5 description) are listed in the following table.

| #  | Feature or Technology |
|----|----------------------|
| 1  | TPM and Smartcard for Trust Ess |
| 2  | Intrinsically Secure ES Firmware |
| 3  | Automatic Access Control and Denial-of-Service |
| 4  | Lightweight Hardware and Software crypto technologies |
| 5  | Power Supply protection |
| 6  | Self re-configurability and self-recovery of sensing and processing task |
| 7  | Multi source audio capture from hundreds of synchronized sensors. |
| 8  | Easy and dependable interface with sensors |
| 9  | Data compression techniques |
| 10 | Personal wearable node for security, privacy and dependability |
| 11 | Multipurpose node for telemetry |
| 12 | Asymmetric Cryptography for low cost nodes |
| 13 | Reputation based schemes for secure routing and intrusion detection system |
| 14 | Anonymity and Location-privacy techniques |
| 15 | Reputation based security resource Management Procedures |
| 16 | Waveform agile and reliable transmission methodologies |
| 17 | Distributed Self-management and self-coordination schemes for unmanaged and hybrid networks |

| # | Feature or Technology |
|---|---|
| 18 | dependable authentic key distribution mechanism |
| 19 | Secure service discovery, composition and delivery protocols |
| 20 | Situational-aware and content-aware SPD |
| 21 | Policy-based SPD management |
| 22 | Semantic representation of the SPD knowledge domain |
| 23 | Secure resource Management Procedure (at middleware level) |
| 24 | Secure Offline Authentication with mobile devices |
| 25 | Rugged High performance computer |

**Table 5.4 - Technologies**

The nSHIELD partners have been selected to deal with these technologies, that are essential in one or more of the selected application scenario as well depicted in Figure 5.5. Each row represents a technology (numbered from 24 to 1). The different grey scale represents the different level to which the technologies belong to (node, network or middleware/overlay). Each column represents a partner. In each cell there are 4 squares, representing the 4 different scenarios. If a square is coloured it means that technology is used by that partner in that scenario.

Starting from this matrix it is possible to highlight the high level of complementarities of the nSHIELD consortium. It is worth to note that:

- Each technology is involved in more than one scenario;
- Each technology is developed by more than one partner for each scenario;
- Except for the scenario leaders, each technological partner is involved in the development of several technologies;

| | | 1 SG | 2 ASTS | 3 AT | 4 ATHENA | 5 CWIN | 6 ED | 7 ESI | 8 ESIS | 9 ETH | 10 HAI | 11 ISL | 12 ISD | 13 MAS | 14 MGEP | 15 NOOM | 16 SCOM | 17 S-LAB | 18 SESM | 19 SICS | 20 T2D | 21 TELC | 22 THYIA | 23 TSI | 24 UNIGE | 25 UNIUD | 26 UOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | TPM and Smartcard for Trust Ess | | | | | | | x | | x | | | | | | | | x | | x | x | | x | | | | |
| 2 | Intrinsically Secure ES Firmware | x | x | | | x | | | x | x | | | | | | | | x | x | x | x | x | | | | | |
| 3 | Automatic Access Control and Denial-of-Service | | | x | x | | | x | | x | | | | | | | | x | | | | | x | x | | x | |
| 4 | Lightweight Hardware and Software crypto technologies | | | | | x | | | x | x | x | x | | x | | | | x | | | | | x | x | | | |
| 5 | Power Supply protection | x | x | x | | x | | | x | | | | | | | | | | | | | | x | | | | |
| 6 | Self re-configurability and self-recovery of sensing and processing task | x | x | x | | x | | | | | | | | | | | | | | | | | x | | x | | |
| 7 | Multi source audio capture from hundreds of synchronized sensors. | | | | | x | | | | x | | x | x | | | | | x | | | | | | | x | | |
| 8 | Easy and dependable interface with sensors | x | x | | | x | | | x | x | | x | | x | | | | | | | | | x | | | | |
| 9 | Data compression techniques | x | | | | | | | | | x | x | x | | | | | | | | | | x | | | | |
| 10 | Personal wearable node for security, privacy and dependability | | | | | x | | | x | x | | | | | | x | | | | | | | x | | | | |
| 11 | Multipurpose node for telemetry | | | | | | | | | x | | x | | | | | | | | | | | x | | | | |
| 12 | Asymmetric Cryptography for low cost nodes | | | | | | | | | | | x | | | | | | x | | x | | x | x | | | | |
| 13 | Reputation based schemes for secure routing and intrusion detection system | x | x | | x | | x | x | | | | x | | | x | | | | | | | | x | x | x | | |
| 14 | Anonymity and Location-privacy techniques | | | | x | x | x | | x | | | | | | | | x | | | | | | x | x | | | |
| 15 | Reputation based security resource Management Procedures | | | | | | x | x | | | | | | | | | | | | | | | | x | | | |
| 16 | Waveform agile and reliable transmission methodologies | | | | | | | | | | | x | | | | | x | | | | | | x | | x | | |
| 17 | Distributed Self-management and self-coordination schemes for unmanaged and hybrid networks | | x | | | x | | | | | x | x | | | | | x | | | | | | x | | x | x | |
| 18 | dependable authentic key distribution mechanism | | x | | | | | | | | | | | | | | | x | | | | | x | | | | |
| 19 | Secure service discovery, composition and delivery protocols | x | | | x | | x | x | | x | | | | | | | | x | | | | | x | x | x | | x |
| 20 | Situational-aware and content-aware SPD | | | | | x | x | | | | | | | | x | | | | | | | | x | x | | | x |
| 21 | Policy-based SPD management | | | | | x | x | x | | | | | | | | | | | | | | | | | x | | x |
| 22 | Semantic representation of the SPD knowledge domain | | | | x | x | x | x | | | | | | | x | | | | | | | | x | | | | x |
| 23 | Secure resource Managment Procedure (at middleware level) | x | | | | x | | | | | x | | | | | | | | | | | | | | | | x |
| 24 | Secure Offline Authentication with mobile devices | | | | | x | | | | | | | | | | | | x | | x | x | x | | | | | |
| 25 | Rugged High performance computer | x | | | | | | | x | x | | | | | | | | | | | | | | | | x | |

**Figure 5-5 - Technology/Partner/Scenario Matrix**

Figure 5-6 shows how during the Design, Implementation, Integration and Demonstration phases at least 2/3 of the consortium is actively involved, thus resulting in a robust and coordinated research team where complementarities are exploited to maximize the project results.
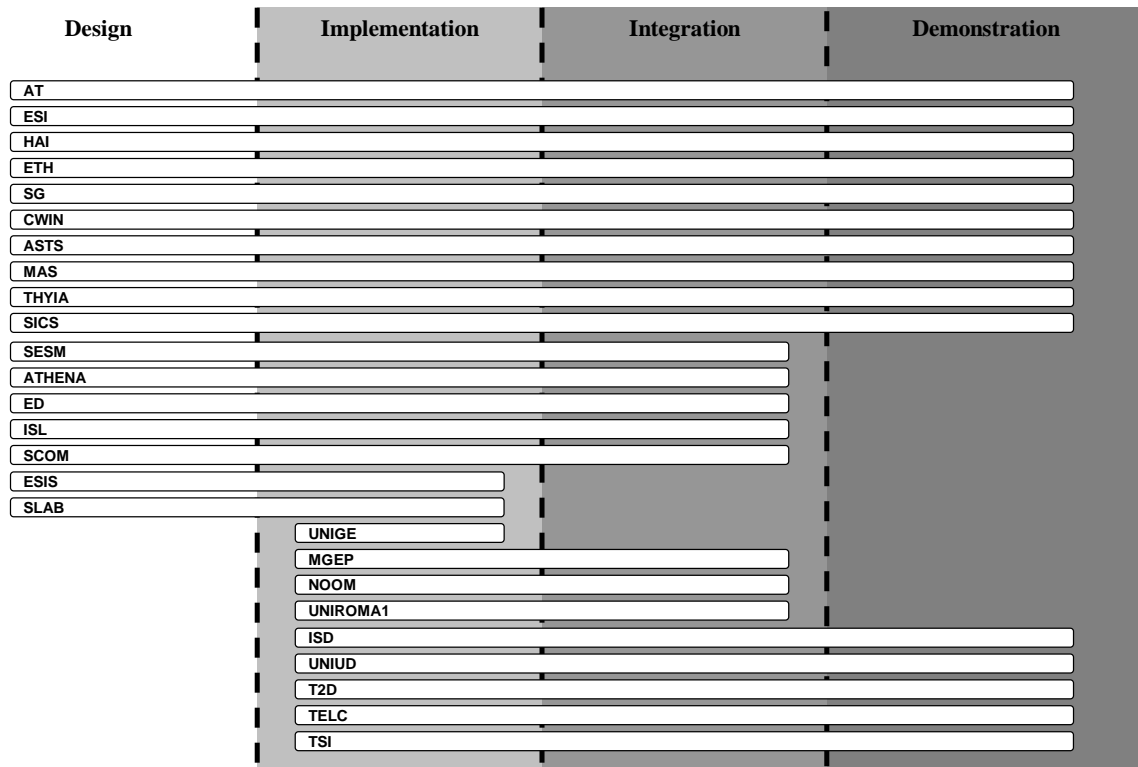
**Figure 5-6 – Complementarities of the nSHIELD consortium**

### i) Sub-contracting:

Some activities within the nSHIELD 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.

_ASTS:_ will subcontract part of work concerning the WP2 (Scenarios, user requirements and architecture design) and WP7 (SPD Applications), regarding the task of their competence (Task 7.1 Railway Transportation). In particular the subcontract amount (40.0 K€) 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.

_SCOM_: The subcontract will be for the architecture of waveform communication for Software Defined Radio (SDR) with Security, Privacy e Dependability (SPD) attributes. These subcontracts will be for:

> 1 – 'Cognitive' Waveform extension with added SPD functions- (UNIGE/DIBE,UniRm2) – value 30.0 KE

> 2 – Customization of the solutions for supporting the Cognitive Manager / Spectrum Sensing for a network with SPD functions and detailed specs - (TICOM, UniGe DIBE) – Value 50.0 KE

> 3 – Cognitive Waveform will be extended to the OMNEST simulator, integration activity in lab environment, test-case definition and result generation - (TICOM, RAL) – Value 90 KE

_THYIA:_ For Social Mobility and Networking (SMN) Scenarios in the _Annex B.3 - Social Mobility and Networking Scenarios_ (page 218) is mentioned that THYIA will use a national initiative in Slovenia related to the city of Kostanjevica. Using electrical grid and combining it

with possibility not only to manage intelligently the street lights, but also to communicate over different access technology (optical, radio and PLC) what is proved in OMEGA project http://www.ict-omega.eu/, represent an important technology breakthrough toward an implementation of the SMN scenarios during this project. For SMN scenarios will be used some existing infrastructure technologies offered by THYIA's consortium composed of THYIA d.o.o., Josef Stefan Institute, and Our Space d.o.o. These resources can't be substitute with other resources of the nSHIELD consortium due to need for using and upgrading the existing infrastructure with new functionalities required by the SMN demonstration scenario.

## 5.4 - Resources to be committed

The nSHIELD project aims at developing proof-of-concept prototypes and integrating them in a composable framework. Four (WP3-WP6) out of the eight work packages are each concerned with development and integration of novel technologies, counting on the 63% of the overall effort (see Table 5.5). In particular the hardware and firmware technologies in WP3 are more intensive and require the 19% of the effort. WP4 deals with SPD solutions at network level and benefit from the results of WP3 and WP5 thus it requires less effort (13%). WP5 develops innovative SPD solutions for middleware and develop a totally new SPD overlay, thus it needs 16% of the resources. WP6 focuses on the development of tools for the SPD lifecycle and the integration of composable technologies in the nSHIELD platform. Thus WP6 is integral part of the R&D and requires a consistent effort (15%).

The system requirements, specification and design (WP2) takes the 9% of the project resources. The demonstration of the nSHIELD results in WP7 plays a very important role (14% of the overall project) resulting in the use of approximately 3% of the total effort for each of the application scenarios. The management of such a big and complex project (see section 5.1 for details) has been taken into account and 8% of the total effort has been dedicated to it. The dissemination, standardization and exploitation activities use the 6% of the total effort to maximize the impact of the project at all level: SPD literature, certifications, standards and market.
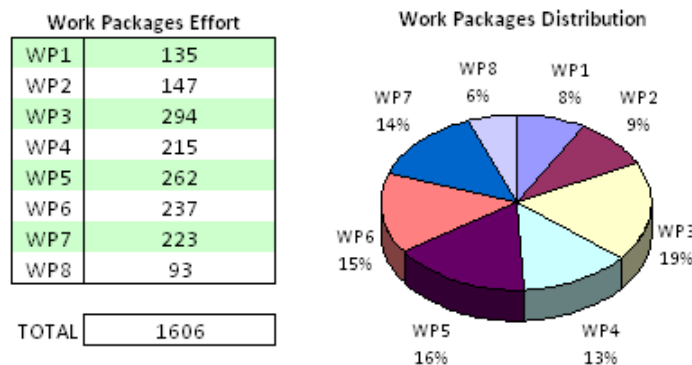


**Table 5.5 – Work Packages effort distribution**

The challenging nSHIELD objectives require an adequate budget, in order to be achieved. The project total cost is approximately 13,8 M€ (refer to Table 5.6). 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 (46%). 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. nSHIELD consortium will be founded with approximately 7,6 M€: 2,3 M€ will be provided by the JU and 5,3 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.
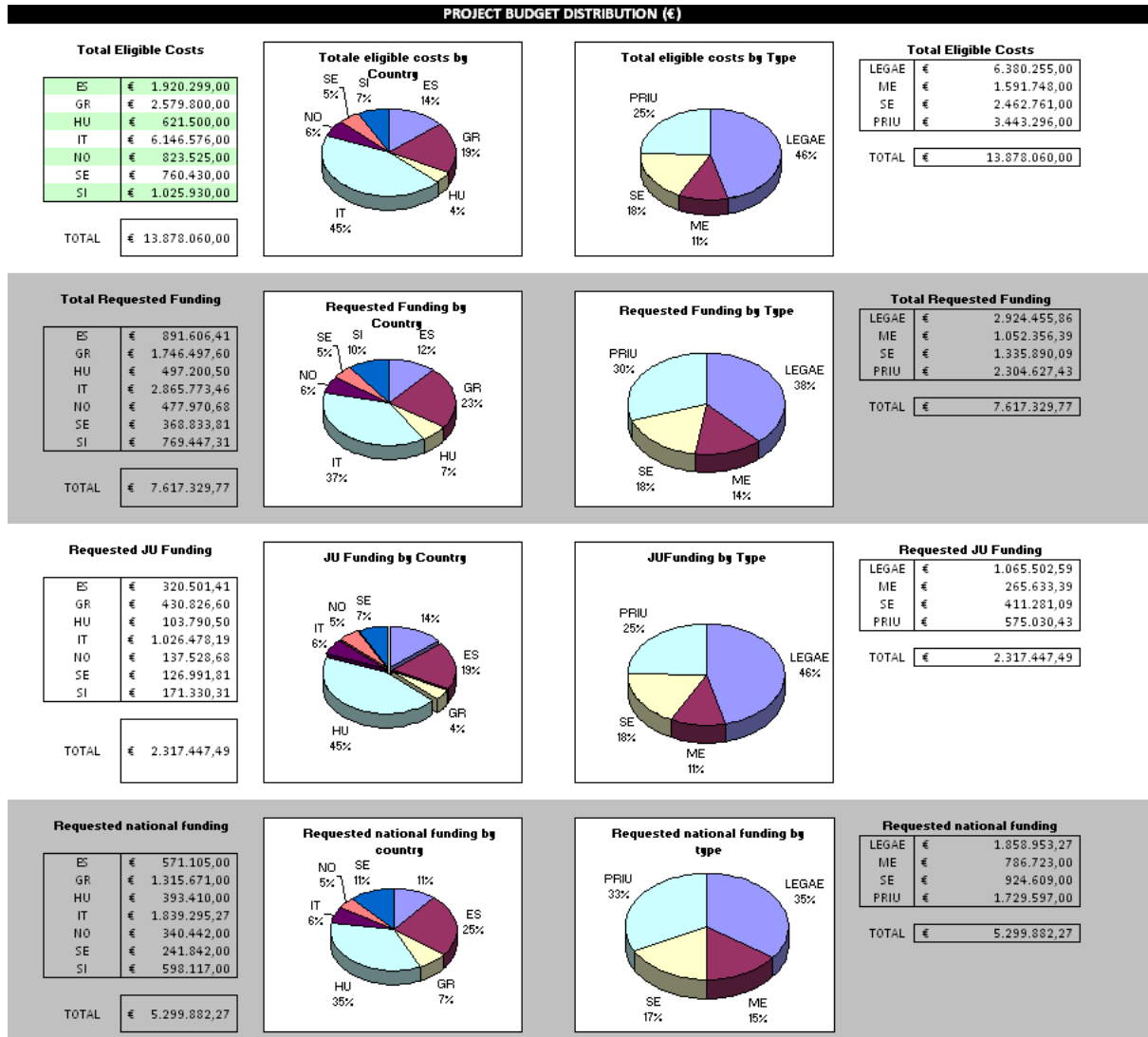
**Table 5.6 – Budget distribution**

Furthermore the project has been planned to leverage existing resources and technologies developed in other projects in order to minimize the resources requested for nSHIELD. 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 nSHIELD 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 list of the resources to be committed

| # | Partners | Resources |
|---|----------|-----------|

| # | Partners | Resources |
|---|----------|-----------|
| 1 | SG | • 2 workstation to run the SW of Aircraft Management Systems (10 K€)<br>• 2 IMA rack for developing and integrating IMA modules with nSHIELD Concept (10 K€)<br>• Specific software licenses (80 K€)<br>• Electronic components, microprocessor emulators, high speed serial analyzers (80 K€)<br>• Avionic Computer (140 K€)<br>Additional developing and computing/networking equipment and consumables will be provided by SG's own resources |
| 2 | ASTS | • 2 workstations to run the central and peripheral software of the security management system (client part) – 6K€<br>• 2 rack servers to run central and peripheral software of the security management system (server part) – 10K€<br>• 1 storage server to run the database of the security management system – 4K€<br>• 1 rack server to run the nSHIELD middleware – 5K€<br>• 1 rack POE Ethernet switch to connect the devices – 1K€<br>• 4 intelligent IP cameras to be used as sensors – 6K€<br>• 8 smart wireless sensors – 4K€<br>• 1 gateway for wireless networks – 1K€<br>• 1 rack and accessories – 2K€<br>• 1 rack UPS – 1K€<br>• 1 intrusion detection junction box – 2K€<br>• 1 intrusion detection gateway and related software licenses – 3K€<br>• 1 intrusion detection sensors (volumetric detectors, active infrared) – 3K€<br>• 2 access control devices – 2K€ |
| 3 | AS | • Electronic components, substrates, chemical products for PCB creation, modules for power supply modules, software tools for prototype – 33,5 k€ |
| 4 | ATHENA | *All necessary developing and computing equipment and consumables will be provided by ATHENA's own resources.* |
| 5 | ---- | ---- |
| 6 | ED | • 2 servers for developing software components and data storage systems - 5K€<br>• 2 small size PCs for hosting software components - 4K€<br>• licenses for Project specific software - 1K€ |
| 7 | TECNALIA | • PC Dell Optiplex 755 (with TPM, Trusted Platform Module) - 3,5 k€<br>• External eDNI LTC31 (C3PO) - 0,5 k€ |
| 8 | ESIS | • *All necessary developing and computing equipment and consumables will be provided by ESIS's own resources* |
| 9 | ETH | Electronics components to develop 3-5 nanonodes, a mobile/personal node and a power node; Freescale (or equivalent) development kit; Windows CE dev. kit; software tools for prototypes – 35 k€ |

| # | Partners | Resources |
|---|----------|-----------|
| 10 | HAI | • Special equipment (e.g. sensors, MOTEs, communication components) for testing and prototyping - 75k€<br>• Development platforms - 15k€<br>• Extra licenses for design and simulation tools, compilers - 30k€ |
| 11 | ISL | • *All necessary developing and computing equipment and consumables will be provided by ISL's own resources.* |
| 12 | ISD | • The following equipment will be purchased for the development of the audio acquisition system: Agilent DSA91204A 12GHz Oscilloscope with probe amplifiers and connectivity kit plus Agilent 16804A Logic Analyzer with extended memory and probes Total cost for equipment: 168,666.67<br>• The cost of the consumables for the audio acquisition system (microphones, boards, electronic components) is estimated to 120,000.00 |
| 13 | MAS | • *All necessary developing and computing equipment and consumables will be provided by MAS's own resources.* |
| 14 | MGEP | • Wireless communication components (wireless sensors, network devices) for construction of a heterogeneous mobile ad hoc network - 4k€ |
| 15 | NOOM | • *All necessary developing and computing equipment and consumables will be provided by NOOM's own resources.* |
| 16 | SCOM | • 2 servers for the HW and SW development, Set of licenses for the HW and SW design suites - 50K€ |
| 17 | S-LAB | *All necessary developing and computing equipment and consumables will be provided by S-LAB's own resources.* |
| 18 | SESM | *All necessary developing and computing equipment and consumables will be provided by SESM's own resources.* |
| 19 | SICS | secure hypervisor code for ARM systems |
| 20 | T2D | Secure software life cycle and recovery management software |
| 21 | TELC | ARM based, customized, access control lock control unit |
| 22 | THYIA | • Special equipment (e.g. embedded nodes), other components (SW&HW test platform) for testing and prototyping - 66k€.<br>• Equipment for 60 GHz radio and RoF technology. |
| 23 | TUC | TPMs, communication equipment, network analyzers, simulation tools/software, programmable wireless sensors & IP cameras and related software licences, €18.5K. Travel €20K. Additional developing and computing/networking equipment and consumables will be provided by TUC's own resources |
| 24 | UNIGE | *All necessary developing and computing equipment and consumables will be provided by UNIGE's own resources.* |
| 25 | UNIUD | • |
| 26 | UNIROMA1 | *All necessary developing and computing equipment and consumables will be provided by UNIROMA1's own resources.* |

**Table 5.7 – Resources to be committed for the nSHIELD 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 *(e.g. Category X in the table below)* in case your corresponding national cost categories do not fit the common ones

| Partic. no. | Partic. short name | Personnel | Durable Equipment | Consumables | Travel | Sub contracting | *(Other national categories)* | Indirect costs | Total costs |
|---|---|---|---|---|---|---|---|---|---|
| 1(C) | SG | 1.137.300,00 | | | 32.000,00 | | | 568.650,00 | 1.737.950,00 |
| 2 | ASTS | 259.200,00 | 0 | 0 | 0 | 40.000,00 | 20.000,00 | 129.600,00 | 448.800,00 |
| 3 | AT | 288.000,00 | | 33.500,00 | | 2.000,00 | 5.803,55 | 57.600,00 | 386.903,00 |
| 4 | ATHENA | 357.500,00 | 0 | 2.000,00 | 23.500,00 | 0 | 0 | 76.600,00 | 459.600,00 |
| 5 | --- | | | | | | | | |
| 6 | ED | 617.265,00 | 8.000,00 | | | | | 308.633,00 | 933.899,00 |
| 7 | TECNAL IA | 457.600,00 | 5.511,20 | 0 | | 0 | | 102.707,28 | 565.818,00 |
| 8 | ESIS | 92.755,00 | | | 5.000,00 | | 2.053,00 | 37.102,00 | 136.910,00 |
| 9 | ETH | 200.000,00 | | | | | | 100.000,00 | 300.000,00 |
| 10 | HAI | 997.920,00 | 50.000,00 | 10.000,00 | | 0 | 0 | 55.680,00 | 1.113.600,00 |
| 11 | INDRA | 572.000,00 | | 178,00 | | | | 114.400,00 | 686.578,00 |
| 12 | ISD | 208.000,00 | 168.666,67 | 50.000,00 | 20.000,00 | | | 22.333,33 | 553.000,00 |
| 13 | MAS | 156.798,00 | | | 8.000,00 | | 3.464,00 | 62.719,00 | 230.981,00 |
| 14 | MGEP | 226.082,70 | 2.150,00 | 1.150,00 | 0 | 0 | 6.402,74 | 45.216,00 | 281.000,00 |
| 15 | NOOM | 40.200,00 | | | 2.000,00 | | 887,00 | 16.080,00 | 59.167,00 |
| 16 | SCOM | 621.600,00 | 50.000,00 | 7.000,00 | 7.600,00 | 173.000,00 | | 310.800,00 | 1.170.000,00 |
| 17 | S-LAB | 540.000,00 | | | 25.000,00 | | | 56.500,00 | 621.500,00 |
| 18 | SESM | 173.600,00 | | | | | | 86.800,00 | 260.400,00 |
| 19 | SICS | 184.600,00 | | | | | | 101.530,00 | 286.130,00 |

| 20 | **T2D** | 244.800,00 | | | | | | 134.640,00 | 379.440,00 |
|----|---------|------------|---|---|---|---|---|-----------|-----------|
| 21 | **TELC** | 61.200,00 | | | | | | 33.660,00 | 94.860,00 |
| 22 | **THYIA** | 699.270,00 | 66.800,00 | 25950 | 15.000,00 | 45600 | 0,00 | 161.404,00 | 1.014.024,00 |
| 23 | **TUC** | 339.500,00 | 18.500,00 | | 20.000,00 | | | 75.600,00 | 453.600,00 |
| 24 | **UNIGE** | 335.580,00 | 1.250,00 | | | | | 130.876,00 | 468.706,00 |
| 25 | **UNIUD** | 222.000,00 | 20.000,00 | 5.000,00 | | | | 111.000,00 | 358.000,00 |
| 26 | **UNIROMA1** | 320.000,00 | | | | | | 160.000,00 | 480.000,00 |
| **Total** | | **9.352.770,70** | **390.877,87** | **134.778,00** | **158.100,00** | **260.600,00** | **38.610,29** | **3.060.130,61** | **13.480.866,00** |

**Table 5.8 - Summary of Effort and Costs**

| Partic. no. | Name | Partic. short name | | Travel | Justification |
|---|---|---|---|---|---|
| | | | | | |
| 1(C) | Selex Galileo | SG | IT | 32.000,00 | 10 trips for year |
| 2 | Ansaldo STS | ASTS | IT | 0,00 | |
| 3 | Acorde Technologies | AT | ES | 0,00 | |
| 4 | Athena Research and Innovation Center | ATHENA | EL | 23.500,00 | 5-6 trips for year |
| 5 | | --- | | 0,00 | |
| 6 | Elsag Datamat | ED | IT | 0,00 | |
| 7 | Fundacion Tecnalia | TECNALIA | ES | 0,00 | |
| 8 | ESIS Norge AS | ESIS | NO | 5.000,00 | 6 trips total |
| 9 | I.P.S. Sistemi Programmabili | ETH | IT | 0,00 | |
| 10 | Hellenic Aerospace Industry | HAI | EL | 0,00 | |
| 11 | Indra Software Labs | INDRA | ES | 0,00 | |
| 12 | Integrated System Development | ISD | EL | 20.000,00 | 5-6 trips for year |
| 13 | Movation AS | MAS | NO | 8.000,00 | 9 trips total |
| 14 | Mondragon Goi Eskola Politeknikoa | MGEP | ES | 0,00 | |
| 15 | Scandinavian Mobile Technology | NOOM | NO | 2.000,00 | 3 trips total |
| 16 | Selex Communication | SCOM | IT | 7.600,00 | 6 trips total |
| 17 | Search-lab Laboratory | S-LAB | HU | 25.000,00 | 5-6 trips for year |
| 18 | SESM | SESM | IT | 0,00 | |
| 19 | Swedish Institute Computer Science | SICS | SE | 0,00 | |
| 20 | T2 DATA | T2D | SE | 0,00 | |
| 21 | TELCRED | TELC | SE | 0,00 | |
| 22 | Thyia Technologije | THYIA | SI | 15.000,00 | 8-9 trips for year |
| 23 | Technical University of Crete | TUC | EL | 20.000,00 | 5-6 trips for year |
| 24 | Università Genova | UNIGE | IT | 0,00 | |
| 25 | Università Udine | UNIUD | IT | 0,00 | |
| 26 | Università Roma La Sapienza | UNIROMA1 | IT | 0,00 | |
| Total | | | | 158.100,00 | |

**Table 5.9 – Travel justification**

| CONSUMABLES | | | | | |
|---|---|---|---|---|---|
| Partic. no. | Name | Partic. short name | | Consumables | Justification |
| 1(C) | Selex Galileo | SG | IT | 0,00 | |
| 2 | Ansaldo STS | ASTS | IT | 0,00 | |
| 3 | Acorde Technologies | AT | ES | 33.500,00 | Electronic components, substrates, chemical products for PCB creation, modules for power supply modules, software tools for prototype |
| 4 | Athena Research and Innovation Center | ATHENA | EL | 2.000,00 | components used for the development of the prototype system |
| 5 | | --- | | 0,00 | |
| 6 | Elsag Datamat | ED | IT | 0,00 | |
| 7 | Fundacion Tecnalia | TECNALIA | ES | 0,00 | |
| 8 | ESIS Norge AS | ESIS | NO | 0,00 | |
| 9 | I.P.S. Sistemi Programmabili | ETH | IT | 0,00 | |
| 10 | Hellenic Aerospace Industry | HAI | EL | 10.000,00 | components used for the development of the prototype system |
| 11 | Indra Software Labs | INDRA | ES | 178,00 | |
| 12 | Integrated System Development | ISD | EL | 50.000,00 | components used for the development of the prototype system, PCB manufacturing. Cost for sensors (which may be significantly high depending on sensor quality) |
| 13 | Movation AS | MAS | NO | 0,00 | |
| 14 | Mondragon Goi Eskola Politeknikoa | MGEP | ES | 1.150,00 | software/middleware licenses acquired strictly for the purposes of the project |
| 15 | Scandinavian Mobile Technology | NOOM | NO | 0,00 | |
| 16 | Selex Communication | SCOM | IT | 7.000,00 | software/middleware licenses acquired strictly for the purposes of the project maintenance costs for the acquired equipment |
| 17 | Search-lab Laboratory | S-LAB | HU | 0,00 | |
| 18 | SESM | SESM | IT | 0,00 | |
| 19 | Swedish Institute Computer Science | SICS | SE | 0,00 | |
| 20 | T2 DATA | T2D | SE | 0,00 | |
| 21 | TELCRED | TELC | SE | 0,00 | |
| 22 | Thyia Technologije | THYIA | SI | 25.950,00 | components used for the development of the prototype system |
| 23 | Telecommunication Standard Institute | TSI | EL | 0,00 | |
| 24 | Università Genova | UNIGE | IT | 0,00 | |
| 25 | Università Udine | UNIUD | IT | 5.000,00 | software/middleware licenses acquired strictly for the purposes of the project |
| 26 | Università Roma La Sapienza | UNIROMA 1 | IT | 0,00 | |
| Total | | | | 134.778,00 | |

**Table 5.10 – Consumables justification**

| **SUB-CONTRACTING** | | | | | |
|---|---|---|---|---|---|
| **Partic. no.** | **Name** | **Partic. short name** | | **Sub contracting** | **Justification** |
| 1(C) | Selex Galileo | SG | IT | 0,00 | |
| 2 | Ansaldo STS | ASTS | IT | 40.000,00 | for technical consultancy, outsourcing SW development and deployment, support for on-the-field installation and assistance during testing on the trial vehicle and track |
| 3 | Acorde Technologies | AT | ES | 2.000,00 | |
| 4 | Athena Research and Innovation Center | ATHENA | EL | 0,00 | |
| 5 | | --- | | 0,00 | |
| 6 | Elsag Datamat | ED | IT | 0,00 | |
| 7 | Fundacion Tecnalia | TECNALIA | ES | 0,00 | |
| 8 | ESIS Norge AS | ESIS | NO | 0,00 | |
| 9 | I.P.S. Sistemi Programmabili | ETH | IT | 0,00 | |
| 10 | Hellenic Aerospace Industry | HAI | EL | 0,00 | |
| 11 | Indra Software Labs | INDRA | ES | 0,00 | |
| 12 | Integrated System Development | ISD | EL | 0,00 | |
| 13 | Movation AS | MAS | NO | 0,00 | |
| 14 | Mondragon Goi Eskola Politeknikoa | MGEP | ES | 0,00 | |
| 15 | Scandinavian Mobile Technology | NOOM | NO | 0,00 | |
| 16 | Selex Communication | SCOM | IT | 173.000,00 | part of the SDR/Cognitive Enabled Node will be subcontracted as explained at page 186 |
| 17 | Search-lab Laboratory | S-LAB | HU | 0,00 | |
| 18 | SESM | SESM | IT | 0,00 | |
| 19 | Swedish Institute Computer Science | SICS | SE | 0,00 | |
| 20 | T2 DATA | T2D | SE | 0,00 | |
| 21 | TELCRED | TELC | SE | 0,00 | |
| 22 | Thyia Technologije | THYIA | SI | 45600 | For Social Mobility and Networking (SMN) Scenarios (Annex B3) is mentioned that THYIA plans to use a national initiative in Slovenia related to the city of Kostanjevica. For SMN scenarios will be used some existing infrastructure technologies offered by THYIA's consortium composed of THYIA d.o.o., Josef Stefan Institute, and Our Space d.o.o. |
| 23 | Telecommunication Standard Institute | TSI | EL | 0,00 | |
| 24 | Università Genova | UNIGE | IT | 0,00 | |
| 25 | Università Udine | UNIUD | IT | 0,00 | |
| 26 | Università Roma La Sapienza | UNIROMA1 | IT | 0,00 | |
| **Total** | | | | **260.600,00** | |

**Table 5.11 – Sub-contracting justification**

This page intentionally left blank

# Annex A - Funding calculation forms

## Annex A.1 (for partners established in ARTEMIS Member States)

| Partner 1 SG | 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% |
| Industrial/Applied Research | 1.378.700,00 | 459.107,10 | 33,3% |
| Experimental development | 359.250,00 | 29817,75 | 8,3% |
| Total | 1.737.950,00 | 488.924,00 | |
| Total requested from the JU (16.7% of total above) | 290.237,65 | | |

| Partner 2 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 | 405.600,00 | 135.064,80 | 33,3% |
| Experimental development | 43.200,00 | 3.585,60 | 8,3% |
| Total | 448.800,00 | 138.650,40 | |
| Total requested from the JU (16.7% of total above) | 74.949,60 | | |

| Partner 3 AT | 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% |
| Industrial/Applied Research | 21.928,93 | 7.308,91 | 33,3% |
| Experimental development | 364.974,62 | 121.646,04 | 33,3% |
| Total | 386.903,55 | 128.954,95 | |
| Total requested from the JU (16.7% of total above) | 64.612,89 | | |

| 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 | 0,00% |
| Industrial/Applied Research | 459.600,00 | 382.846,80 | 83,3% |
| Experimental development | 0,00 | 0,00 | |
| Total | 459.600,00 | 382.846,80 | |
| Total requested from the JU (16.7% of total above) | 76.753,20 | | |

| Partner 5 --- | 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 | | | |
| Industrial/Applied Research | | | |
| Experimental development | | | |
| Total | | | |
| Total requested from the JU (16.7% of total above) | | | |

| Partner 6 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% |
| Industrial/Applied Research | 793.610,00 | 264.272,13 | 33,3% |
| Experimental development | 140.287,50 | 11.643,86 | 8,3% |
| Total | 933.897,50 | 275.915,99 | |
| Total requested from the JU (16.7% of total above) | 155.960,88 | | |

| Partner 7 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% |
| Industrial/Applied Research | 565.818,00 | 188.606,16 | 33,3% |
| Experimental development | 0,00 | 0,00 | 33,3% |
| Total | 565.818,00 | 188.606,16 | |
| Total requested from the JU (16.7% of total above) | 94.303,08 | | |

| Partner 8 ESIS | 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% |
| Industrial/Applied Research | 136.910,00 | 45.591,03 | 33,3% |
| Experimental development | 0,00 | 0,00 | 8,3% |
| Total | 136.910,00 | 45.591,03 | |
| Total requested from the JU (16.7% of total above) | 22.863,97 | | |

| Partner 9<br>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% |
| Industrial/Applied Research | 270.000,00 | 89.910,00 | 33,3% |
| Experimental development | 30.000,00 | 2.490,00 | 8,3% |
| Total | 300.000,00 | 92.400,00 | |
| Total requested from the JU (16.7% of total above) | 50.100,00 | | |

| Partner 10<br>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% |
| Industrial/Applied Research | 1.113.600,00 | 370.828,80 | 33,3% |
| Experimental development | 0,00 | 0,00 | 18,3% |
| Total | 1.113.600,00 | 370.828,80 | |
| Total requested from the JU (16.7% of total above) | 185.971,20 | | |

| Partner 11 INDRA | 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% |
| Industrial/Applied Research | 686.578,00 | 159.972,67 | 23,3% |
| Experimental development | 0,00 | 0,00 | 23,3% |
| Total | 686.578,00 | 159.972,67 | |
| Total requested from the JU (16.7% of total above) | 114.658,53 | | |

| Partner 12 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 | 33,3% |
| Industrial/Applied Research | 553.000,00 | 184.149,00 | 33,3% |
| Experimental development | 0,00 | 0,00 | 33,3% |
| Total | 553.000,00 | 184.149,00 | |
| Total requested from the JU (16.7% of total above) | 92.351,00 | | |

| Partner 13 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 | 0% |
| Industrial/Applied Research | 230.981,20 | 76.916,74 | 33,3% |
| Experimental development | 0,00 | 0,00 | 8,3% |
| Total | 230.981,20 | 76.916,74 | |
| Total requested from the JU (16.7% of total above) | 38.573,86 | | |

| 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% |
| Industrial/Applied Research | 281.000,00 | 93.573,00 | 33,3% |
| Experimental development | 0,00 | 0,00 | 33,3% |
| Total | 281.000,00 | 93.573,00 | |
| Total requested from the JU (16.7% of total above) | 46.927,00 | | |

| Partner 15 NOOM | 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% |
| Industrial/Applied Research | 59.167,00 | 19.702,61 | 33,3% |
| Experimental development | 0,00 | 0,00 | 8,3% |
| Total | 59.167,00 | 19.702,61 | |
| Total requested from the JU (16.7% of total above) | 9.880,89 | | |

| SCOM | Total eligible costs according to national rules (in €) | National Contribution requested (in €) | National Funding % |
|---|---|---|---|
| Fundamental/Basic Research | 0,00 | 0,00 | 0% |
| Industrial/Applied Research | 956.000,00 | 318.348,00 | 33,3% |
| Experimental development | 214.000,00 | 17.762,00 | 8,3% |
| Total | 1.170.000,00 | 336.110,00 | |
| Total requested from JU (16.7% of total above) | 195.390,00 | | |

| Partner 17 S-LAB | 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% |
| Industrial/Applied Research | 621.500,00 | 393.410,00 | 63.3% |
| Experimental development | 0,00 | 0,00 | 0% |
| Total | 621.500,00 | 393.410,00 | |
| Total requested from the JU (16.7% of total above) | 103.791,00 | | |

| Partner 18 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% |
| Industrial/Applied Research | 260.400,00 | 86.713,20 | 33,3% |
| Experimental development | 0,00 | 0,00 | 8,3% |
| Total | 260.400,00 | 86.713,20 | |
| Total requested from the JU (16.7% of total above) | 43.486,80 | | |

| Partner 19<br>SICS | 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% |
| Industrial/Applied Research | 286.130,00 | 165.955,40 | 58,0% |
| Experimental development | 0,00 | 0,00 | 0,0% |
| Total | 286.130,00 | 165.955,40 | |
| Total requested from the JU (16.7% of total above) | 47.783,71 | | |

| Partner 20<br>T2D | 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% |
| Industrial/Applied Research | 379.440,00 | 60.710,40 | 16,0% |
| Experimental development | 0,00 | 0,00 | 0,0% |
| Total | 379.440,00 | 60.710,40 | |
| Total requested from the JU (16.7% of total above) | 63.366,48 | | |

| Partner 21 TELC | 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% |
| Industrial/Applied Research | 94.860,00 | 15.177,60 | 16,0% |
| Experimental development | 0,00 | 0,00 | 0,0% |
| Total | **94.860,00** | **15.177,60** | |
| Total requested from the JU (16.7% of total above) | **15.841,62** | | |

| Partner 22 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% |
| Industrial/Applied Research | 1.014.024,00 | 591.175,99 | 58,3% |
| Experimental development | 0,00 | 0,00 | 0,0% |
| Total | **1.014.024,00** | **591.175,99** | |
| Total requested from the JU (16.7% of total above) | **169.342,01** | | |

| Partner 23 TUC | 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 | 83,3% |
| Industrial/Applied Research | 453.600,00 | 377.848,80 | 83,3% |
| Experimental development | 0,00 | 0,00 | 83,3% |
| Total | 453.600,00 | 377.848,80 | |
| Total requested from the JU (16.7% of total above) | 75.751,20 | | |

| Partner 24 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% |
| Industrial/Applied Research | 468.075,00 | 155.868,98 | 33,3% |
| Experimental development | 0,00 | 0,00 | 8,3% |
| Total | 468.075,00 | 155.868,98 | |
| Total requested from the JU (16.7% of total above) | 78.168,53 | | |

| Partner 25 UNIUD | 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% |
| **Industrial/Applied Research** | 316.000,00 | 105.228,00 | 33,3% |
| **Experimental development** | 42.000,00 | 3.486,00 | 8,3% |
| **Total** | **358.000,00** | **108.714,00** | |
| **Total requested from the JU (16.7% of total above)** | **59.786,00** | | |

| Partner 26 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** | 480.000,00 | 159.840,00 | 33,3% |
| **Experimental development** | 0,00 | 0,00 | 8,3% |
| **Total** | **480.000,00** | **159.840,00** | |
| **Total requested from the JU (16.7% of total above)** | **80.160,00** | | |

This page intentionally left blank

# Annex B - Application Scenarios

The following application scenarios will be detailed in this section:
- Railways security;
- Voice/Facial Recognition;
- Dependable Avionic Systems;
- Social Mobility.

All the selected application scenarios address Security, Privacy and Dependability as a whole, however each scenario focuses on peculiar needs:
- Security and Dependability for railways;
- Privacy, Security and Dependability for Voice/Facial recognition
- Security and Dependability for Avionic Computer;
- Privacy, Security and Dependability for Social Mobility Network.

# *Annex B.1 – Railway Security*

## **Case (1)**

Rail-based mass transit systems are vulnerable to many criminal acts, ranging from vandalism to terrorism. Therefore, physical security systems for infrastructure protection have been designed by Ansaldo STS which are specifically tailored to urban or metropolitan railways (mainly subways, i.e. featuring underground stations and tunnels). In these systems, heterogeneous intrusion detection, access control, intelligent video-surveillance and abnormal sound detection devices are integrated in a cohesive Security Management System (SMS). The core of the SMS consists of a web-based software application featuring a graphical user interface. System architecture is distributed and hierarchical, with both local and central control rooms collecting alarms according to different scopes and responsibilities. In case of emergencies, the procedural actions required to the operators involved are orchestrated by the SMS. Redundancy both in sensor dislocation and hardware apparels (e.g. by local or geographical clustering) improve detection reliability, through alarm correlation, and overall system resiliency against both random and malicious threats. Video-analytics is essential, since a small number of operators would be unable to visually control the large number of cameras which are needed to extensively cover all the areas needing to be protected. Therefore, the visualization of video streams is activated automatically when an alarm is generated by smart-cameras or other sensors, following an event-driven approach. The system is able to protect stations (accesses, technical rooms, platforms, etc.), tunnels (portals, ventilation shafts, etc.), trains and depots. Very high resolution cameras installed close to the turnstiles are used to automatically detect and store the faces of passengers, whose database can be accessed for post-event investigations. Real-time communication between the on-board and the ground is allowed by a wide-band wireless network.

## *Application of SHIELD to SMS dependability and security*

Currently, the security system described above is highly heterogeneous in terms not only of detection technologies (which will remain such) but also of embedded computing power and communication facilities. In other words, sensors differ in their inner hardware-software architecture and thus in the capacity of providing information security and dependability. This causes several problems:

- Information security must be provided according to different mechanisms and on some links - which are not "open" but still vulnerable to attacks - information is not protected by cryptographic nor vitality-checking protocols;
- Whenever any new sensor needs to be integrated into the system, a new protocol and/or driver must be developed and there is no possibility of directly evaluating the impact of such integration on the overall system dependability;
- New dedicated and completely segregated network links often need to be employed in order not to make the sensor network exposed to information related threats;
- The holistic assurance and evaluation of dependability parameters (e.g. for assessment/certification purposes) would be a very difficult task.

In particular both natural and malicious faults can impact on system availability and indirectly on safety, since the SMS is adopted in critical infrastructure surveillance applications.

The problems mentioned above can be solved by adopting the SHIELD architecture. Cohesion will be assured by wrapping sensors of any nature with homogeneous embedded hardware and software providing information security, by e.g.:

- Cryptographic protocols
- Vitality checking (heartbeat/watchdog timers based on sequence numbers and time-stamping)

The mechanisms provided by SHIELD would mitigate the effects on the system of the following logical threats:
- Repetition (a message is received more than once)
- Deletion (a message is removed from a message stream)
- Insertion (a new message is implanted in the message stream)
- Re-sequencing (messages are received in an unexpected sequence)
- Corruption (the information contained in a message is changed, casually or not)
- Delay (messages are received at a time later than intended)
- Masquerade (a non-authentic message is designed thus to appear to be authentic)

*SHIELD-SMS demonstrator*

We aim at developing an example application of SHIELD to a reference SMS architecture which includes a significant yet reduced set of detection devices. To achieve this objective, some sensors will be converted into smart-sensors by integrating the sensor unit with the SHIELD "standard" processing units (both hardware and software), then the (possibly wireless) sensor networks will be integrated by the SHIELD middleware before data is collected by the SMS. SMS will then process received data considering sensors as fully trusted information sources. The process is reversible, in order to provide bidirectional dependable communications, thus to include remote control commands from SMS to actuators (e.g. visual or audio alarm activation, access lock/unlock, etc.). Before developing the prototype, a set of non functional specifications (including quantitative indices) will be issued considering the dependability requirements of the example application.

## Case (2)
This use case deals with the complex processes in the railroad administration, responsible for functionality, safety and quality in the operation of the railroad infrastructure. The processes and platforms involved in the administration of the railroad infrastructure have strong dependability, and small disturbances may cause parts of the network to dysfunction.

The goal of this use case is to add sensors and mobile technologies to the processes and platforms, and by that enhancing the processes, delivering better performance, acting faster on disturbances and increase the quality of the whole railway operation.

A simplified example of such dependability between processes is the train scheduling based on railway infrastructure, train infrastructure and devices carried by on-board personnel. Normal reporting of train positions is performed through railway infrastructure, typically train axis counters at certain points of the track. A miss-counting will normally establish an error message, which might cause the whole rail segment to be closed for traffic. By involving the power-reporting cycle of the respective train an updated situation update can be requested, which can relax the strict "no-traffic" relation. Looking forward towards the European Rail Traffic Management System (ERTMS) will require an even tighter dependability between both onboard and railway infrastructure. ERTMS level 1 calculates the maximum speed of the train based on onboard equipment and the next braking point if needed, taking into account the train braking characteristics and the track description data. The main challenge is to bring the various sources of information into the railroad administration infrastructure.

This use case answers:
multi-layer: from sensors, mobile technologies towards business processes
dependable: dependable processes, sensor input
embedded:   use of sensors and mobile technology (not that strong, mainly active sensors)

## *Annex B.2 – Dependable Avionic Computer*

The trend for modern aircrafts is to support aircraft applications with an Integrated Modular Avionic (IMA) Platform instead of Federated platform. The next generation of IMA platform should include reconfiguration capabilities in order to limit the effects of hardware failures on aircraft operational reliability.

Therefore future On Board Computer shall be developed in accordance with IMA philosophy that takes in consideration all the MOSA (Modular Open System Approach) principles.

Integrated Modular Avionics (IMA) employs partitioned environment, where different avionics functions share a unique computing environment that can still be certified against an airworthiness code.

Being IMA essentially a real time computer network for airborne system, by definition it is composed by different modules capable of supporting numerous application and different functions. This will allow also to develop HW and SW to share in the same IMA cabinet both safety and not safety functions.

This will allow the avionic architecture to be more easily scaled to meet the different interfacing and processing requirements of different aircraft types. Scalability will allow the capability to add more I/O interfaces independently of the processing resources. This approach will also allow flexibility in locating and relocating software applications, which is requisite for reconfiguration to achieve fault tolerance and very high availability.

System (computers) built with the IMA/MOSA philosophy can be adapted easily for a great variety of platform, this philosophy fully implements and exploit the concept of design flexibility and open HW and SW architecture (MOSA), intended to grant to third part Avionics Industries the real possibility to integrate their HW/SW modules i.a.w. open standards.

Because the logical distribution and physical separation of I/O functions and processing, the Integrated Avionics System configuration can be easily tailored to match the End-User's (i.e. Airline Company) specific requirements.
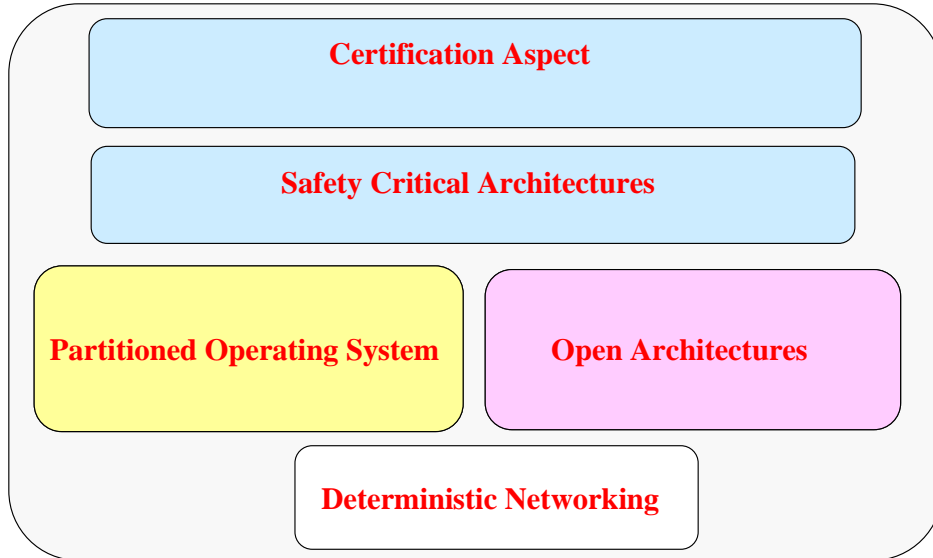
The strategy considered to cope with the required modularity is based on the identification of On Board Computers and Remote Interface Units (RIU), the former being devoted to host high complexity software applications and planned not to be subject to hardware modifications when transferred from one aircraft to another, while the latter are planned to host low complexity software applications, since they will have to bear the impact of hardware modifications in order to adapt to the different installation environments.

As the hardware modules are shared across between various software applications therefore there are tight legal requirements imposed by the aviation authorities on the design of the IMA. The design proposal is based on the ARINC architecture in which the resources such as processing, memory and communication ports are shared between the various software applications.
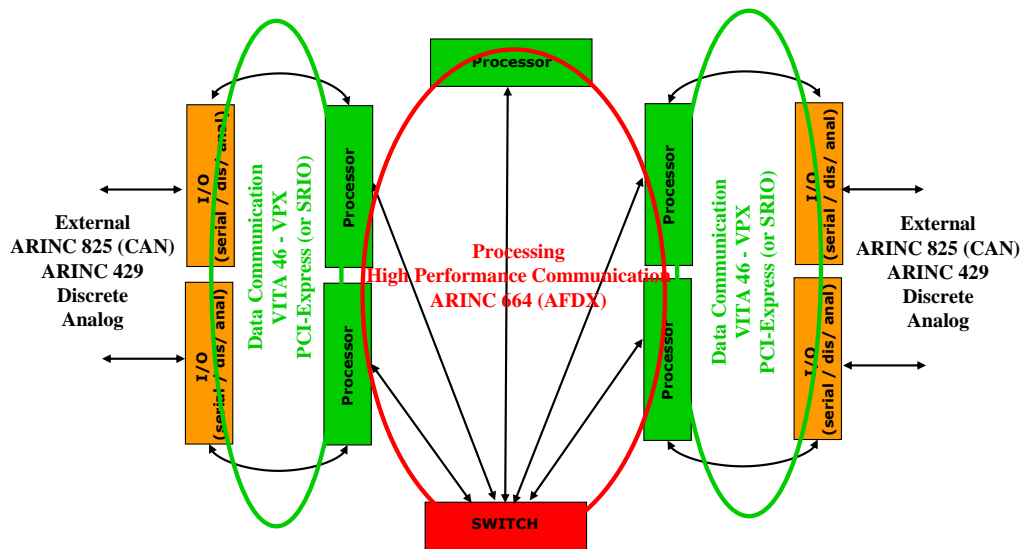
In addition, the intrinsic modularity of IMA will allow avionic architecture will be more easily scaled to meet the different interfacing and processing requirements of different aircraft types. Scalability will allow the capability to add more I/O interfaces independently of the

processing resources. This will also allow flexibility in locating and relocating software applications, which is requisite for reconfiguration to achieve fault tolerance and very high availability

**Avionic Computing Key Pillars**

**Certification Aspect**

**Safety Critical Architectures**

**Partitioned Operating System**

**Open Architectures**

**Deterministic Networking**

Avionic Computing key pillars

Modular Avionic Architecture

# Annex B.3 - Social Mobility and Networking Scenarios

## Introduction

In sociology and economics, as well as in common political discourse, **social mobility** refers to the degree to which an individual or group's status is able to change in terms of position in the social hierarchy. In this project it is related to humans to move from one place to other. Mobility is human's nature. The project nSHIELD is considered social mobility and networking (SMN) as a scenario of humans that are moving from one place to other by walking, using public means of transport or personal one, such a bicycle, car, etc., and they desired to communicate with other persons or things (here we are referring to the future **I**nternet of **T**hings and **H**umans, named here ITH). There will be two different sub-scenarios, indoor and outdoor.  Indoor sub-scenario is related to social mobility of people inside the houses, buildings, etc. Outdoor sub-scenarios is related to social mobility of people on the streets in cites/towns, villages, highways, and other roads.

## Definition

**Social mobility** is related to movements of persons within a collective co-existence, irrespective of whether they are aware of it or not in which a social interaction can be created between two or more individuals.

**Social networking** is related to a social or *opportunistic network* is a social structure made up of individuals called "nodes," which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, etc.

**Opportunistic networks** will change the way people communicate by allowing direct one-hop communications between handheld or other devices carried by human beings while on the move. Users will be involved in participatory interactions with their surrounding using applications (e.g., mobile social networking, content distribution, flea-markets, micro-blogs) enhancing the experience of real-world social networks with digital and ubiquitous features.

## Description of MSN scenario

Many kinds of communication networks, in particular social and opportunistic networks, rely at least partly on humans to help move data across the network. Thus these networks will play an important role in development of future ITH. In this vision of the future a multitude of devices carried by people will be dynamically networked. The tremendous demands from social market are pushing the booming development of mobile communications faster than ever before, leading to plenty of new advanced techniques emerging. Mobile communications are changing people's life style in many ways. Behind the scenario, the fantastic characteristic that makes this reality is mobility. In the field of computing and communication technologies, to be able to communicate with other persons and access and process information simultaneously while moving has been as a long expectation that causes great deal of efforts having been made to turn the fancy into fact. The humans would like to communicate with other persons in any place and time, as well to access any information it is important the use of existing communication networks. Additionally, a convergence of mobile and fixed communications (global trend) with enhanced functionality offered by a convergence and continuity of services over radio, optical, and PLC technologies developed in OMEGA project will made the future ITH a true reality.

In this project we are also referring to Directive 2009/125/EC of the European Parliament, i.e., eco-design directive and other energy-efficient legalization for household lamps and

streets lights.  These lights in many municipalities accounts for nearly half of the electrical expenditure. In addition to the energy bills, the replacement and maintenance of low-pressure sodium or metal halide lamps pose additional costs and disruption of traffic. Solar-powered street lights using High Brightness LEDs (HBLED) do not depend on the grid for electric power and have the potential of saving billions of dollars in electricity and maintenance costs. Since, we are expecting an important implementation of this directive in Europe in forthcoming years, nSHIELD project set-up the SMN scenario based also on the possibility to build on top of existing electricity infrastructure a new communication infrastructure everywhere where the new lumps and technologies will replace old one. Despite their possibilities, the new street lights are not commonplace because of their price compared to conventional alternatives. Nevertheless, as the world looks for cleaner and greener alternatives, the new street lights continue to benefit from advancements in the field of semiconductors, both in photovoltaic and integrated microcontrollers, embedded devices, to produce more cost-effective implementations.

In the scope of MSN in the nSHIELD project we are aiming to present this as a common R&D area in which SPD play an extremely important role for a successful implementation of SMN scenario. The Figure below illustrates how different filed will interact jointly in this scenario. There are four fundamental areas:

1. new Streets and Building Lights (SBLs),
2. Public and Private Transportation Means PPTMs,
3. the future Internet of Things and Humans (ITHs), and
4. Ubiquitous and/ Pervasive Computing (U&PC)

that have a common one, i.e., SPD aspects that are considered in details in this project in which a common nSHIELD system architecture is composed of four layers: node, network, middleware and overlay, that play an important role in the implementation of SMN scenario. In SMN scenarios a focus will be given to intelligent systems and intelligent ICT, since intelligent street lighting is maturing and providing cost-effective approach to manage municipal street lighting.
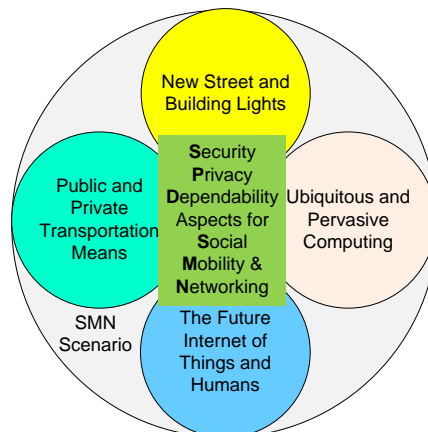


Social Mobility and Networking Scenario.

*How different areas presented in this Figure will interact in the MSN scenario and framework of nSHIELD?*

There were 4.1 billion mobile phone users around the world in the year 2008 that surpassed the total number of Internet users. It is anticipated that at least 15% of mobile phone users will be involved in mobile social applications over the next few years.  The nSHIELD system architectural concept with emphasis on SPD aspects will contribute even more to a highest

penetration of social networking. For that we need to integrate the old and new communication infrastructures. This lead to the creation of large and complex networks called *real-life networks* that include: electrical power grid, World Wide Web, the Internet backbone, collaboration and citation networks, and airline connection networks. Step-by-step, we are moving into a world of ubiquitous and pervasive computing (U&PC), Security, Trust, Privacy and Dependability Privacy (STPD) issues will be in focus more than ever before. Sensor networks have been used in numerous applications such as remote sensing, environmental monitoring, habitat, human activity, health monitoring, industrial appliances monitoring, medical applications, space and underwater phenomena monitoring, home and building automation and so on. Capturing sensory data from Body Area Networks (BANs), or Body Sensor Networks (BSNs) and sending it to social networks is challenging task, because it required a number of distributed networks to work together seamlessly. Disseminating the sensory data in real time to one's community of interest such as family, friends, family doctors, and emergency services is very crucial and critical. Therefore, SPD aspects are needed in such a complex networks and environments. Location Based Social Networking (LBSN) applications such as Google Latitude, Loopt and BrightKite enhance our ability to perform social surveillance. These applications enable users to view and share real time location information with their "friends".

*How the four areas interact with SPD aspects is briefly described below*?

First, **PPTMs** play important role in social life of people. For example, bus, tram, trains, ships, cruisers, aircrafts, etc., are place that an individual can interact with other people and surrounding environments. The same when an individual is using his/her bicycle, motorcycle, car, camions, boats/yachts, etc. For example, the railways scenario e easily integrated in SMN scenario. Second, the future **ITH** is one of the most important areas of research in FP7. Additionally, internet based social networking services have experienced an enormous growth over the past years. Popular social networking services, such as MySpace or Facebook, have gained tens of millions of users in less than 10 years. Simultaneously to the social networking services' triumphant advance, mobile devices in general and smart phones in particular have rapidly penetrated the consumer market. Recent phones do not only exhibit considerable computing resources but also feature means for Internet access as well as wireless short distance communication such as Bluetooth and Wi-Fi. They seem to be the perfect platform to combine the market potential of traditional social networking services and the success story of mobile devices. Even though several attempts that have tried to merge the two worlds could not reach the masses, experts expect that future mobile social networking systems possibly even exceed the success of their Internet bound counterparts. We believe that two key features are the user's permanent reachability and location awareness, which is called P3 (Pear-to-Pear-to-Place). Third, **U&PC** devices are very tiny - even invisible - devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods - all communicating through increasingly interconnected networks. "*Things that think want to link*", Nicholas Negroponte of MIT Media Labs is quoted as saying. This is the doctrine on which pervasive computing is based! A scenario where all devices are networked, human-centric, communicate and interact with each other without any hiccups; their primary objective being to bestow quality life to the user. What's so beautiful about pervasive computing is that it is an important part of our lives even now, but in ways that we don't really notice. Fourth, **SBLs** will have impact on streets and building lighting, since it is a European directive acting as new European standard. The state-of-the art of the street lighting and the future expectation in the partner-countries is enormous. There are already projects like E-street [www.e-strretlight.com](www.e-strretlight.com), Lites project [http://www.lites-project.eu/](http://www.lites-project.eu/), and other national initiative, such as Slovenian in city of Kostanjevica. Using electrical grid and combining it with possibility not only to manage intelligently the street

lights, but also to communicate over different access technology (optical, radio and PLC) what is proved in OMEGA project http://www.ict-omega.eu/ represent an important technology breakthrough toward an implementation of SMN scenarios during this project and thus prove the concept. The SMN scenario to be proved includes: 1) SPD concept, 2) intelligent applications built on the nSHIELD system architecture, and 3) new street lights with LED or other solid state lighting technologies. This scenarios lie in ecodesign, embedded systems that contribute not only for social interactions of humans, but also in sense significant carbon dioxide reduction, significant energy savings, safety regulation, and SPD aspects. The scenarios will be demonstrated inside a big meeting room (indoor), or on the street in a village (outdoor). The lights will provide wireless optical down link. The user will have different possibility for access technologies in up-link. For example UMTS, or short range 60 GHz radio communication link.

## *Literature*

[1]    J. Rana et all, "An Architecture for Mobile Social Networking Applications," Int. Conference on Computational Intelligence, Communication Systems and Netwoks, 2009, pp. 241-245.
[2]    R. M. Savola, "Current and Emerging Security, Trust, Dependability and Privacy Challenges in Mobile Telecommunications, 2009 International Conference on Dependability, pp, 7-12.
[3]   S. Trifunovic et all., "Social Trust in Opportunistic Networks," IEEE INFOCOM 2010.
[4]   R. S. Monclar, "Analysis and Balancing of Social Networks to Improve the Knowledge Flow on Multidisciplinary Teams," 2009 13th Int. Conf. on Computer Supported Cooperative Work and Design," pp. 662-667.
[5]    Eva Jaho and Ioannis Stavrakakis, "Joint Interest- and Locality-Aware Content Dissemination in Social Networks," FP7 project SOCIAL-NETS.
[6]    Jun-Zhao and J. Sauvola, "On Fundamental Concept of Mobility for Mobile Communications, PIMRC 2002, pp. 799-803.
[7]   K. Lee et all., "SLAW: A Mobility Model for Human Walk," IEEE INFOCOM 2009, pp. 855-863.
[8]   D. Quercia and S. Hailes, "Sybil Attack Against Mobile Users: Frends and Foes to the Rescue, IEEE INFOCOM 2010.
[9]   Marco von Arb et all, "VENETA: Serverless Friend-ofFriend Detetction on Mobile Social Networking," 2008 IEEE Int. Conf. on Wireless & Mobile Computing, Networking & Communications, pp. 184-189.
[10]   S. J. Fusco et all., "Exploring the Social Implications of Location Based Social Networking," 2010 Int. Conf. on Mobile Busoness, pp. 230-237.
[11]    S. Gunasekarn and N. Nagarajan, "Improving the Community Behaviour of Social Network Theory Based Mobility Model for MANET," ICCCN 2008.
[12]   E-street project, http://www.e-streetlight.com/
[13] LITES: Led-based intelligent street lighting for energy saving, http://www.lites-project.eu/lites-led-based-intelligent-street-lighting-energy-saving
[14]    B. Qureshi et all, "An Adaptive Content Sharing protocol for P2P Mobile Social Networks," 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, pp. 413-418.
[15]    G. Chen and F. Rahman, "Analyzing Privacy Designs of Mobile Social Networking Applications", 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, pp 83-88, December 17-20,2008.

[16] J. Wu (eds), "Peer-to-Peer Overlay Abstractions in MANETs", Handbook on Theoretical and Algorithmic Aspects of Sensor Ad Hoc Wireless, and Peer-to-Peer Networks, Auerbach Publications, Pp 857-874, 2005.
[17] OMEGA project, http://www.ict-omega.eu/
[18] IMSKA project, http://cordis.europa.eu/fetch?CALLER=FP7_SECURITY_PROJ_EN&ACTION=D&DOC=6&CAT=PROJ&QUERY=0123edbf115d:0f9b:05bcccb2&RCN=90096 .
[19] TITRES (Telecommunication Innovation in Telecomuncation for Rational Ecological Systems) Project, A Slovenian project, RIP 09/67 lead by THYIA d.o.o.

# Annex C - List of conferences and journals

| # | Title | Period | Language | Link |
|---|-------|--------|----------|------|
| 1 | **IEEE Transactions on Software Engineering** | Monthly | English | http://www2.computer.org/portal/web/tse/ |
| 2 | **ACM Transactions on Software Engineering Methodology** | Monthly | English | http://tosem.acm.org/ |
| 3 | **International Journal of Software Engineering & Knowledge Engineering** | Every 2 months | English | http://www.worldscinet.com/ijseke/ijseke.shtml |
| 4 | **IEEE Software** | Every 2 months | English | http://www2.computer.org/portal/web/software/ |
| 5 | **IEEE Transactions on Computer** | Monthly | English | http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=12 |
| 6 | **IEEE Transactions on Reliability** | Every 3 months | English | http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=24 |
| 7 | **IEEE Embedded Systems Letters** | Every 3 months | English | http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5170179 |
| 8 | **ACM Transactions in Embedded Computing Systems (TECS)** | Every 3 months | English | http://acmtecs.acm.org/index.htm |
| 9 | **IEEE Transactions on Signal Processing** | Monthly | English | http://www.signalprocessingsociety.org/publications/periodicals/tsp/ |
| 10 | **IEEE Signal Processing Letters** | Monthly | English | http://www.signalprocessingsociety.org/publications/periodicals/letters/ |
| 5 | **Logistics Research** | Halbyearly | English | http://www.bvl.de/8049_1 |
| 6 | **Transportation Science** | Quarterly | English | http://www.informs.org/site/TranSci/ |
| 7 | **Naval Research Logistics** | Monthly | English | http://www.nrljournal.com/ |
| 8 | **International Journal of Shipping and Transport Logistics  (IJSTL)** | Quarterly | English | http://www.inderscience.com/browse/index.php?journalCODE=ijstl |
| 9 | **Maritime Policy & Management** | Every 2 month | English | http://www.tandf.co.uk/journals/titles/03088839.asp |
| 10 | **Transport Review** | Every 2 month | English | http://www.tandf.co.uk/journals/tf/01441647.html |
| 11 | **RFID im Blick** | Monthly | German | http://rfid-im-blick.de/index.php |
| 12 | **RFID Update** | daily | English | http://www.rfidupdate.com/ |
| 13 | **RFID Journal** | Every 2 month | English | http://www.rfidjournal.com/ |
| 14 | **SMART Mag** | Monthly | German | http://www.smartmag.de/ |
| 15 | **SMART Solutions 200x** | Yearly | German | http://www.rfid-ready.de/printausgabe-smart-solutions.html |
| 16 | **Logistik Journal; Transportlogistik** | | German | http://www.logistik-journal.de |
| 17 | **Internationales Transportjournal** | Every 2 weeks | German/ English | http://www.transportjournal.com/ |
| 18 | **Journal of Commerce** | Wöchentlich | English | http://www.joc.com/ |

**Table C.01 – selected Journals for dissemination**

| # | Title | Period | Link |
|---|-------|--------|------|
| 1 | **International Conference on Dependability** | yearly | http://www.iaria.org/conferences2009/DEPEND09.html |
| 2 | **International Cryptology Conference** | yearly | http://www.iacr.org/conferences/crypto2009/ |
| 3 | **Annual International Conference on the Theory and Applications of Cryptographic Techniques** | yearly | http://www.iacr.org/conferences/eurocrypt2009/ |
| 4 | **International Conference on Software Engineering** | yearly | http://www.icse-conferences.org/ |
| 5 | **International Conference on Software Engineering and Knowledge Engineering** | yearly | http://www.ksi.edu/seke/seke09.html |
| 6 | **International Conference on Software Engineering and Data Engineering** | yearly | http://sce.uhcl.edu/sede09/ |
| 7 | **IEEE International Symposium on Circuits and Systems (ISCAS)** | yearly | http://www.iscas2011.org/ |
| 8 | **Embedded System Conferences (ESC)** | quaterly | http://esc-sv09.techinsightsevents.com/ and related sites |
| 9 | **IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)** | yearly | http://conference.cs.cityu.edu.hk/rtcsa2010/ |
| 10 | **IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)** | yearly | http://www.rtas.org/ |
| 7 | **Conference on Container Security** | yearly | http://ec.europa.eu/enterprise/security/csc.htm; |
| 8 | **Supply Chain Security** | yearly | http://www.container-security.org/ |
| 9 | **Transec World Expo; Maritim Supply Chain and Security** | yearly | http://www.transec.com/page.cfm/Link=110/t=m/goSection=4 |
| 10 | **European Supply Chain and Logistics Summit** | yearly | http://www.supplychain.eu.com/ |
| 11 | **IEEE International Conference on RFID** | yearly | www.ieee-rfid.org |
| 12 | **Western Europe Regional Final 2009** | yearly | http://www.globalsecuritychallenge.com/page_display.php?p=7&id=116 |
| 13 | **Germaner Logistik Kongress** | yearly | http://www.bvl.de/dlk |
| 14 | **Germaner Materialfluss Kongress** | Every 3 years | www.materialflusskongress.de |
| 15 | **InnoLogIST 2009** | Every 3 years | https://sabreconference.wifa.uni-leipzig.de/frontend/sabre2009/media/inno/innoLogIST2009.pdf |
| 16 | **Seminar: Logistikmanagement - RFID-Anwendungen** | Every 3 years | Seminar: Logistikmanagement - RFID-Anwendungen |
| 17 | **International Conference on Dynamics in Logistic** | Every 3 years | http://www.logdynamics.com/ldic.html |
| 18 | **GSC Security Summit** | yearly | http://www.globalsecuritychallenge.com/gsc_conferences.php |

**Table C.02 – Selected Conferences for dissemination**