Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D8.5: Preliminary Exploitation Plan

Due date of deliverable: M24 –2013.08.31

Actual submission date: M24 – 2013.08.25

Start date of project: 01/09/2011 Duration: 36 months

Organisation name of lead contractor for this deliverable:

Indra Software Labs, INDRA

Revision *Final*

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2012)		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	X
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Authors and Approvals			
Authors		**Date**	**Signature**
Name	**Company**		
Ester Artieda	INDRA		
Lorena de Celis	AT		
Cecilia Coveri	SES		
Reviewed by			
Name	**Company**		
Approved by			
Name	**Company**		

Applicable Documents		
ID	**Document**	**Description**
AD-01	TA	nSHIELD Technical Annex
AD-02	D8.2	Dissemination Plan
AD-03	D8.3	Standardization Plan

Modification History		
Issue	**Date**	**Description**
Issue 1	16.08.2013	Initial version
Issue 2	17.08.2013	AT comments
Issue 3	19.08.2013	Some modifications according to the comments
Final	25.08.2013	Final review

Executive Summary

The document shows the preliminary exploitation plan which will follow after the end of nSHIELD project.

The aim of this deliverable is to identify and analyse the market reality within which the nSHIELD project could operate, identify the market through potentialities and competition, take into account the costs and risks it could face and finally to organize a marketing and promotion plan.

Contents

Figures

Tables

Glossary

Please refer to the Glossary document, which is common for all the deliverables in nSHIELD.

This Page is intentionally left blank

1 Introduction

The nSHIELD project proposes an innovative layered architecture to provide Security, Privacy and Dependability (SPD) features and functionalities to modern Embedded Systems. This is achieved by enriching these systems with innovative functionalities, among which the most important is the "composability", i.e. the possibility of dynamically enable/disable/configure system's components in order to achieve a desired end-to-end behaviour.

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, such as nSHIELD project. Therefore, such activities have been considered as integral part of the project both in terms of industrial research and experimental development.

The content of this Deliverable D8.5 "Preliminary Exploitation Plan" reflects the work and progress done in Task T8.3, and focuses on the exploitation activities so far. The target of Task 8.3 is to promote and facilitate the exploitation of the achieved results during the nSHIELD project development. At the end of the project, 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.

The exploitation is expected to orientate to different 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 are being developed in nSHIELD. Another one will be the exploitation strategies that have been devised for the projects results that are submitted for standardization.

Issues of intellectual property and exploitation rights (including patents) have also been considered in this task, including potential synergies among the project partners.

To support the exploitation of the project results, two workshops were scheduled to interested final users, industrial partners and other colleague institutions from the scientific community, in order to present the achievements of the project, thus demonstrating the validity of the ideas. The first workshop will be organized in autumn 2013 and will be focused on measurable security for sensor systems while the second workshop will take place at the end of the project (month 36). During these events, demonstration of nSHIELD abilities and technical lectures will be offered.

In addition to these workshops, nSHIELD partners have participated in more than 10 seminars, presentations and exhibitions where we can highlight "arcHItecturE for multi-Layer Dependable solutions (nSHIELD)", or the Measurable Security- a discussion of potential approaches on the FFI Seminar on Advances in ICT.

Exploitation activities are closely related to Tasks T8.1 (Dissemination) and T8.2 (Standardization), which set the necessary background to develop successful exploitation actions.

With these activities nSHIELD intends to show to potential customers its advantages over their own solutions providing Security, Privacy and Dependability (SPD) features and functionalities to modern Embedded Systems decreasing costs (time and money) using a new framework with a wide range of support, doing easier compatibility with other companies which will use nSHIELD and reducing development time due to the layer.

Finally, during the last phase of the project, partners are going to analyse how to support nSHIELD after the end of the investigation project, and one alternative could be to dedicate a part of the incomes nSHIELD will generate to finance its future development.

2 Objectives

The target of nSHIELD project is to develop a technology-independent, intrinsically secure and dependable architectural framework, which allows seamless exploitation of Security, Privacy and Dependability (SPD) resources in heterogeneous domains:

- Industrial systems (e.g. manufacturing plants)
- Nomadic environments (e.g. mass gathering events)
- Private spaces (e.g. home)
- Public infrastructures (e.g. railway stations)

Four scenarios, with their corresponding demonstrators, have been carefully selected in an industry exploitation perspective, in order to cover a wide and significant view of the foreseen industrial needs:

1. Dependable surveillance systems for urban railways security
2. Dependable system for voice/facial recognition
3. Dependable avionic system
4. 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 main objective of this Preliminary Exploitation Plan is to make a first approach on the methodologies and activities to be designed and performed during the life of the project and once its development is finished, in order to make a successful product of it. Other secondary objectives are:

- To obtain a market preliminary analysis, so that potential clients can be identified and their needs met.
- To know how the nSHIELD project contributes to both the general ARTEMIS targets and industrial competitiveness and sustainability.
- To make an approach to the individual exploitation plans of the partners involved in the project, both industrial and academic ones.
- To perform an introductory risk analysis.
- To manage the patents they may arise during the project development.
- To manage the intellectual property of the results achieved in the nSHIELD project.

A complete Final Exploitation Plan (D8.10) will be delivered at the end of the project (M36), detailing in depth all the contents outlined in this document.

3 Market Analysis

3.1 Current market needs

The **current technological situation finds a market with different** Embedded Systems solutions (ES) in the area of Security, Privacy and Dependability (SPD) which are ad-hoc designed, thus implemented and deployed for each specific system, causing sub-optimized performances, incompatibility and higher costs. Meanwhile, the growing number and quality of treats are emphasizing new challenges pursuing secure, dependable ES that will be operative in increasingly complex scenarios in the future.

The lack in well-defined SPD metrics constitutes, furthermore, a big obstacle for a fast validation and certification of the proposed technical solutions.

To face 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.

The nSHIELD project aims to **drastically improve SPD quality of ES** while addressing the above mentioned industrial requirements, by proposing to design and develop embedded SPD via standardized design methods mainly based on:

- *frameworks of composable technologies* to be settled on the specific industrial solution;
- a *set of new SPD metrics* allowing fast, standard validations and certification;
- *methods and mechanisms to easily design and keep SPD level compliant for all the system's lifetime*.

Due to heterogeneity and wideness of the overall embedded systems market, it 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 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.

3.2 General Market Impact

To obtain the valuable goals of nSHIELD, the project will completely fit in ARTEMISIA Subprogram Six as well as in the overall ARTEMISIA Target.

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

The nSHIELD project will contribute to reach the target of the Sub programme 6. Following it is presented how nSHIELD will effectively contribute to reach the main impacts expected by such work programme (as indicated in the official Annual Work Programme 2009):

Table 3-1: Contributions of nSHIELD to reach the target of ARTEMISIA Sub-programme 6

ARTEMISIA SP6 targets	nSHIELD contribution
Enhancing security, privacy and dependability to increase people's confidence in applications, systems, devices and infrastructures	In actual embedded systems, SPD solutions are extremely tailored on the specific system features. The European Commission (EC) has been addressing the problems of SPD already for IST in the FP6[1] but its efforts haven't arrived in ES's yet. That's why ARTEMIS specifically addresses the topic and why nSHIELD is so necessary. Moreover, the growing number of breaches in information security[2] [3] [4] [5], is provoking continuous challenges for secure electronic systems, aggravated by the augmented complexity of future ES's. The impossibility to use well defined metrics and standardized parameters for SPD does not allow a quick and reliable evaluation of the effectiveness of the ad-hoc solution, nor a precise rating of alternative solutions to the same SPD problem. nSHIELD aims to enhance SPD, thus increasing people's confidence in applications, systems, devices and infrastructures that were considered vulnerable or untrustworthy in the past. 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 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 ES's is expected to produce new secure architectures for the use of TPM. The weakness of SPD in the perception from citizens, currently avoid the possibility to use advanced technological systems in applications strongly sensible to privacy issues. Security and dependability are fundamental, not just a strategic advantage, but an enabler of the application. The level of ubiquity, the pervasiveness, and the fusion with the environment, with personal space and every-day life, expose pervasive systems to several SPD issues that strongly require future systems to be intrinsically secure. nSHIELD will study these issues and will define suitable solutions to satisfy these SPD requirements 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 SP6, could not be achieved without addressing SPD – like nSHIELD intends – with an holistic approach covering systems and their lifecycle process (design, development, testing, deployment, maintenance) together. Moreover if we want to increase confidence, we will have to connect this with a strong dissemination strategy as detailed in deliverables D8.2 and D8.9.

[1] See ftp://ftp.cordis.europa.eu/pub/ist/docs/istag_kk4402464encfull.pdf
[2] Oyster card crack - http://www.v3.co.uk/vnunet/news/2219828/london-oyster-cracked, the original presentations at http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html, while a more scientific: http://eprint.iacr.org/2008/166
[3] Keeloq crack - http://www.wired.com/threatlevel/2007/08/researchers-cra/ or http://hackedgadgets.com/2007/09/08/keeloq-remote-vehicle-entry-system-cracked/
[4] Dutch passport readout - http://www.rfid-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
[5] iPhone SMS bug - http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html

Enabling industrial actors and service providers to offer new features or services with minimal additional cost to the customer	nSHIELD will provide industrial actors with a reference framework for developing "SPD compliant" applications in the Embedded Systems, 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. 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. More secure and dependable products will be offered in the final market at a minimal additional cost. An example is Selex. Taking advantage from nSHIELD framework, their TETRA[6] technology could improve its intrinsic security with a modular and compliant development strategy where integration and interoperability with other nSHIELD technologies will be addressed. Such an approach will allow nSHIELD-oriented TETRA to broaden market perspectives and applications towards innovative, secure, dependable and privacy oriented transmission / communication modules.
Definition of a common conceptual framework to meet requirements for SPD, with particular focus on compositional design & development. Research should consider the interplay between properties such as maintainability, security, reliability, safety, availability and survivability. It should work with certification and qualification authorities to establish new approaches to certification and qualification required to accommodate the new technology.	nSHIELD researches will concentrate mainly in achieving a common framework for SPD accounting new composability mechanisms. In this respect nSHIELD fully address these topics in WP2 (Tasks 2.1 and 2.3) where its requirements, specification and design are delivered. The Liaison Task foreseen in WP1 will take in account the development in other ARTEMISIA and FP7 areas relevant to safety, seamless connectivity and sustainability of future ES's, while the methods and tools developed in nSHIELD for supporting all the lifecycle quality of SPD take into 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 ES products to be based on platforms that can be evolvable throughout their whole lifecycle. nSHIELD 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, 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 XMLSecurity) and (2) the standards of TCG – Trusted Computing Group. Additionally the valuable nSHIELD results will be presented to the most

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

	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;
Instantiation of this framework with components, methods, architectures, interfaces and communications, tools and tool chains, to enable the design, development, analysis, validation and deployment, as well as certification (or qualification).	nSHIELD performs an instantiation of the framework with components, methods, algorithms, procedures and interfaces in the following tasks: • 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).
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 the SPD lifecycle tools developed by Task 6.3.

3.2.2 Contribution to the general ARTEMIS targets

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

Table 3-2: Contributions of nSHIELD to reach the ARTEMIS general targets

ARTEMIS Target	nSHIELD contribution
ARTEMIS Target #1: Reduce the system design cost from 2005 levels by 15% by 2013	All 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 a tool-set for creating application code, capable to build SPD into ES's. The possible application of the new nSHIELD based architecture in ES's 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: implementing them using nSHIELD framework will 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 will reduce 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 goals. A valuable part of the development for SPD compliant ES is constituted by certification costs, time and complexity. Compliance of such development aspects will contribute to this ARTEMIS target.
ARTEMIS Target #3: manage a complexity increase of 25% with 10% effort reduction by 2013	The future ES will be requested to work in higher complex configurations, 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 this to happen in an easier way for the designer, by providing SPD features in all those scenarios. A key role to obtain these results will be performed by the composability of SPD technologies, via the logical composability-mechanisms, to behave in a different way in static and 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 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 ES 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 ES's 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. These early validation techniques adapted to SPD will also contribute to increase quality of final products and decrease time-to-market and costs. nSHIELD is aimed at 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 nSHIELD automated tools will produce the necessary evidence for these claims. In this respect nSHIELD focuses on the biggest problem in ES development: the elimination of programming bugs and vulnerabilities, 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, etc.)	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 takes 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.

3.2.3 Contribution to industrial competitiveness and sustainability: 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 products and 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[7] [8] [9] [10], the nSHIELD consortium has identified three impacts-

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

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

parameters (grade of reusability, development cost reduction and time-to-market reduction) and promoted an internal survey to foreseen how they will be influenced by the projects result. The survey assessment could be presented in synthesis as follows: considering the advantages in design process originated by the reusing of the common functionalities among ES parts and taking in account similar experiences in software engineering[9][10], 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 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:

[9] "*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

[10] 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

3.3 Specific Market Impacts

The embedded systems market is mainly characterized by the great technology fragmentation. Each manufacturer develops its own security systems, and metrics depend on the work area and the place where the product is sold.

nSHIELD project aims to drastically improve SPD quality of ES proposing to design and develop embedded SPD via standardized design methods mainly based on:

- *frameworks of composable technologies* to be settled on the specific industrial solution;
- a *set of new SPD metrics* allowing fast, standard validations and certification;
- *methods and mechanisms to easily design and keep SPD level compliant for all the system's lifetime*.

With these perspectives, the market will reduce fragmentation, and companies will improve their competitiveness reducing design and development times and having common metrics which could compare competitor's security levels.

In the following lines it will be analysed the impact on the specific partner's markets.

3.3.1 Contributing to the partners specific competitiveness

The specific exploitation plan of partners is presented in section 5. 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:

3.3.1.1 Railway market impact - reduction of costs

As mentioned in the individual industrial 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.

3.3.1.2 Dependable Avionic Systems market impact

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

The implementation of the nSHIELD concepts, in the avionic computers based on IMA platform, allows a cost reduction in development, due to the shared activities. A primary goal of IMA is to establish the application of a "standard" set of hardware modules, directly line-replaceable, encompassing as much of the total avionics suite as possible. Emphasis is also placed on the development of key sensors and on processing technologies (both HW and SW) capable to support a fully integrated open architecture sensor/processing package.

While a preliminary set of requirements have been already provided and documented, the complete definition of the functional requirements is still in progress; in particular it will vary depending on the safety level of the platform. Related investment in all the LoBs (Line of Business) in Selex ES 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.

3.3.1.3 Social Mobility market impact

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.

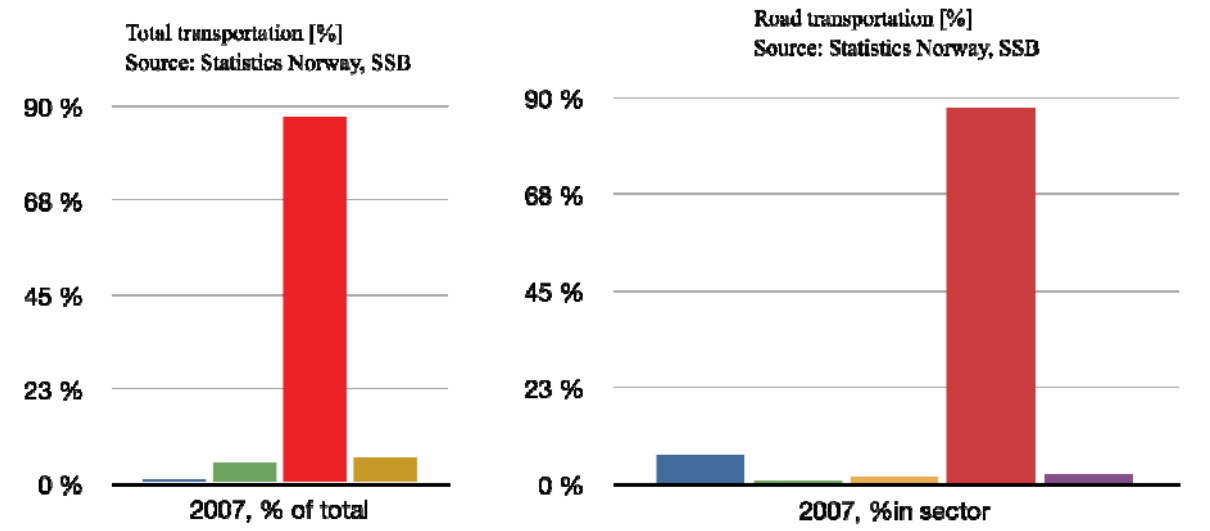

Figure 3-1: Transport distribution in Norway

The technological advancement in transport sector (e.g. smart vehicle) may account for up to 27% reduction of transportation cost[113]. 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 Euros 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.

Table 3-3: Estimation of the cost reduction in the transport sector in Norway

	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 MNOK (1km=3 NOK)		131,134	35,406	10,491	45,897
Costs MEuro (1€=8,1 NOK)		16,189	4,371	1,295	5,666

3.3.2 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, which are represented in large part within the nSHIELD consortium, 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, defence, 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 defence 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.).

3.4 Market Example Scenarios

3.4.1 Example 1 –The Railways Security Scenario

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

The growth in 2006 and 2007 has been very high. The world market volume has increased by approximately 19 billion EUR. This means 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, which 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.

3.4.2 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% [5]. 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 [6].

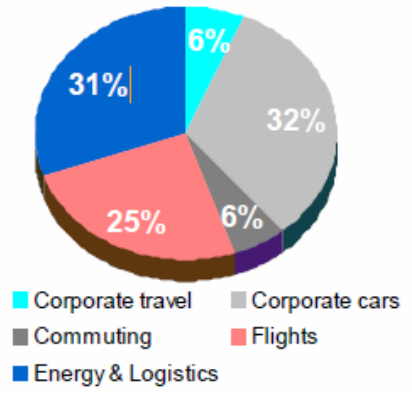

Figure 3-2: SAP carbon dioxide footprint, segment usage [5]

We believe that another 8% of CO2 can be reduced through a change of attitude and behaviour of people, thus 'social mobility' due to 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 CO2 neutral will adopt the nSHIELD results. With more than 20% of public employees the city has plans to substantially reduce the travel-related CO2 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 [7]. 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 [8]. 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.

3.5 Geographical scope of Exploitation Plan

Logically, given the geographical location of the companies participating in the nSHIELD project, the original operating area will be at European level, taking into account that direct contact with some of the potential customers has been already made.

However, it would be possible to adapt the application to other areas, and thus extend the potential market of nSHIELD. This would need a deep analysis of the ES application target and characteristics. It would also be necessary to operate the product outside Europe, making a previous survey to identify potential customers in each country, again in close relation with Dissemination and Standardization activities.

3.6 Potential customers

As already stated, successful Dissemination and Standardization tasks will take nSHIELD to a leading role for proving modern ES with SPD. Therefore, all the providers and final users of this kind of systems

are potential users of the nSHIELD final product, and not only in the European market. Above all, if the result standards will be mandatory for the development of SPD in modern Embedded Systems.

The exploitation is expected to be mainly in **many business segments in the industrial sector**, 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 are being developed in nSHIELD. On the other hand, it will be also important to start with the standardization process to disseminate our results and be an important influence to the market. And we have to note that although the exploitation will be independent of the standardization, it will help nSHIELD to be known.

Other potential customers who would make a profit of nSHIELD project would be:

- Public infrastructures (e.g. railway stations)
- Nomadic environments (e.g. mass gathering events)
- Private spaces (e.g. home)

At the end of the project, the partners and, in particular, the large industrial companies, will elaborate definitive business plans to evaluate and explore the impact of the results on their business scenarios. These plans should be continuously updated, in order to adapt them to the evolution of the project and the changes in the relevant markets.

Every partner plays a leading role in the identification of potential customers, since each of them has a particular area of work / study. And therefore, each of them can easily identify target customers in their scope. That's the reason why the collection of individual exploitation partners, is more relevant for the project than the production of a general, maybe superficial, general exploitation plan.

3.7 Competitors

As far as our enquiries have enabled us to know, there are some companies focused on embedded security systems like Green Hills or Wind River, and others like Airbus which give their own solutions to their products, but which have different objectives than nSHIELD project. Also, we did find some smaller projects, focused on particular scopes and areas of application, and, mainly, some competitions and challenges mainly targeted on Research & Development tasks in the Academia scope.

3.7.1 Wind River

Wind River [9] offers the industry's most comprehensive device development portfolio, backed by award-winning customer support. They offer complete vertical platforms built on a real-time operating system and commercial open source solutions. One of them focuses on ad-hoc Security in Embedded Systems products (thus not seeking standardization), with application in areas such as Aerospace and Defence, Industrial, Medical, Networking, Automotive and Mobile Devices.

3.7.2 Green Hills

Green Hills is one of the largest independent vendors of embedded software solutions. The company offers embedded development solutions support to a wide range of hardware and software platforms and in 2008, one of its products, INTEGRITY-178B RTOS was the first and only operating system to be certified by the NSA to EAL6+ High Robustness, the highest level of security ever achieved for any software product.

In addition, Green Hills have a complete development solution for embedded systems with its integrity program (INTEGRITY), operative system (µ-velOSity), different protocol stacks (IPv6, TCP/IP) and integrated development tools.

3.7.3 CSAW - CyberSecurity Competition

The 2012 Challenge of this competition [10], focused on how to provide security and trustworthiness of hardware platforms.

Teams are invited to participate in this challenge and attack a target hardware platform. They will discover vulnerabilities in the target platform and exploit them by using their hardware design skills. Such attacks lead to a better understanding of the vulnerabilities in hardware platforms and thereby enable designers to build trustworthy hardware that can thwart such attacks. Participants mainly include Institutes of Technology (such as Kharagpur IT or ESISAR from Grenoble) and Universities (Iowa State, San Diego, Massachusetts, etc.). Therefore, this competition is clearly targeted on Academia, and not on direct industrial activities.

The 2013 Challenge [11] has similar aims, though has not started yet.

3.7.4 Intel Embedded Systems Competition 2013

Organized by the “III Simpósio Brasileiro de Engenharia de Sistemas Computacionais” (SBESC), this competition is open only to undergraduate and graduate students, as an academic challenge. In principle, it has no industrial or commercial applications.

3.8 Conclusions

After analysing all the information, we can conclude there are a wide range of potential customers due to the fact embedded system market is growing every year and nSHIELD offers a drastically improvement of SPD quality, a development cost reduction and a serial of methods and mechanisms to easily design and keep SPD level compliant for all the system’s lifecycle.

Successful tests on the different project scenarios will provide the best marketing strategy to promote nSHIELD, and the dissemination plan will be one of the main steps to make the project known to the potential customers.

We also have to take into account competitors and the standardization processes to adapt nSHIELD as much as possible to the market and be in touch with customers to analyse their needs.

To sum up, the success of nSHIELD is to provide a big quality to SPD technology for embedded systems according to the ARTEMIS targets and disseminate it among the potential customers to increase their efficiency when they implement their projects, always without forgetting the competitors.

4 Dissemination & Standardization: Brief Summary

nSHIELD partners have a strong interest in disseminating and exploiting the project results. For this reason they have planned effective and realistic industrial and academic dissemination, standardization and exploitation plans.

The scope of this deliverable focuses on the Exploitation of the project. Anyway, we will give a brief glimpse of the dissemination and standardization tasks, since they are closely related to the exploitation itself because are tools to inform potential customers about nSHIELD goods and meetings, seminars and workshops are useful to start a commercial relationship with companies interested on SPD technology.

4.1 Dissemination Tasks

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:

- Publication of all important results in well-known conferences and journals
- Promotion of nSHIELD through the organization of special sessions in conferences and workshops on the research topics of the project
- Producing scientific publications
- Organizing and participating to dissemination events (international conferences and workshops)
- Organizing an international journal special issue on the main research nSHIELD topics.

More details of these dissemination activities can be found in AD-02, **Deliverable D8.2** “Dissemination Plan”, which will be enlarged in a final version in **Deliverable D8.9**.

4.2 Standardization Tasks

On the other hand, standardization tasks are a key component to increase the impact in the SPD sector. The main activities for reaching the standardization objectives are:

- Close interaction with standardization groups to monitor on-going activities
- Preparation of documents and proposals for standardization group
- Production of 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.

More details of these dissemination activities can be found in AD-03, **Deliverable D8.3** “Standardization Plan”, which will be enlarged in a final version in **Deliverable D8.8**.

5 Exploitation of nSHIELD

This project will give opportunity to industries and SMEs to acquire know-how and the possibility to exploit results introducing *new commercial products* and identifying new possible application scenarios of SPD technologies, and also to contribute to regulatory bodies with *effective services and a solvent technology architecture* proposal.

5.1 General Objectives

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

Following sections describe, at partner level, the exploitation plan, both for academia and industries.

5.2 Individual industrial exploitation plans

5.2.1 SELEX ES

The results of the nSHIELD project will be used to enhance the Selex ES innovation activities with the purpose of developing prototypes and products and enabling the enhanced of the avionic family computer to be proposed on national and international markets. Furthermore Selex ES 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.

On its communications area, Selex ES 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 ES further research activities.

5.2.2 Ansaldo STS

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.

5.2.3 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.

5.2.4 European Software Institute

ESI will use the knowledge and results generated in nSHIELD to mature their technologies and generate avant-garde service packages and training courses, especially centred on TPM-based solutions, the SPD Metric-based solutions, and Secure Embedded and Services Management-based solutions. For this purpose, ESI 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, ESI 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. ESI will make use of its normal commercial channels to exploit nSHIELD project results. That is, mainly "ESI Consultancy Services Dpt.", ESI@net (A commercial Network) and ESI@centers (A Network of Excellence Centers). In addition, the commercial force at ESI, integrated by 4-5 commercials, will support project results exploitation.

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

ESICenter is the Network of Centers for Software Engineering Excellence that comprises a series of technology centers that are similar to ESI in their goals, objectives, activities and legal status; each centre is directed towards supporting the software industry in a certain region. The ESICenter network

complements ESI's existing technological capabilities, and enables us to launch initiatives at a global level.

Expected Impact: ESI 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 3 M euros per year. Among these companies around the 60% are small organizations, therefore ESI estimates that the results of nSHIELD will be made available to over 25 SMEs per year as well as to the 52 partners of ESI@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 ESI dissemination and exploitation (in cumulative numbers):

Table 5-1: Expected impact of nSHIELD results (ESI)

ESI - 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
SME's using nSHIELD results	10	40	60
Expected economical income for ESI 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 ESI due to nSHIELD	2	5	8

5.2.5 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 worldwide.

nSHIELD project represents an opportunity to increase Eurotech Group presence in pervasive, wearable and nano computer 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 centre 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.

5.2.6 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 SHIELD in the areas of ad-hoc networks, sensor networks, and services over dynamic networks, systems integration and lifecycle support.

5.2.7 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.

5.2.8 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.

5.2.9 MOVATION AS

It is a Norwegian platform for open innovation. Movation will exploit the results of nSHIELD 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 nSHIELD 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-border 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 nSHIELD results will contribute to these discussions.

During the last two years Movation has been involved in about 70 companies with evaluation, advice 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 nSHIELD Movation will extract relevant technological advancements and outcomes of nSHIELD, and will bring it into one of these companies.

5.2.10 NOOM AS

They provide communication interfaces to services. The results of nSHIELD will contribute to enhancing NOOM's capabilities by enabling the communication to Internet of Things. Thereby NOOM can expand its product portfolios.

5.2.11 SESM

They 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.

5.2.12 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.

5.2.13 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.

5.2.14 THYIA

THYIA is aiming to explore embedded technology and SPD approach that are key technologies for nSHIELD scenarios.

Exploring new SPD technologies for such complex system infrastructure is a primary aim of THYIA in this project. The focus will be in demonstrating networked SPD nodes as SPD sensor networks used for different nSHIELD application scenarios.

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

5.2.15 Alfatroll

Alfatroll will be able to demonstrate a dependable avionics system, envisaged through the agreed scenario. It is the hope of the company that more participants in the nSHIELD project considers evaluating Alfatroll's technology for their other avionics systems.

Referring to the cancelling of the prestigious EuroHawk project due to this reason: "On 14 May, the German Ministry of Defence announced it would be withdrawing from the planned purchased of the Euro Hawk unmanned aerial vehicles. The reasons given for this were the difficulties and high costs of introducing the system to general air traffic in Germany and Europe. Germany abandoning one of its largest armament programmes has turned into an unprecedented scandal over the procurement of armament and military equipment in Germany. This concerns both the costs incurred (between 600 and 800 million euros) and the manner in which the programme was being run by the Ministry of Defence."

Alfatroll intends to demonstrate how even extremely advanced systems can be implemented with simple and efficient on-board avionics systems, given that Alfatroll's Knowledge Based System is used. The company will approach the aerospace community with this message and a working prototype.

5.2.16 SknFnd

Seek and Find 'sknfnd' will demonstrate and develop several working prototype, including user friendly control and monitoring system and end-user equipment and other embedded system. Here embedded Internet of things based on GSM, GPS and sensor technology can example provided alarm and notification before an accident happens, or if the transport system is in a critical situation. The nSHIELD login will be here for the demo, prototype and future development: http://67.223.97.18:8080/

5.3 Individual academic exploitation plans

5.3.1 ATHENA/Industrial Systems Institute

ATHENA 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).

5.3.2 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.

5.3.3 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.

5.3.4 Telecommunication System Institute

The TSI will exploit the results in numerous ways. Firstly it will publish them in the relevant conferences and journals. Secondly, TSI 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 TSI. Moreover, the specific topics of nSHIELD 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, TSI 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 TSI 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 TSI already takes up, for National and European Large Companies and SMEs.

5.3.5 Università di Genova

They 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.

5.3.6 Università di Roma

They will intend 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.

6 Cost & Risk Analysis

6.1 Cost Analysis

The following table shows the budget needed to carry out nSHIELD project and the effort each company is going to do along the whole life of the project.

Table 6-1: nSHIELD budget

Participant no.	Part. short name	Total person months	Total Eligible Costs	Maximum National Contribution	Maximum JU contribution
1(C)	MAS	15	187,892.00 €	62,122.00 €	31,378.00 €
2	ASTS	49	431,045.00 €	133,231.24 €	71,984.52 €
3	AT	64	386,903.00 €	128,838.70 €	64,612.80 €
4	ATHENA	66	459,600.00 €	459,599.20 €	0 €
5	SELEX Elsag	77.5	772,537.00 €	224,447.00 €	129,014.00 €
6	TECNALIA	88	565,818.00 €	188,417.40 €	94,491.61 €
7	ALFA	15	172,956.00 €	57,420.00 €	28,884.00 €
8	ETH	50	300,000.00 €	92,400.00 €	50,100.00 €
9	HAI	144	1,113,600.00 €	556,799.20 €	0 €
10	INDRA	100	686,578.00 €	159,972.00 €	114,658.53 €
11	ISD	72	553,000.00 €	276,500.00 €	0 €
12	SG	52.6	672,497.00 €	189,188.00 €	112,307.00 €
13	MGEP	45	281,000.00 €	93,573.00 €	46,927.00 €
14	NOOM	1	4,200.00 €	1,396.00 €	701.00 €
15	S-LAB	108	621,500.00 €	393,410.00 €	103,790.50 €
16	SESM	31	260,400.00 €	86,713.00 €	43,486.80 €
17	SICS	26	286,130.00 €	165,955.00 €	47,783.71 €
18	T2D	36	379,440.00 €	60,710.00 €	63,366.48 €
19	TELC	9	94,860.00 €	15,177.00 €	15,841.62 €
20	THYIA	38	397,884.00 €	231,966.37 €	66,446.63 €
21	TUC	97	453,600.00 €	453,599.20 €	0 €
22	UNIGE	60	467,706.00 €	155,868.00 €	78,106.90 €
23	UNIUD	36	351,981.00 €	117,209.67 €	58,780.83 €
24	UNIROMA1	48	480,000.00 €	159,840.00 €	80,160.00 €
25	SES	215.9	2,386,242.00 €	416,636.00 €	241,321.00 €
26	SknFnd	5.5	62,500.00 €	20,625.00 €	10,437.50 €
	Total	**1550**	**12,853,156.00 €**	**6,879,161.63 €**	**1,715,650.45 €**

As we can see the total eligible cost are over 13 million, an important budget to improve SPD technologies on ES.

The exploitation plan has been put in place since the completion of the development work, and from now we will focus our efforts on disseminate the project and in getting customers for nSHIELD to make it viable after the end of the research time.

6.2 Risk Analysis

The exploitation of nSHIELD results is exposed to several risks that might cause unexpected situations and even some problems when facing the exploitation. This phase has its own intrinsic risks, but may be affected by more general risks.

6.2.1 Agreement and Financial risks

nSHIELD exploitation can be affected by some "general" risks, most of them are common to any other projects of different nature.

Table 6-2 – Risks for the nSHIELD exploitation: common risks

Description	Probability	Gravity	Contingency Plan
Agreement risks			
Consortium partners cannot agree because of different interests	LOW Partners are ES manufacturers, integrators and their suppliers, who have common targets and objectives	MEDIUM	In case one of the partners didn't want to continue with the exploitation of nSHIELD results, the wide range of partners would allow any of them to take their role.
Financial risks			
Some of the partners cannot afford the implementation of the exploitation plan	LOW Exploitation doesn't imply a high cost to the partners, especially when they've been able to afford the other phases	HIGH	Many of the partners have a financial capacity, high enough to overtake the share of the leaving partner

6.2.2 Market and User-related risks

Table 6-3 –Risks for the nSHIELD exploitation: market and user-related risks

Description	Probability	Gravity	Contingency Plan
Agreement risks			
Consortium partners cannot agree because of different interests	**LOW** The partners are ES manufacturers, integrators and their suppliers, who have common targets and objectives	**MEDIUM**	In case one of the partners didn't want to continue with the exploitation of nSHIELD results, the wide range of partners would allow any of them to take their role.
Financial risks			
Some of the partners cannot afford the implementation of the exploitation plan	**LOW** Exploitation doesn't imply a high cost to the partners, especially when they've been able to afford the other phases	**HIGH**	Many of the partners have a financial capacity, high enough to overtake the share of the leaving partner
Market environment			
The market environment or the user is subject to change and makes the results obsolete			
No customers			
No major customers for using the results are found (during the Dissemination Phase)			
Competition risks			

A competing solution comes up and makes the results less valuable	**LOW** The key players in this market are ES manufacturers, integrators and suppliers, of which several major ones are in the consortium. They are aware of on-going work on small-scale single-technology, especially from 2001. And they have no knowledge of a similar activity to nSHIELD	**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	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.
Standardization risks			
Standards emerge that prevent the deployment of the results, or lead towards a different solution to that being developed in the project	**LOW** The key players in standardization groups are present in the nSHIELD consortium. They are aware of the work in relevant standards organizations.	**HIGH** If standards did emerge they could prevent the deployment of the results or led towards a different solution	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.

7 Patents and Intellectual Property

7.1 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.

7.2 Contribution to standards and regulations

As we have said on the Standardization Tasks paragraph, the main objectives of the project on this area are:

- Close interaction with standardization groups to monitor ongoing activities
- Preparation of documents and proposals for standardization group
- Production of guidelines, quality test procedures and certification rules to cover open needs of end-users.

But to delve deeper into this point we can find more information in Deliverable D8.3 "Preliminary Standardization Plan" where are described all the actions partners are going to take part regarding regulations and standards.

7.3 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, and 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 uses 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:

7.3.1 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.

7.3.2 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.

7.3.3 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 favourable 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 knowhow, 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 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.

Table 7-1: The provisions relating to Access Rights

<table>
<tr><th></th><th>Access rights to pre-existing know-how</th><th>Access rights to knowledge resulting from the projects</th></tr>
<tr><td rowspan="2">For carrying out the project</td><td colspan="2">Yes, if a participant needs them for carrying out his own work under the project</td></tr>
<tr><td>Royalty-free unless otherwise agreed before signing the contract</td><td>Royalty-free</td></tr>
<tr><td rowspan="3">For use purposes (exploitation + further research)</td><td colspan="2">Yes, if a participant needs them for using his own knowledge</td></tr>
<tr><td>On non-discriminatory and reasonable conditions to be agreed</td><td>Royalty-free unless otherwise agreed before signing the contract</td></tr>
<tr><td colspan="2">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)</td></tr>
</table>

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.

8 Promotion and marketing

During the project development phase of nSHIELD, will be launched several actions to facilitate the dissemination and commercialization of its results.

The diffusion will be carried out by holding two workshops that allow potential customers to see features and improvements nSHIELD provides over its competitors and the partners will also participate on seminars, exhibitions, presentations and other dissemination activities.

In addition each industrial partner will use their commercial departments to promote nSHIELD among their customers.

8.1 Detecting potential customers and touchdown

The market research phase and the initial contact will be done in several ways:

The first is through the celebration of the workshops mentioned above, where you can display the results of the project and convince the audience that it is a good way to make improvements to their products related to SPD technologies.

The second way will be through the partners of the project members. Here the communication will be easier to establish and each member will know the needs and problems of their business partners where nSHIELD can help.

And finally, we may explore the market on a pyramidal way, looking first on the main embedded system markets like transport, health, security and sending invitations to the main companies to attend to workshops or seminars where nSHIELD will be presented.

8.2 Dissemination tasks

All project participants will work on these tasks, including:

- Press releases, articles, reports, etc. in mainstream media.
- Participation in forums, seminars, exhibitions and other events related to the sector, such as SPD technologies on embedded systems.
- Product Presentations.
- Websites.

Regarding this last task, is now available nSHIELD project website, from which you can access all information related to the project.

During these months several dissemination activities have been carried out:

Table 8-1: Dissemination activities

Activity	Title
Journal papers	“Interoperability of Security-Enabled Internet of Things”
Conferences	Securing DMA through virtualization
	The SHIELD framework: How to control Security, Privacy and Dependability in complex systems

	Reputation-based Intrusion Detection System for wireless sensor networks
	Distributed cognitive radio architecture with automatic frequency switching
	Secure policy-based management solutions in heterogeneous embedded systems networks
	Building Trust in Ad hoc Distributed Resource-sharing Networks Using Reputation-based Systems.
	An Overview of Security Issues in Embedded Systems Based on EU-Funded Research Projects.
Workshops, exhibitions and presentations	"Measurable Security for the Internet of Things", Semantic Days 2013
	Measurable Security for the Internet of Things, 7. Strategic Workshop
	Measurable Security – a discussion of potential approaches, Josef Noll at FFI Seminar on Advances in ICT
	"Measurable Security in Mobile Networks", IDC Enterprise Mobility Series
	Security, Privacy and Dependability in Mobile Systems at the Second International Conference on Mobile Services, Resources, and Users,
	Researchers Night pSHIELD motorbike demonstration
	arcHItecturE for multi-Layer Dependable solutions (nSHIELD)
	Internet of Things – Finding its Way to Industry
	Secure Interoperability – The Challenge for the Internet of Things
	Internet of Things – Internet of the Future
Industrial dissemination	Press release at Indra web site
	UAS Nordic Conference 2012 organization with high profile representatives from European UAV business
	ITEA2/Artemis Co-Summit 2012 assistance
	Internet of Things Value Creation Network in Norway
	Meetings with ZIV, Ikusi, Metro Bilbao
	Standard Norway has invited Movation and CWIN to become more active in standardisation
	ABB has two groups with research interests related to SHIELD issues
Organization of special sessions	2nd IEEE Workshop on Complexity in Engineering (COMPENG 2012)
	XII Spanish Meeting on Cryptology and Information Security (RECSI 2012)

In addition to these tasks, on the Deliverable DL8.2 “Preliminary Dissemination Plan” we can find a deeper description about nSHIELD dissemination.

8.3 Marketing

The marketing process is actually a natural extension of the previous phases, and they include it.

It is important to continue with the commercial work after the customer purchases the product, and ensure good post-sales service. This will keep customer satisfaction and willingness to acquire new products or updates. In short, it’s important to maintain their loyalty.

1. Identifying potential customers.
2. Hunt customers, thanks to the promotion and dissemination.
3. Initial contact.
4. Prototype demonstrations.
5. Taking requirements and needs of the client, if applicable.
6. Business Action: submission of offers, etc.
7. Training on the product, if applicable.
8. Post-sales service and technical support.

9 Business plan

As we have said previously, only after a deep analysis of the nSHIELD different scenarios' results, a more detailed and rigorous business plan could be done.

The Business Plan purpose is to present the main dissemination and exploitation strategy to bring out nSHIELD. To do that, we will base on market analysis performed, as well as in the promotion and marketing plans outlined above, and most important, in the validation of pilot results.

In the absence of greater detail until the project will be finished, the business model is marked by paragraphs set forth herein and in other nSHIELD deliverables, and that respond to the key issues that should be considered in a model with these features:

Figure 9-1: Business plan

10 Conclusions

Throughout this deliverable has:

- Defined the nSHIELD Exploitation Plan objectives.
- Identified the potential markets and customers.
- Identified the potential competitors with similar products on the market.
- Analyzed the risks and cost of the project.
- Planned marketing and sales activities
- Defined dissemination task
- Designed a preliminary business case which could be modified depending on the development of the Project

This document attempts to collect the information related to the awareness and dissemination activity for the work developed in nSHIELD project.

All the consortium members involved in the different WP and tasks will report periodically the results carried out for the update of this document.

References

[1] European Commission - Guide to successful communications, 2004 http://ec.europa.eu/research/science-society/science-communication/index_en.htm

[2] Aniketos FP7-funded project: http://www.aniketos.eu. For project description, see project presentation at http://aniketos.eu/content/project-presentation-slides

[3] PROSPER: Provably Secure Execution Platforms for Embedded Systems, http://www.sics.se/projects/prosper

[4] Global Platform, http://www.globalplatform.org/

[5] SAP Sustainability Report,

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

[7] [EPA, 2010] EPA Analysis of the Transportation Sector: Greenhouse Gas and Oil Reduction Scenario,

[8] Environmental Protection Agency, March 2010, www.epa.gov/oms/climate/ GHGtransportation- analysis03-18-2010.pdf, [assessed 23.8.2010]

[9] http://www.windriver.com/announces/embedded-device-security/

[10] https://csaw.isis.poly.edu/

[11] https://isis.poly.edu/esc/