Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D8.4: SHIELD run-through for the nSHIELD-project

Comment [1]: Andrea: I would suggest to use SHIELD to indicate the final platform, product, standard or whatever… nSHIELD is only the name of the project, but its output is SHIELD.

Comment [2]: Is this the final name for the project? If so it should be changed in the TA (amendment)

Due date of deliverable: M12 - 2012.08.31

Actual submission date: [xxx]

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

Organisation name of lead contractor for this deliverable:

Mondragon Goi Eskola Politeknikoa, MGEP

Revision [Issue 6]

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**		
Roberto Uribeetxeberria	Mondragon Goi Eskola Politeknikoa		
Luigi Trono	Selex Galileo		
Josef Noll	Movation		
Lorena de Celis	Acorde		
Andrea Morgani	Selex ES		
Renato Baldelli	Selex ES		
Andrea Fiaschetti	University of Roma “La Sapienza”		
Iñaki Eguia	Tecnalia		
Nikolaos Pappas	HAI		
Reviewed by			
Name	**Company**		
	Selex Galileo		
Approved by			
Name	**Company**		
	Selex Galileo		

Applicable Documents		
ID	**Document**	**Description**
[01]	TA	nSHIELD Technical Annex

Modification History

Issue	Date	Description
Issue 1	01.11.2012	First draft with TOC
Issue 2	07.12.2012	Contribution from HAI included
Issue 3	13.12.2012	Contribution from Tecnalia included
Issue 4	21.12.2012	Contribution from Movation and Selex Galileo included
Issue 5	14.01.2012	Adaptation to nSHIELD deliverable template
Issue 6	21.01.2012	Contribution from Uniroma and Selex ES included

Executive Summary

This document provides ….

Contents

Figures

Tables

Glossary

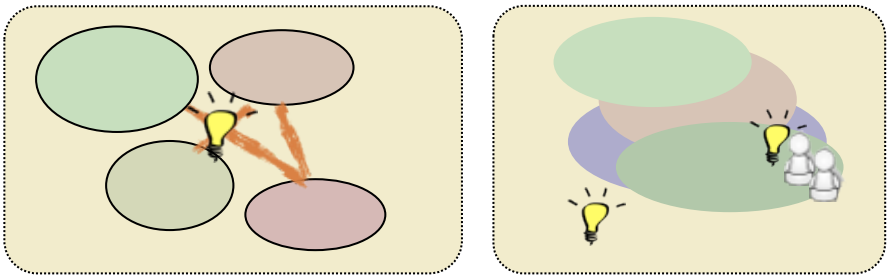
Please refer to the Glossary document, which is common for all the deliverables in nSHIELD.


This Page is intentionally left blank

1 Introduction

We are at the beginning of a new age of business, where dynamic interaction is the driving force for our business. The Internet-based service world today is based on collaborations between entities in order to optimize the delivery of goods or services to the customer (Figure 1-1a). The evolution towards the dynamic interaction between entities, as indicated in Figure 1-1b, is ongoing. One of the real challenges on this way ahead is the disappearing borders between companies, and the exchange of sensor- and process-based information between the entities. Given the second trend of dynamic modelling creating autonomous decisions is the lack of a measurable security when exchanging information. «Is the information that your system receives from one of the suppliers (or competitors) reliable? » is one of the key questions which you need to answer if your process or business model depends on those data.

This document will address the challenges of measurable security, coming up in the communication within and between enterprises, with the focus on information provided by sensor systems. We address the challenges of new infrastructures, new ways of communication and new devices. The two dominant trends in this domain are (i) wireless sensors contributing to automated processes and (ii) the move of control into mobile devices. The example "bring your own device" (BYOD) exemplifies the trends of devices accessing processes and information in enterprises. In the upcoming years not only phones, tablets and computers will demand access, but also sensors and embedded system will deliver and request information. Sensors will contribute to automated processes, and thus require a knowledge management.



a) Internet today – collaboration based b) Upcoming – dynamic interaction

Figure 1-1: The upcoming business world of dynamic interaction between entities

In the traditional way of handling security the attempt was to secure the whole infrastructure of a company. BYOD is often seen as a threat, and answered in the classical way by declining employees to use their devices, as security cannot be ensures. A second variant of counteracting classic threats as insufficient authentication and loss of devices is addressed through an approach of integrating, managing and securing mobile devices. Such a short-sighted approach, as suggested by leading IT companies, is deemed to fail. A paradigm shift in handling security is required, **addressing the need for securing information instead of securing infrastructure**. The paradigm shift includes the need for measurable security, and is the core of this document. It addresses a metrics-based approach for a quantitative assessment of both the potential attack scenario and the security measures of the infrastructure, and will outline the **methodology of measurable security for the Internet of Things**.

Comment [3]: I´d try to avoid using this a reference too often. I think it does not represent the majority of the scenarios (more in line with the IoT)

Measurable security is often misinterpreted as a good risk analysis. When “banks are secure”, it means that they have a decent risk analysis, calculating the loss against the costs of increased security. Hereby loss does not only mean financial loss, but also loss of customers due to bad reputation or press releases. Likewise, costs of increased security are not only the costs of applying new security mechanisms, but also a loss of customers, as customers might find the additional security mechanisms too cumbersome.

Our suggested approach works towards measuring security in terms of cardinal numbers, representing the application specific security methods as compared to the specific threat scenario. The approach is

based on the semantic description of both a potential attack scenario, the security-related aspects of my sensors/systems and semantic policies. **The outcome is a methodology for measurable security, and provides composable security for sensor systems**.

2 Is security an issue for your company?

Security has traditionally been a subject of intensive research in the area of computing and networking. However, security of embedded systems is often ignored during the design and development period of the product, thus leaving many devices vulnerable to attacks. The growing number of embedded systems today (mobile phones, pay-tv devices, household appliances, home automation products, industrial monitoring, control systems, etc.) is subjected to an increasing number of threats as the hacker community is already paying attention to these systems. On the other hand, the implementation of security measures is not easy due to the constraints on resources of this kind of devices.

One of the biggest challenges in security today is how the software in our operating systems and applications are so full of holes. And while traditional software makers have made (some) headway in developing more resilient applications, experts say embedded device and systems makers -from those who create implanted medical devices to industrial control systems- are eons behind in secure system design and development maturity.[1].

2.1 Introduction to Security features

Short explanation of security components, not only confidentiality, integrity and aut…

2.2 The nSHIELD run-through

The nSHIELD way of measuring security… - introducing and describing the words we are using.

Table 2-1: Run-Through from Antonio di Marzo presentation

Comment [4]: Check it

STEP	INPUT	OUTCOME
Environment and threats identification		Awareness
SPD Assessment	Application case *	SPD Guidelines
Metrics Implementation	SPD Guidelines and Tools*	Metrics (security measure)
Ontology Definition	Application case *, Tools*	Ontology (OWL)
Technological Injection	Software Module*, IP *, Template*, Trusted run time environment *	Software/Firmware customized modules (SPD SF Module)
Integration	SPD SF Modules + Design files	E.S. physical Implementation
Validation/Verification	SPD Validation tools*	Validation Report
Deployment		E.S physical Implementation + end user application note

Being able to set security as cardinal numbers on embedded systems.

2.3 Security for interoperability

Results of nSHIELD security discussion.

[1] George V. Hulme, http://www.csoonline.com/article/704346/embedded-system-security-much-more-dangerous-costly-than-traditional-software-vulnerabilities

Validate nSHIELD platform on real application demonstrators

- S1: Urban railways protection
- S2: Voice/Facial recognition
- S3: Avionic Computer that is an embedded system by definition: to provide a methods for dependable design in order to make possible a high functionality integration.
- S4: The objective for SMN application scenarios is to provide proof of the concept by using 4 key building blocks for this scenario:

3 Run-through details

3.1 Overview

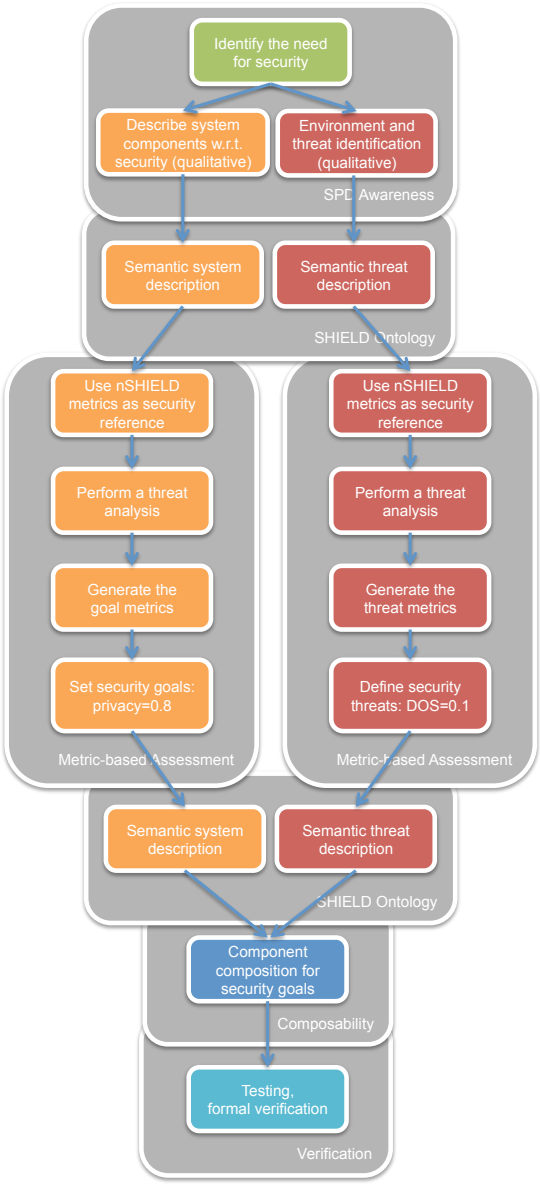


Figure 3-1: SHIELD framework for measurable security

Embedded system security is much more dangerous, costly than traditional software vulnerabilities; Experts say embedded device manufacturers too often lack maturity when it comes to designing secure embedded systems. There are a number of things that are different when it comes to embedded and industrial control system security. First the consequences of poor system design can create substantially more risk to society than the risks created by insecure traditional software applications. Second, it is much more costly -- if it is reasonably possible at all -- after the fact to update these systems.[2]

Figure 3-1 represents the SHIELD framework for measurable security from the awareness of the need of security of the embedded system designer to a successfully tested and verified secure embedded system implementation. During the design process the SHIELD framework will guide and help the designer to choose the appropriate security components according to its specific needs, the resources of the system and the threats it is facing.

The following sections will describe the different parts of the framework.

3.2 The Need for Security

Comment [5]: Josef and Luigi

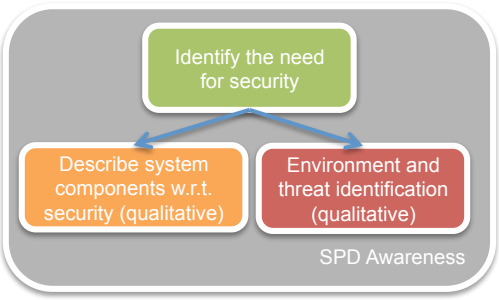


Figure 3-2: SPD awareness

The first and most important step is to be aware of the security risks. Even if the problems may be similar between traditional software development and embedded device security, the engineering teams do not take them into consideration so far. Therefore, a preliminary qualitative description of the system, the environment and threats will serve as input for a more formal semantic description, threat modeling and risk analysis described in the next sections.

3.3 SHIELD ontology

Comment [6]: Andrea Fiaschetti

The second step is to provide a formal description of the SHIELD components with the aim to:

1. Identify the atomic SPD functionalities and their mutual relations
2. Identify the functional and technological dependencies between SPD functionalities and system's components

These two descriptions are necessary because the point 1) prepares the system for an easier "quantification" of SPD metrics (see next step), while the point 2) prepares the system for to the "implementation" of the composition decisions.

[2] Nate Kube, chief technology officer and founder at critical infrastructure security software and services provider Wurldtech Security Technologies

These information are represented by means of an “ontology” or more in general a “semantic description” because it is simply a matter of “knowledge representation”: there are information to be stored in a structured way and the ontology allows, better than traditional data bases, to have a great expressiveness with a reduced size (in terms of bytes).

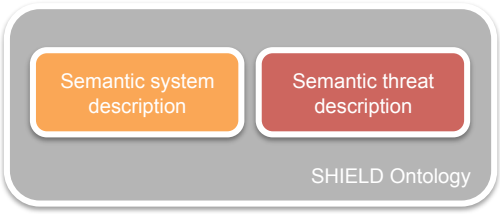


Figure 3-3: SHIELD ontology

The SHIELD Ontology, as depicted in Figure 3-3 comprises two sections: one about the ‘system’ and one about the ‘threat’. This distinction follows the Common Criteria guidelines according to which, in order to assess the security level of a system, it is necessary to start from the menaces that affect that system.

In particular the SHIELD logical procedure for Ontology structuring follows the logical process depicted in Figure 3-4:

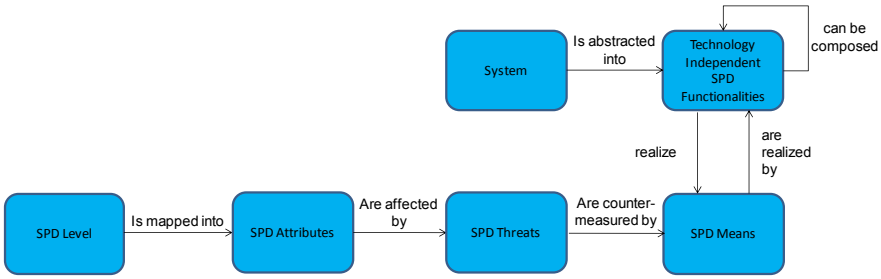


Figure 3-4: SHIELD ontology logical process

1. The system is decomposed into atomic elements, named SPD functionalities
2. These functionalities, individually, or composed with the other, realises an SPD mean, i.e. a mean to prevent a menace
3. This means are mapped over the SPD threats to countermeasure or mitigate them.
4. According to the mitigated threats, it is possible to quantify the impact on the overall SPD level, thanks to the SPD metrics that assign a value to the threats.

On an operational point of view, this step is translated into the following guidelines:

- Each manufacturer producing a SHIELD compliant device, equipes it with a file containing a semantic description of the related SPD functionalities
- Each SHIELD device is able to provide this semantic description to the Security Agents by means of service discovery or specifically tailored signalling protocols

3.4 Metrics-based assessment

Comment [7]: Renato and Iñaki Egia

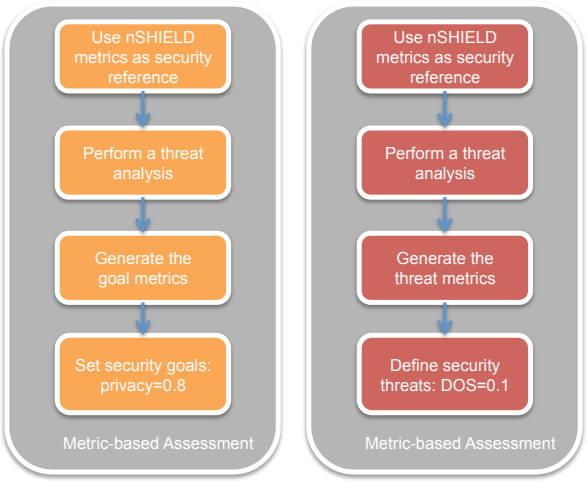


Figure 3-5: Metric-based assessment

Security, privacy and dependability concepts are measured in systems of systems as a whole: this means that metrics measure each sub-system (component) and compose them until the entire system measurement is gathered. This requires a full process performance and a security-interoperability searhing taks in order to collect quantifiable and confiable measurements and a composition model for computing the all-inclusive system.

nSHIELD defines a set of security, privacy and dependabilty metrics[3] which determine the formal quantification of the SPD metric. This is valid in order to have the correct scale and value for measuring the metric importance as an independent metric. This definition is consistent with the nSHIELD architecture as metrics are taxonomized in 4 layers (node, network, middleware and overlay)

As stated, one particular system might be composed of multiple subsystems (i.e.an aircraft is considred a system – D0-178B[4]- but contained with multiple subsystems). Each metric alone only measures a concrete part (subsystems or component) of the entire element. Therefore a composition of these measurements must be included in the process for measuring the system in an holistyc mode. nSHIELD will guarantee a formal method to compose metrics both in design and runtime scopes being able to provide an imput towards the overlay layer which is also capable to compose other SPD functionalities in a semantic way[5].

[3] SPD Preliminary Metrics in nSHIELD. 2.5 Document.

[4] RTCA/DO-178B "Software Considerations in Airborne Systems and Equipment Certification", p.82

[5] Notice that there is a difference between metrics composition and composable security in 3.5

The formal method used is inspired by Manadhata and Wing work titled as: "An Attack surface Metric". The middleware of the nSHIELD, entirely developed by the consortium, and one of the core system entity providing security functionalities is meausered introducing the notion of a software system's attack surface, presenting a systematic way to measure security both qualitatively and quantitatively. Intuitively, a system's attack surface is the set of ways in which an adversary can enter the system and potentially cause damage. Hence the "smaller" the attack surface, the more secure the system.

The formalization of the notion of a system's attack surface is achieved using I/O automata model of the system and its environment. Manadhata and Wing defined a qualitative measure and a quantitative measure of the attack surface introducing an abstract method to quantify attack surfaces.

System's entry points are the ways through which data "enters" into the system from its environment and exit points are the ways through which data "exits" from the system to its environment. Many attacks on software systems require an attacker either to send data into a system or to receive data from a system; hence the entry points and the exit points act as the basis for attacks on the system. Choosing I/O automata model it's possible to map naturally the notion of entry points and exit points to the input actions and output actions of an I/O automaton. Also, the composition property of I/O automata allows us to reason easily about a system's attack surface in a given environment.

For a complex system, as nSHIELD is, we can con construct an I/O automaton modeling by composing the I/O automata modeling the system's simpler components. The composition of a set of I/O automata results in an I/O automaton.

Metric asssesment is the enforcement and validation of the measurement per se. This will be a test-based enforcement as it is depicted in the previous figure and will converge with the Common Criteria standard. The main problem for the measurement is to establish the correct value (seeting the goal) for the metric. This value often is provided by manufacturers and integrators according to norms and regulations continuing with empirical and experimental stress tests. The difficulty comes when new modules and components are interoperating with existing elements: this entails unexpected behaviours that shall be corrected through metrics and monitoring mechanism. nSHIELD will deal with this problem in an interdomain, heterogenous and distributed environment.

Nowadays, there is no instrument or tool able to measure systems as nSHIELD will do. This mechanism will impact in the industry setting a new reference in two ways: generating a new formal and quantifiable model for measuring systems of systems and industrialising a tool for implementing this model. These two results will impact specially in the Critical Infrastructure market.

3.5 Composable Security

Comment [8]: Andrea Fiaschetti and Andrea Morgani

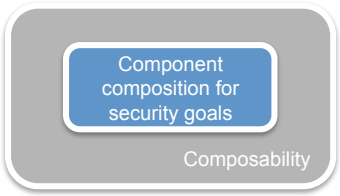


Figure 3-6: Composability

3.6 Testing and Verification

Comment [9]: Helenic Aerospace

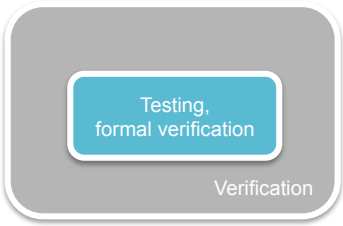


Figure 3-7: Testing and verification

The consortium, in the framework of respective work packages, has started the technical development of nSHIELD components, with the final aim of forming an overall integrated functional platform. As a first stage and to assist this process we have registered an analytical set of requirements and metrics and designed a reference system architecture. The prototypes, that will be developed, will constitute nSHIELD platform, which in turn will be the subject of a formal validation procedure, that will prove the venture's correctness. The testing and verification plan is formalized upon specific methodology, taking into account all necessary validation parameters. A brief synopsis of this plan will be exposed hereafter.

The grounds for a coherent, modular and composable *architecture* has already been established. The design is based on the definition of three types of devices (nS-ESD, nS-ESD GW and nS-SPD-ESD) and four layers (Node, Network, Middleware and Overaly), that host the nSHIELD SPD functionalities. The architectural outline feeds the technical preparation of real components, that partners have started to develop. Software modules will be installed on these nodes, to control functionalities and services (SPD and not) we wish to implement. Important role will be played by the proper specification of interfaces, either the latter concern internal and external communication or application and user services. The above are summarized in the formation of prototypes, that will constitute the objects of integration and the core ingredients of the overall *platform*. The architecture shall be finalized and reflected in reality in what will be the nSHIELD platform. This platform will be evaluated and validated through the testing and verification procedure, on the grounds of connection with real world needs, as they are represented by the four application scenarios predescribed.

Comment [10]: References? Acronyms?

The selection of the four *scenarios* is based on real application domains, that form common objectives, such as to demonstrate enhanced SPD functionalities. The first concerns Railroad Security, mitigating the vulnerability against criminal acts in infrastructures or on board. nSHIELD will be involved in the establishment of a smart-surveillance system. The second scenario is about Voice/Face Recognition, designated to improve security and simplify everyday services (logistics, automating tolling payment etc.). nSHIELD aims to provide solutions in compliance to international standards. The third scenario involves Dependable Avionic Systems, attempting to follow the rapid advances in electronics technology. Our focus will be set mainly to avionics for Unmanned Aerial Vehicle. The last application scenario will be activated in the framework of Social Mobility and Networking, applied in the context of smart cities environment. We expect that Security, Dependability and Privacy issues, addressed by nSHIELD, will play an important role in the applications of this area.

One more nSHIELD aspect to consider, before proceeding with the presentation of validation methodology, is the system's *functionalities* and *services*. Since the process of developing them is on going we can recite some, indicatively:

- SPD Audit
  - ✓ Recognizing, logging and analysing information about SPD functionalities

- Cryptography
  - ✓ Several implementation types of cryptographic functions
- Identification and authentication
  - ✓ Verifying the identity of users
- Protection of the SPD functionalities
  - ✓ Ensuring the integrity of SPD functionalities data
- SPD functions Management
  - ✓ Management of SPD functionalities

Proof of concept for the nSHIELD Platform will be achieved through its *Validation against* a list of "parameters" (more correctly basic "concepts" or "sections" of nSHIELD System). At this stage we can only suggestively enumerate the terms that will be used to verify the consistency of components. Firstly, validation will be held against the semantic model that defines the nSHIELD Ontology. Secondly, the platform's robustness shall be tested against the sequence of actions that constitute the provided services, namely "discovery, composition and orchestration". Another evaluating term shall be the desired SPD levels that is the thresholds our system we wish to comply with, in order to have an effective operating level. To the above we could add the validation against WSN networking parameters: system integration test (interfaces between sensors), performance test (network operational parameters), security and cryptography levels, field tests, communication protocols' testing and unit test (sensor software). The deployment of WSN networks should comply with the specifications registered.

The *Testing* procedure shall be adequately predefined and codified to a conceptual and effective methodology. Beginning with the test-bed details (available equipment, HW & SW), this involves constructing the application domains through the connection of scenarios to a list of use cases, in which the system's performance must fulfil specific measurement criteria and validate system capabilities. Comprehensive and illustrative reporting and monitoring tools will be deployed. This relates also with the analytic but straightforward organization and representation of the testing functions (e.g. use of standard templates). The trials framework will be settled, depicting the input, the expected output and quantification of requirements during the tests. The proposed test plan, translating the output of an action-result sequence, shall guarantee the demonstration of nSHIELD services and features.

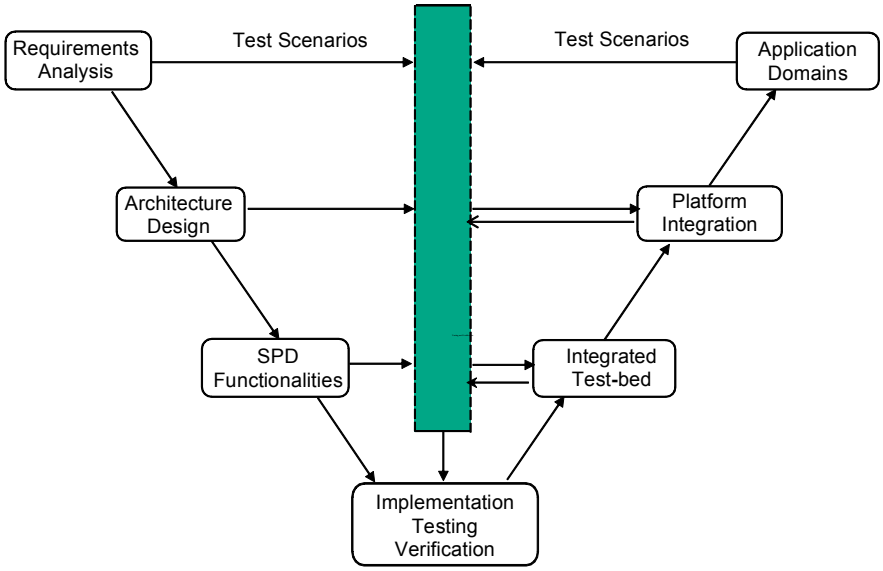


Figure 3-8: Platform Validation Procedure

3.7 Expected Outcome

4 Conclusions

nSHIELD is an international research project. The scientific and technical works of the project are going to be performed by the partners from several countries.

Further information:

- nSHIELD Web page:
  The main reason for having an “own-standing platform” for the publication of information and news is the requirement for a good “look and feel”. Such functionality is not core functionality of wiki implementations and except for the Institute of Applied Informatics and Formal Description Methods at the Karlsruhe Institut for Technology. An implementation as done by AIFB would have exceeded the frame of the project, and nSHIELD therefor decided to go for traditional Web design for the nSHIELD Web, which is available at: http://www.newshield.eu/.

  Further details on the Web page are provided in deliverable D8.1.1. The main deficiencies of conventional web pages are the non-interactive way of updating information and handling documents. This is the reason for using a Wiki as document repository and collaboration.

- Semantic Media Wiki for collaboration:
  Wiki software is the state-of-the-art collaboration software and used in a number of international projects. It supports day-to-day work through a useable interface. Special focus in nSHIELD is on the semantic extensions, allowing machine-readable information and information exchange through the platform. The latter capability was introduced to open for an extension of sensor input into business process, being a part of a M2B platform. The Norwegian associate partner Norwegian Rail Authorities (Jernbaneverket - JBV) has structured all their internal processes on a semantic mediawiki, thus one of the visions of nSHIELD is to allow for sensor input towards these processes.
  The Semantic Wiki is available at http://nshield.unik.no

Through these platforms nSHIELD enables an efficient way of collaboration, and opens for the vision of nSHIELD sensor input for business processes.