Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

D8.3: Standardisation Plan

Due date of deliverable: M6 – 2012.02.29

Actual submission date: M10 – 2012.06.28

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

Organisation name of lead contractor for this deliverable:

Selex Galileo, SG

Revision [Final v1.0]

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)	

nSHIELD

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Cennamo Francesco	Selex Galileo		
Luigi Trono	Selex Galileo		
Esposito Mariana	Ansaldo STS		
Flammini Francesco	Ansaldo STS		
Iñaki Eguia	Tecnalia		
Eider Iturbe	Tecnalia		
David Abia	Acorde		
Lorena de Celis	Acorde		
Ignasi Barri	Indra		
John Gialelis	ATHENA		
Spase Drakul	THYIA		
Stefano Gosetti	ETH		
Josef Noll	Movation		
Reviewed by			
Name	**Company**		
Roberto Uribeetxeberria	MGEP		
Approved by			
Name	**Company**		

Applicable Documents

ID	Document	Description
[01]	TA	nSHIELD Technical Annex

Modification History

Issue	Date	Description
Final v1.0	28.06.2012	Final version

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

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

2 nSHIELD relevant standards and regulations

2.1 Standards and regulations for Security

The standardization that nSHIELD is looking for, first has to has taken into account other existing standards and fit into them as seamlessly as possible. Some of these standards are domain specific and as demonstrators in nSHIELD will be deployed in railway systems, the first step is the adaptation to existing standards in railway security. Safety-related electronic systems for signalling include hardware and software aspects. The requirements for safety-related hardware and for the overall system, in particular in railway industry, are defined in the CENELEC [1] standard. The aim of this standard is to develop compatible railway systems based on common standards of European railway authorities and European railway industry. These standards concern Electromagnetic compatibility, use of the range frequency and protection of the communication. For the railway sector, it is responsible for the development of European Standards for electro technical applications related to the Rail Transport Industry of the European Union.

The industry comprises:

- Rail users;
- Public and private rail transport operators (passenger and freight);
- Infrastructure owners;
- Manufacturers and maintainers;
- Service providers (e.g. consultants, financers, etc.);
- Public authorities (National and European);
- Regulatory bodies;
- Trade associations.

The EU aims to achieve free and unrestricted transfer of goods, services and passengers across national frontiers within Europe, has adopted two directives concerning the Interoperability of the European Railway System and the Railway Safety. The implementation of these directives is aided by standards developed by CEN, CENELEC and ETSI (European Telecommunications Standards Institute).

In particular, the most relevant norm and regulation are the following:

1. EN 50131 *Alarm systems - Intrusion and hold-up systems*
2. EN 50133 *Alarm systems - Access control systems for use in security applications*
3. EN 50134 *Alarm systems - Social alarm systems.*
4. EN 50136 *Alarm systems - Alarm transmission systems and equipment*
5. EN 50159-1 *Railway applications – Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems.*
6. EN 50159-2 *Railway applications – Communication, signalling and processing systems - Part 2: Safety related communication in open transmission systems*

The EN 50131 standard specifies the requirements for Intrusion and Hold-up Alarm Systems (I&HAS) installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. This standard specifies performance requirements for installed I&HAS but does not include requirements for design, planning, installation, operation or maintenance. These requirements also apply to I&HAS sharing means of detection, triggering, interconnection, control, communication and power supplies with other applications. The requirements of this European Standard also apply to IAS (Intrusion Alarm System) and HAS (Hold-up Alarm System) when these systems are installed independently. When an I&HAS does not include functions relating to the detection of intruders, the requirements relating to intrusion detection do not apply. When an I&HAS does not include functions relating to hold-up, the requirements relating to hold-up do not apply.

The EN 50133 specifies requirements for automated access control systems and components in and around buildings. It includes: system architecture and general requirements of an access control system for security applications, requirements for functions, definition of the environmental and electromagnetic compatibility conditions, requirements for communication of an access control with others, such as access point actuators and sensors, alarm system, etc...

The EN 50134 specifies the requirements and tests for manually-activated trigger devices forming part of a social alarm system. This standard only applies to manually-activated trigger devices that transmit the alarm triggering signal to a local unit or controller via cable or wire-free radio transmission, i.e. Push button fixed; Pull switch fixed; Push button portable; Pull activated portable. This standard also gives guidance on automatically-activated trigger devices. For the requirements and tests applicable to such trigger devices, references are made to appropriate CEN/CENELEC standards for fire alarm, gas alarm and intruder alarm system components. This standard does not specify EMC emission or electrical safety requirements. These are covered by other standards.

The EN 50136 specifies the requirements for the performance, reliability and security characteristics of alarm transmission systems. It specifies the requirements for alarm transmission systems providing alarm transmission between an alarm system at a supervised premises and annunciation equipment at an alarm receiving centre. This European Standard applies to transmission systems for all types of alarm messages such as fire, intrusion, access control, social alarm, etc. Different types of alarm systems may in addition to alarm messages also send other types of messages, e.g. fault messages and status messages. These messages are also considered to be alarm messages in the context of this standard.

The EN 50159-1 standard deals with safety-related communication between safety-related equipment using a closed transmission system. Both, safety-related and non-safety-related equipment can be connected to the transmission system. This standard does not impose safety requirements on the non-trusted transmission system itself, but its properties and its physical characteristics shall be defined.

The 50159-2 standard is closely related to EN 50159-1 “Safety-related communication in closed transmission systems” and ENV 50129 “Safety related electronic systems for signalling”. The standard is dedicated to the requirements to be taken into account for the transmission of safety-related information over open transmission systems. Cross-acceptance, aimed at generic approval and not at specific applications, is required in the same way as for ENV 50129 “Safety related electronic systems for signalling”. If a safety-related electronic system involves the transfer of information between different locations, the communication system then forms an integral part of the safety-related system and it must be shown that the end-to-end transmission is safe in accordance with ENV 50129.

The CENELEC 50159-part 2 norms report the threats of a communication based on an open network (i.e. deletion, re-sequencing, insertion, repetition, delay, corruption and authentication of a message; see Table 1) and suggests some means to ensure the safety of the system with respect to such threats.

Table 1: Means

CENELEC EN 50159 Keywords	
Keyword	**Meaning**
Repetition	A message is received more than once
Deletion	A message is removed from a message stream
Insertion	A new message is implanted in the message stream
Re-sequencing	Messages are received in an unexpected sequence
Corruption	The information contained in a message is changed, casually or not
Delay	Messages are received at a time later than intended
Masquerade	A non-authentic message is designed thus to appear to be authentic (an authentic message means a valid message in which the information is certificated as originated from an authenticated data source)

2.2 Standards and regulations for Privacy

Before addressing standards and regulations for privacy, we will first provide a term definition of privacy. The former concept of “private” information as compared to “public” information gets a completely new meaning when entering the digital world, where sensors and systems provide and distribute date which might (i) violate the private information about a user, but which might also (ii) violate the protection of information being vital for a company.

Thus this section will first address the historical meaning of privacy; it will then address privacy for corporate information in the Web 3.0, and will finally address the rules and regulations for privacy protection.

2.2.1 Historical dimension of privacy

Privacy is a term established as long back as in the Roman empire [15], and was established to separate the roles of people, being public as part of a government in one situation, and private in another. Though privacy is stronger announced in Europe as in other parts of the world, it became a common understanding that respecting a certain amount of privacy is necessary for the function of a society. Before addressing laws and constitutions on privacy, we will first address our understanding of the term.

Assuming that privacy protection means the protection of private data, we need to analyse the use of private data. A good discussion on this topic is provided in the PhD thesis of Were Oyonmo [11], where he lists several scientific viewpoints, ranging from Erickson [12] «*any information that is owned by a person, such as a calendar, maps, notes, addresses…»* to a definition inspired by Al-Fedaghi [13] «*any information individually or collectively generated or that is owned by a user, which may include any individuals’ name, group’s identifiable information, physical or electronic, including names, addresses, phone numbers, race, ethnicity, nationality, origin, gender, marital/family status, identifiable numbers, codes, symbols, registers, biological, educational, financial, criminal, and situational information that can be used to dissociate them from the population*».

The main differences are (i) the situation awareness and (ii) the dissociate from the population. Thus the latter definition is much stronger than the definition from Erickson.

This diverging expectation of privacy leads to the principle problem in defining standards for privacy. Depending on the background of the community or the authorities, they have implemented constitutions and laws to protect privacy.

The Universal Declaration of Human Rights states in article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*.

In Europe the article 8 of the European Convention on Human Rights guarantees the right to respect your private and family life, one’s home and correspondence. This principle article is the basis for decisions of the European Court in Strasbourg and the EU Directive 95/46/EC on the protection of personal data as mentioned in chapter 2.2.3. All European Countries have adopted the directive into national law.

2.2.2 Privacy in the Web 3.0 epoch

While the principle laws on privacy are taken care of in each European Country, technology developments have established a “grey zone” of collecting de-facto identifiers and thus are able to identify a person. The most obvious one is the use of the mobile phone, where the phone number - so being able to be changed - has become a de-facto identifier of a person and is used in digital forensics. All digital equipment and services have such identifiers, being it IP-addresses of devices, credit card numbers or transaction IDs.

The Internet has in the era of «Web 2.0» provided the opportunity to combine information, and search engines like Google have given the opportunity for everyone to combine information and establish details on a person which were thought to be “private”, e.g. pictures from parties. Search has become much more advanced, using machine-readable technologies to get an even better understanding of the search topic, and to combine search results into an automatically represented picture. Examples of such are 123People.com and Arnetminer.org. Through the collection of all their Google services, from picture, maps to Google Plus (G+), Google has initiated a debate on violating the principle of privacy through this common accounting. Google still claims that they will not use your personal information, and just use it for developing “user profiles”.

Other actors are not that reluctant and collect personal information in a wide range. Apple had stored all movements of users and made them available on their servers, but had to stop this service thanks to the invention of public authorities. Facebook is legally on the safe site when asking for a user agreement to «allow for access to phone data» in their newest Android app, but it remains to be seen if the usage of those data is in agreement with the EU directive. To collect and use all phone information, including currently whom you talked to and how long you talked with that person, and in a later stage analyse the content of the talk and use the topics for their services makes the user extremely vulnerable, and is to the authors opinion a non-acceptable violation of privacy.

Privacy information in the Internet was always a target for compromises, as the previous examples show. In the upcoming «era of Web 3.0» computer-readable mechanisms will extend the ability of retrieving information across domains and make them available for services.

The Web 3.0 will also change the structure of corporate organisations. While collaboration currently is based on mutual agreement and limited exchange of information, information about companies will be “available” to a much wider degree thanks to embedded systems and their capabilities to communicate. Thus protection of relevant information is a challenge for all corporates. The legal dimension is weak, as the immense grey zone of what are collaborate data and what is “private” knowledge retrieved from collaborate and public data is hard to be defined.

2.2.3 Rules and regulations for privacy protection

The previous chapter provided an introduction to the challenges of establishing rules, regulations and standards for privacy, especially taking into account the technology developments of the Web 3.0 era.

Measures of privacy are difficult, and so is the user- and corporate behaviour when it comes to "private data". Andrea DiMaio, a member of the Gartner Blog Network, provides a good summary of the challenges that the Internet brought to Privacy [16]. In his blog on "Forget Privacy, It Is Just an Illusion" he pointed out the variety of people and their behaviour when it comes to private information. Users have their "circles of trust", and share information accordingly.

A short introduction on the principle laws of privacy was given before, and is further outlined for Europe and the USA in this chapter.

The European Union Data Protection Directive 95/46/EC [17], defines private information for the European citizens under the term "personal data". The understanding of "personal data" encompasses «*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity*». The United States government uses the term "Personal Identifiable Information" in the meaning of «*information which can be used to distinguish or trace an individual's identity, such as their names, Social Security Number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date or place of birth*» [10]

The nSHIELD project works on «measurable security» and thus «measurable privacy», which is the basis for a discussion on how data collection and usage will violate the use of "private data". Whether this will lead to new standards, to new laws or support court decisions is yet to be shown.

Standard organisations like ETSI have identified the challenge, and are currently in the stage of defining their strategy towards this eminent subject. ETSI has announced the 8th ETSI Security Workshop [18] on 16-17 January 2013, where privacy is one of the topics. A statement given by Eike Wolf in the 2010 workshop addresses the challenge [14]: «Data privacy was a general concern at all times and it becomes a legal basis in EU with the Data Privacy Directives 1995. It was more or less neglected in the past but it is a must for all future standards when they should be accepted by the stakeholders, the administrations, the legal courts and therefore by the market. The reason for these activities is the much greater awareness of data privacy by the general public»

2.2.4 Aspects of a novel vision for privacy

Following the discussion of privacy as given in the previous chapters does lead to a user- or corporate-defined value of information. The currently ongoing discussions include the following topics:

- Focus on the value of information rather than securing all infrastructures. Only when measures of the value of information are available, one knows on how to protect them.
- The challenge of virtualisation and cloud services, including the grade of information from embedded systems.
- The role of authorities versus standards when it comes to privacy protection. Standard bodies usually discuss the specifications for information exchange, while authorities build the "rule-set" on which the information is based.

These discussions are ongoing in nSHIELD, and will emerge into recommendations and actions on where and how to contribute to ensure «measurable security».

2.3 Standards and regulations for Dependability

2.3.1 Integrated modular avionics

Integrated modular avionics (IMA) represent real-time computer network airborne systems. This network consists of a number of computing modules capable of supporting numerous applications of differing criticality levels.

The IMA concept proposes an integrated architecture with application software portable across an assembly of common hardware modules. IMA architecture imposes multiple requirements on the underlying operating system.[6]

Standardization efforts were on-going at this time (see ASAAC or STANAG 4626), but no final documents were issued then.

Allied Standards Avionics Architecture Council, or **ASAAC**, is an effort to define and validate a set of Open Architecture Standards for Avionics Architecture, particularly in the field of Integrated Modular Avionics. A specificity of Integrated modular avionics in the certification process of avionics systems is that standards such as ARINC 653, which form the basis of Integrated modular avionics today, allow each software building block of the overall Integrated modular avionics to be tested, validated, and qualified independently (up to a certain measure) by its supplier [7].

2.3.2 Aviation Industry Activities Organized by ARINC

AEEC, AMC, and FSEMC are aviation industry activities organized by ARINC to establish consensus technical standards, known globally as ARINC Standards, and develop shared technical solutions that no one organization could accomplish independently.

ARINC Standards and collaborative solutions improve cost effectiveness, increase productivity, and reduce life-cycle costs for airlines and their partners in the avionics, cabin system, and flight simulation and training segments of the aviation industry.

AEEC, AMC, and FSEMC are global technical activities comprised of airlines and other organizations eligible to be Member Organizations with additional support provided by Corporate Sponsors.

Each activity operates under the leadership of aviation industry committees elected by the AEEC, AMC, and FSEMC Member Organizations in accordance with their Terms of Reference (TOR) approved by the ARINC Board of Directors. The activity leadership committees -i.e., AEEC Executive Committee, AMC Steering Group, and FSEMC Steering Committee- include representatives of more than 40 airlines and aviation organizations.

The leadership committees are responsible for providing oversight to their respective activity including defining the work program, planning for the major technical meetings, monitoring progress in accomplishing the technical projects, and approving the resulting ARINC Standards [19].

ARINC Industry Activities (IA) serves as the secretariat for the AEEC, AMC, and FSEMC. As secretariat, IA arranges the major international meetings held annually, schedules and reports on the results of subcommittee and working group meetings, and publishes the ARINC Standards and other technical products that result from the work of three activities. An unbiased and objective secretariat is essential to the success of the AEEC, AMC, and FSEMC. Therefore, IA is managed and financially accounted for independently of other ARINC businesses.

The ***Airlines Electronic Engineering Committee (AEEC)*** creates value for airlines and the aviation industry by developing engineering standards and technical solutions for avionics, networks, and cabin systems that foster increased efficiency and reduced life cycle costs throughout the aviation community.

ARINC Standards, developed and adopted by AEEC, deliver substantial benefits to airlines and aviation industry by promoting competition, providing interchange ability, and reducing life-cycle costs for avionics and cabin systems.

Over 4000 engineers and scientists representing nearly 250 sponsoring organizations participate in the development of ARINC Standards. These standards define key elements of equipment and systems installed in more than 10,000 aircraft around the world.

The activities of the AEEC are led by the AEEC Executive Committee in accordance with the Terms of Reference approved by the ARINC Board of Directors. The ARINC Standards Development Document specifies the procedures used to develop voluntary consensus-based ARINC Standards.

The **AMC** is an air transport industry activity organized by Aeronautical Radio, Inc. (ARINC). The objectives of AMC are to promote reliability and reduced operating cost in air transport avionics by improving maintenance and support techniques through the exchange of technical information.

AMC consists of representatives from the technical leadership of the air transport avionics maintenance community. The voting membership of AMC consists of the representatives of commercial air transport operators. AMC accomplishes its objectives through a number of activities including the annual Avionics Maintenance Conference, known worldwide as the AMC; Steering Group meetings, Plane Talk®, a quarterly newsletter; Task Group activities; and liaison with the AEEC and with other aviation or electronic industry activities. AMC promotes improved avionics reliability and performance at lower life-cycle cost through the coordination of common technical problems in the airlines. AMC saves the industry over $100 million each year through participation in the annual Avionics Maintenance Conference. AMC also tracks developing maintenance issues and new products and makes inputs to or develops guidance to maintain safe aircraft with lower life-cycle costs.

The annual AMC, held every spring, provides airlines and suppliers an opportunity to openly and collectively discuss chronic avionics maintenance questions. Before the meeting, airlines and suppliers are invited to submit discussion items using the following categories:

- Avionics Philosophy
- Line Maintenance
- Product Support
- Test Systems
- Environmental Control Systems
- Communications Systems
- Software
- IFE Systems
- Indicating Systems
- Navigation Systems
- Auto flight Systems
- Flight Controls
- Engine Systems
- Fuel Systems
- Electrical Power
- Lighting
- Landing Gear
- Others

Once the questions are received by the IA Staff, they are forwarded to the named equipment suppliers. Then the IA Staff prepares the questions in the form of the AMC Program, which is mailed to all preregistered attendees.

During the meeting, a moderator presents each question for discussion. By design, airline attendees are given the first opportunity to respond. This is to emphasize that the organization submitting the question may not be the only organization experiencing the problem. In some cases, another organization may have already experienced the problem and may have a solution to offer. Next, the moderator will call for the suppliers to respond. In many cases, a solution is already available, because the supplier has been aware of the problem well in advance of the meeting. If the solution is accepted, the question is closed. If the solution is not accepted or one is not yet available, the question is usually held open and will be so noted in the report of the meeting.

To ensure that the final AMC Report presents an accurate record, the meeting is recorded and a report is prepared.

The **FSEMC** is an air transport industry activity organized by ARINC Industry Activities. The objectives of FSEMC are to promote reliability and reduced operating cost in flight simulators by improving engineering, maintenance, and support techniques through the exchange of technical information. FSEMC includes users of flight and cabin simulators (dynamic and static). Users include airlines, commuter airlines, and other simulation users. Participants include airframe manufacturers, simulator manufacturers, aircraft equipment suppliers, and simulator equipment suppliers. The FSEMC consists of representatives from the technical leadership of the air transport flight simulator engineering and maintenance community (Operators), other companies whose primary involvement with flight simulators is as users with significant engineering and maintenance resources committed to the support of simulator use (Other Users), organizations who support the above named groups through provisions of materials or services (Suppliers), and other interested organizations (Others). The voting membership of FSEMC Member Organizations who are present and registered at the annual conference. FSEMC accomplishes its objectives through a number of activities including an annual conference, steering committee meetings, task group activities, and liaison with the AEEC and with other aviation or electronic industry activities.

3 Contribution to standards and regulations

3.1 Contribution in standardization bodies and industrial fora

3.1.1 ISO/IEC 27000

One of the main challenges in nSHIELD project is the achievement of the standardized SPD certificability of a system. It is important for nSHIELD to cover the system approach taking into consideration the SPD properties of the overall system instead of each component individually. SPD metrics in particular are considered the indispensable basement for building standardized methods and industry-wide accepted parameters for certificability in security, privacy and dependability field.

nSHIELD aims to define and establish a new way to build and integrate security into an application based on the idea that the application has to be designed integrating security properties as requirements from the beginning. Thus the security will be part of the overall system from scratch.

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

Therefore nSHIELD will lead the development and the institutionalization of a new SPD integration approach for a generic embedded system based on the definition of SPD metrics in order to track the SPD requirements of the overall system (through the nSHIELD layers: node, network and middleware) and therefore defining a single level of SPD assurance for the whole system. This SPD metrics based-solution consists of well-defined procedures for the management of the lifecycle of the SPD applications.

As a result, nSHIELD will define a metrics-based and procedures-based standard security model for a generic embedded system addressed for obtaining the system certification.

One of the most known security models is the ISO/IEC 27000 Series Standard where the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within an organization are specified.

The ISO/IEC 27000 standards family, central to the theory of security management, defines the specification for an Information Security Management System driven by a continuous organizational process improvement (following the Plan-Do-Check-Act cycle).

An Information Security Management System standards comparative study [3] provides a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. It is important for a standard being accepted and recognized at world level; hence the successful deployment of the standards in the industrial sectors will be straightforward. In the mentioned comparative study the ISO standard is most widely used by 163 countries, compared with BS (110), PCIDSS (125), ITIL (50) and COBIT (160).

"*Standardized security techniques are becoming mandatory requirements for e-commerce, health-care, telecoms, automotive and many other application areas in both the commercial and government sectors. ISO/IEC 27000:2009, together with the other ISO/IEC 27000 family of standards, aims to assist organizations more effectively achieve an appropriate level of information security*." [2]

Regarding ISO's challenges nSHIELD aims to contribute to ISO/IEC 27000 series standard defining a well-defined SPD metrics catalogue and the procedures for the management of the SPD properties through the whole SPD application lifecycle. As a result, the continuous process improvement approach of ISO/IEC 27000 will benefit from a well-defined SPD framework in the field of embedded systems.

3.1.2 IEEE - Institute of Electrical and Electronic Engineers Standardisation

The key concept of nSHIELD project are definition of SPD metrics in order to address the SPD requirements in the context of Embedded Systems (ESs), proposing and perceiving the first step toward SPD certification for future ES. Furthermore, the leading concept is to demonstrate composability of SPD metrics. The composability of this architectural framework will have great impact on the system design costs and time to market of new SPD solutions in ESs. At the same time, the integrated use of SPD metrics in the framework will have impact on the development cycles of SPD in ESs because the qualification, certification and validation process of a SHIELD framework instance will be faster, easier and widely accepted. SPD metrics in particular are considered the indispensable basement for building standardized methods and industry-wide accepted parameters for certificability in security, privacy and dependability field. The effort will be reduced by the definition of common SPD metrics and the development of tools to support the SPD lifecycle over the whole ES. Integrated with a validated SPD framework the further will allow to deploy standard method of quality assessment for the ES solution while the latter will controls the SPD quality conformance of the system through its upgrades during the years it will be deployed and operational on the field. The standardization activities will be led by the strong industrial partnership of the consortium, influencing new and existing standards and regulations also at international level as IEEE [9].

IEEE stands for Institute of electrical and Electronic Engineers. IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities. The IEEE is engaged in an enterprise-wide strategic planning process. IEEE applies strategic thinking, explores new ideas about strategic governance, and uses new methodologies for strategic dialogue. IEEE's strategic and long-range plan is grounded in core values, describes a desired vision, and what will be essential to achieving this vision. IEEE's commitments are articulated in goals that declare the outcomes the organization intends to achieve. Underlying this plan is the adoption of an ongoing process of planning and thinking strategically, designed to ensure relevance of direction and action over time. IEEE creates an environment where members collaborate on world-changing technologies – from computing and sustainable energy systems, to aerospace, communications, robotics, healthcare, and more. The strategic plan of IEEE is driven by an envisioned future that realizes the full potential of the role IEEE plays in advancing technology for humanity. IEEE is led by a diverse body of elected and appointed volunteer members. The governance structure includes boards for operational areas as well as bodies representing members in the 45 Societies and technical Councils and ten worldwide geographic regions.

For over a century, the IEEE has sponsored various programs to honour achievements in education, industry, research, and service. These awards and recognitions each have a unique mission and criteria, and offer the opportunity to praise distinguished colleagues, dedicated teachers, and corporate leaders who have made a lasting impact on humanity, technology, and the profession.

Among the mission of the IEEE is to develop electronics and computer science standards. Though it is a U.S. based organization, standards developed by the IEEE often become International standards. Some examples of commonly-used products standardized by the organization are the IEEE 1284 interface (a.k.a. Parallel Port), which many printers use, and the IEEE 1394 interface (a.k.a. Firewire), which is a super-fast connection for digital video cameras, hard drives, and other peripherals.

The IEEE activities improve the capability of standardization process through valuable feedbacks and brand-new solutions to those issues. The first step toward IEEE standardisation is to exploit and develop nSHIELD tasks about metric and composition and to disseminate project results in IEEE conferences and workshops by organizing special sessions, specific panel, paper submission and workshop. Some of most important IEEE (co)sponsored events are the following:

- DSN (Conference on Dependable Systems and Networks) is the most prestigious international forum for presenting research results in the field of dependability and security. It aims at offering a value focused program including plenary talks, papers, experience reports, panels, demonstrations of tools and technologies, debate sessions, together with state-of-the-art workshops and tutorials.

- SRDS (International Symposium on Reliable Distributed Systems) is a forum for researchers and practitioners interested in distributed systems design, development and evaluation, with emphasis on reliability, availability, safety, security, trust and real time. Is possible to propose research papers as well as practical experience reports that deal with design, development and experimental results of operational systems.
- HASE (IEEE International Symposium on *High Assurance Systems Engineering)* is a forum on tools and techniques used to design and construct systems that, in addition to meeting their functional objectives, are *safe* and *secure*. Of central importance, is the strength of the evidence supporting the *assurance case* - the argument that a system satisfies its safety and security policies.
- ECBS (IEEE International Conference and Workshops on the Engineering of Computer Based Systems) is conference devoted to the analysis, design, development, deployment and evolution of complex systems whose behaviour is largely determined or controlled by computers. It integrates several disciplines, including software, hardware, and communication into a complete systems engineering approach.

Furthermore, it is possible to activate a specific IEEE geographic unit. The major geographic organizational units of IEEE are Regions, Sections, Chapters, Student Branches, and Affinity Groups.

- **REGION**

  A Region is a Geographic Unit established by the Member and Geographic Activities (MGA) Board as an operating organizational unit of IEEE to help manage the activities of IEEE Sections to ensure that IEEE members are engaged in IEEE activities on the local level. All IEEE members are part of an IEEE Region. The boundaries of the Regions are specified in each Region's Bylaws.

- **SECTION**

  Established by the IEEE MGA Board, a Section consists of at least 50 IEEE members within a specific geographic area. A Section serves a vital role within IEEE by serving as the local IEEE presence for IEEE members. An IEEE Section serves the public by promoting the IEEE mission (Fostering Technological Innovation and Excellence for the benefit of humanity). The Section also serves the members by conducting activities which promote the MGA Mission (Inspire, Enable, Empower and Engage Members of IEEE). A Section contributes to the professional growth and development of their members by establishing professional and social networks. Through these activities, the Section and the member can form a collaborative relationship in which both the member and IEEE benefit.

- **TECHNICAL CHAPTER**

  An IEEE Technical Chapter is the local unit of an IEEE Technical Society or an IEEE Technical Council formed by a Region, one or more Sections, or a Geographic Council. The purpose in forming a Technical Chapter within a Geographic Unit is to meet the technical needs of the members within the geographic boundaries of the Section(s). Technical Chapters provide a valuable opportunity for local members to network with their peers and enable them to improve their personal and professional growth. IEEE Technical Society Chapters conduct activities within the scope of the technical field of interest of the sponsoring Society/Societies. IEEE Technical Council Chapters shall conduct activities within the technical field of interest of the Technical Council

  A Chapter shall comprise a minimum of 12 IEEE voting members of a Society, or group of Societies in the case of a joint chapter, and shall be established by petition to the parent geographical and technical organizational units concerned to fulfill the mission of IEEE.

- **AFFINITY GROUP**

An IEEE Affinity Group is a non-technical unit of an IEEE Organizational Unit formed by a Region, one or more Sections, or a Geographic Council. The purpose in forming an Affinity Group within a Geographic Unit is to meet the needs of the members of similar interest who are concerned with fulfilling the mission of IEEE. Affinity Groups provide a valuable opportunity for local members to network with their peers and enable them to improve their personal and professional growth. An Affinity Group shall be required to maintain a membership of not fewer than 6 members and to hold not less than two group-interest meetings per year, or to maintain a level of activity acceptable to the Section/Council Chair(s) and Region Director.

3.1.2.1 Working Group to develop Standard

It is possible to activate a workgroup for develop a standard. IEEE Standards are developed using a time-tested, effective and trusted process that is easily explained in a six stage lifecycle diagram.

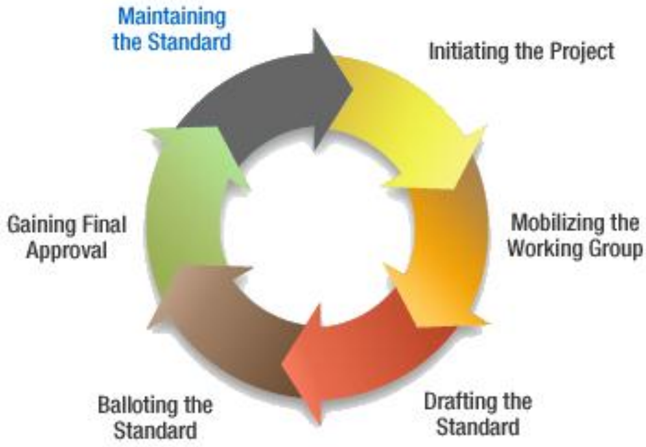

Figure 1: Standard Lifecycle

Initiating the Project and Mobilizing the Working Group

Working Groups are open groups. They are comprised of individuals for individual standards projects or representatives from entities (such as corporations, government agencies or academic institutions) for corporate standards projects. All participating in working groups have technical expertise, knowledge and dedicated interest in the technology being standardized in the standard. Working Groups meet and make technical decisions in the process of developing standards. Those participating in working groups have strong technical knowledge and expertise in the subject matter of the standard project, and understand and respect diverse points of view.

With Project Authorization Request (PAR) approval, a Working Group is defined and it can officially begin its work to develop or write the standard. In short, Working Groups work to create and write the standard. Overall, Working Groups strive for broad representation of all interested parties and encourage global participation.

Usually before the PAR is officially approved by the IEEE-SA (Standard Association) Standards Board, the foundation of the Working Group has been formed via collaboration with colleagues during the identification of the need for a proposed standard and in creating the PAR for submittal. Study groups - which consist of potential working group participants who have gathered to work on the PAR, to gain support of their potential sponsor and to study the need for the standards- can also serve as the foundation of a Working Group.

Once a PAR is approved and the working group can officially begin its work to develop the standard, sometimes to garner more expertise and to ensure representation from all impacted parties and/or balance among the industries affected by the standard, a call for participation is issued. Call for participation is usually coordinated with the IEEE-SA Media Contact.

Drafting the standard

The first milestone for many Working Groups is finishing their first complete draft. One of the ways to start is to break the document down into segments or sections. First, a scope and purpose is prepared based on the PAR information. The scope and purpose should be kept in mind at all times, since this will be what the IEEE-SA Standards Board will be evaluating the document against. Next, an outline is created. Often, this outline will also serve as the structure for the standard as well. The subjects in the outline will become the clauses and sub-clauses in the document. This outline should be thoroughly reviewed against source materials and Working Group ideas to ensure that it is conclusive. Then the Working Group should work to fill in the outline. Often, this is done by splitting up the work among Working Group members. One of the challenges in splitting up the work is the potential for inconsistency of tone in the document as a result. One way to avoid this problem is to remember to use standards verbs (shall, should, and may) as the primary means of conveying the tone of the document. Standards primarily use "shall," recommended practices primarily use "should," and guides primarily use "may". Remember, however, that this is not an exclusive definition. Standards can use "may" every once in a while, just as guides can use "shall". Indeed, this kind of use is almost inevitable. What needs to be attained is an overall consistency of tone. The overall tone is mandatory, so consistency in the use of verbs, and the use of proper standards verbs, can help to achieve an even tone in the document. One other aspect of standards writing can be confusing for Working Groups is the use of the word "must". The word "must" is not a defined standards verb in standards organizations. Therefore, the mandatory nature of a statement with "must" in a standard could be called into question in a court of law, and there would be no existing practice or rules to back up its meaning (keep in mind what was discussed earlier, the quasi-legal nature of standards and the need for a clear understanding of a standard's intent). For this reason, "must" should be avoided unless it is being used in a descriptive fashion (if it is raining, the sky must be gray). Stick to the defined standards verbs for the sake of clarity between you and the users of your standard.

Another good preparatory step is to examine the related publications area, in order to avoid duplication of available work. Every draft version of a standard has to be labelled with the appropriate copyright notices. One brief notice appears on every page of the standard. The other appears at the beginning of the document. These notices are crucial to guarantee copyright protection and should not be overlooked.

To help Working Groups in the editing and preparation of their document, the IEEE-SA has a professional staff of editors. The IEEE-SA editor is a member of the IEEE Standards staff and does not necessarily have a technical background. However, a staff editor does many things both before and after standards approval.

Balloting the standard – Final approval and maintenance

Before a draft standard is approved, the editor will review multiple drafts during development of a standard to provide global and specific editorial comments. The major review —Mandatory Editorial Coordination (MEC) —is conducted at the time the document goes to ballot. MEC ensures those basic elements of the document, such as draft labelling; the title, scope, and purpose matching the PAR; and copyright statements and releases are all handled properly in the draft.

After a standards project is approved by the IEEE-SA Standards Board, the editor prepares the final text for publication. The editor works with the Working Group chair and/or the technical editor to create a professionally produced standard.

It is important to note that although the editor can provide comments or suggestions to the committee based on technical items in the standard, he or she cannot make technical changes. Editors make grammatical, structural, and stylistic changes that do not modify the meaning or the technical integrity of the document.

Balloting begins when the Sponsor decides the draft of the full standard is stable. The Sponsor forms a balloting group containing persons interested in the standard. While anyone can contribute comments, the only votes that count toward approval are those of the eligible members of the balloting group. IEEE-SA membership is required to sponsor ballot on standards (ballot or vote on the standards outside of the working group). Balloting is a balanced process that prevents any one group or company from dominating. The IEEE-SA Standards Board approves or disapproves standards based on the recommendation of its Standards Review Committee (RevCom). This committee makes sure working groups follow all procedures and guiding principles in drafting and balloting a standard. As with PARs, completed draft standards come before the Board four times a year or during the continuous approval process. After approval, the standard is edited by an IEEE-SA editor, given a final review by the members of the working group, and published.

A standard is valid for ten years from its approval date. During this time, a working group can develop and ballot revisions or extensions to the standard, which are appended as amendments. After ten years, a standard is revised or withdrawn.

Regarding IEEE standardization, nSHIELD aims at contributing with a well-defined SPD metrics catalogue and the procedures for the management of the SPD properties through the whole SPD application lifecycle. The continuous process improvement approach of IEEE will benefit from a well-defined SPD framework in the field of embedded systems. As matter of fact, currently, there are no IEEE standards for the nSHIELD concepts. Some of the existing and active standards candidates to become “SHIELD compliant” are cover software verification and validation, lifecycle and architecture. Some of them are the following:

- **1012-2012 - IEEE Standard for System and Software Verification and Validation:** Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs. V&V life cycle process requirements are specified for different integrity levels. The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces. This standard applies to systems, software, and hardware being developed, maintained, or reused [legacy, commercial off-the-shelf (COTS), non-developmental items]. The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes documentation. V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.
- **829-2008 - IEEE Standard for Software and System Test Documentation:** Test processes determine whether the development products of a given activity conform to the requirements of that activity and whether the system and/or software satisfy its intended use and user needs. Testing process tasks are specified for different integrity levels. These process tasks determine the appropriate breadth and depth of test documentation. The documentation elements for each type of test documentation can then be selected. The scope of testing encompasses software-based systems, computer software, hardware, and their interfaces. This standard applies to software-based systems being developed, maintained, or reused (legacy, commercial off-the-shelf, Non-Developmental Items). The term "software" also includes firmware, microcode, and documentation. Test processes can include inspection, analysis, demonstration, verification, and validation of software and software-based system products.
- **12207-2008 - IEEE Systems and software engineering -- Software life cycle processes:** This International Standard establishes a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry. It applies to the acquisition of systems and software products and services, to the supply, development, operation, maintenance, and disposal of software products and the software portion of a system, whether performed internally or externally to an organization. Those aspects of system definition needed to provide the context for software products and services are included. Software includes the software portion of firmware. This revision integrates ISO/IEC 12207:1995 with its two amendments and was coordinated with the parallel revision of ISO/IEC 15288:2002 (System life cycle processes) to align structure, terms, and corresponding organizational and project processes. This standard may be used stand alone or jointly with ISO/IEC 15288, and supplies a process reference model that supports process capability assessment in accordance with

ISO/IEC 15504-2 (Process assessment). An annex provides support for IEEE users and describes relationships of this International Standard to IEEE standards.

- **982.1-2005 - IEEE Standard Dictionary of Measures of the Software Aspects of Dependability**: A standard dictionary of measures of the software aspects of dependability for assessing and predicting the reliability, maintainability, and availability of any software system; in particular, it applies to mission critical software systems.
- **1061-1998 - IEEE Standard for a Software Quality Metrics Methodology:** A methodology for establishing quality requirements and identifying, implementing, analysing and validating the process and product software quality metrics is defined. The methodology spans the entire software life-cycle.
- **42010-2011 - IEEE Systems and software engineering -- Architecture description:** ISO/IEC/IEEE 42010:2011 addresses the creation, analysis and sustainment of architectures of systems through the use of architecture descriptions. A conceptual model of architecture description is established. The required contents of an architecture description are specified. Architecture viewpoints, architecture frameworks and architecture description languages are introduced for codifying conventions and common practices of architecture description. The required content of architecture viewpoints, architecture frameworks and architecture description languages is specified.

This lack makes necessary the activation of specific workgroups and standards.

3.1.3 European Telecommunications Standards Institute (ETSI)

The ETSI produces globally-applicable standards for ICT, including fixed, mobile, radio, converged, broadcast and internet technologies. All about ETSI, membership, news and events, services, standards, technologies and ETSI portal can be found on http://www.etsi.org/WebSite/homepage.aspx. The ETSI is recognised as an official European Standards Organisation by the European Union, enabling valuable access to European markets.

3.1.3.1 ETSI standards

On the ETSI portal you can find the following standards and activities:

Table 2: ETSI Structure

GA	**BOARD**	**FC**	**IPR**	**OCG**	**NUG**	3GPP	AERO	ATTM
BRAN	BROADCAST	CLOUD	DECT	EE	eHEALTH	EMTEL	ERM	ESI
HF	INT	ITS	LI	M2M	MCD	MSG	MTS	PLT
RRS	RT	SAFETY	SAGE	SCP	SES	STQ	TETRA	TISPAN
USER	ISG AFI INS ISI LIS MOI OEU ORI OSG QKD SMT	NSO	STF	WORKSHOP				

There are four main groups:

1. ETSI Technical Committees/ETSI Projects
2. ETSI Partnership Project
3. ETSI Special Committees
4. Industry Specification Groups

In the last decade a rapid development of nanotechnologies, micro and nanoelectronics is showing that Embedded System Devices (ESDs) are penetrating in many different projects presented in Figure 2. Therefore, there are many ETSI standards in which the research topics addressed in nSHIELD are important and vice-versa there are many security, privacy and dependability issues already considered in some ETSI standardisation activities. So, the nSHIELD partners have a strong interest to identify in which projects we can contribute with the nSHIELD research results.

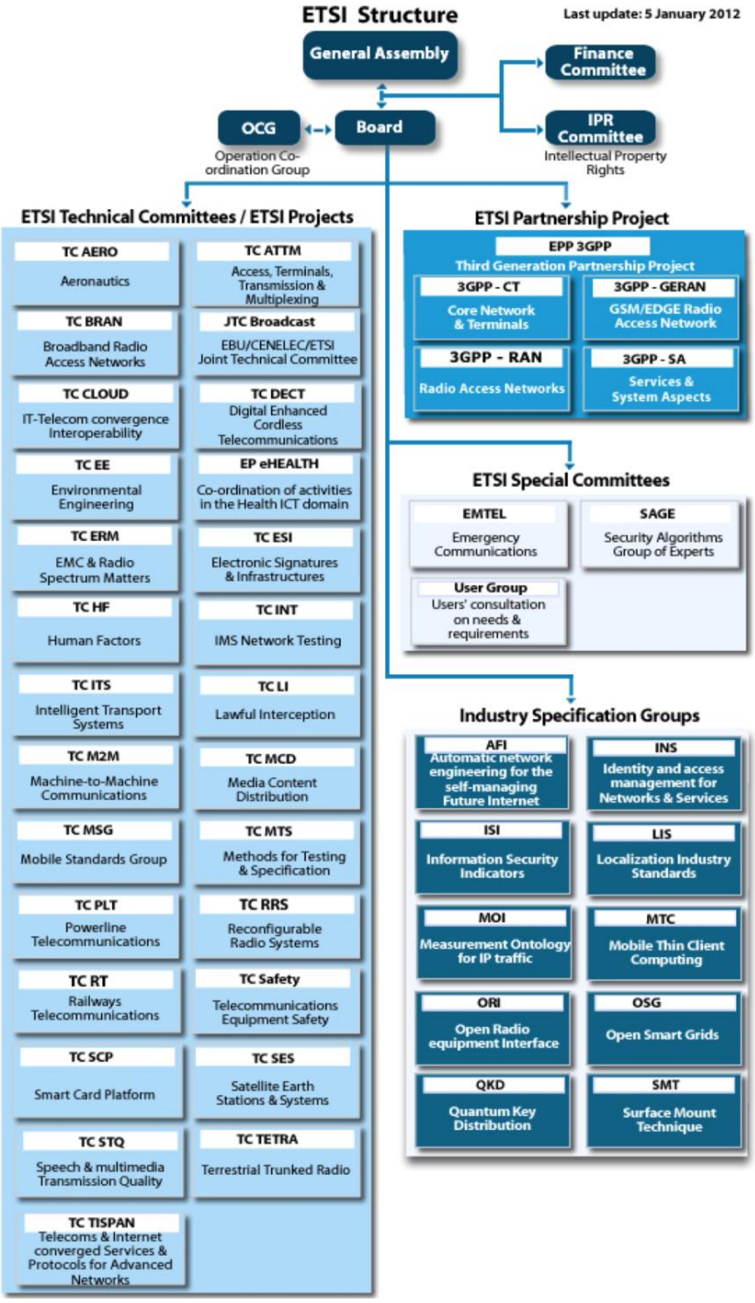
ETSI Structure
Last update: 5 January 2012
General Assembly
Finance Committee
OCG
Operation Co-ordination Group
Board
IPR Committee
Intellectual Property Rights
ETSI Technical Committees / ETSI Projects
TC AERO
Aeronautics
TC ATTM
Access, Terminals, Transmission & Multiplexing
TC BRAN
Broadband Radio Access Networks
JTC Broadcast
EBU/CENELEC/ETSI Joint Technical Committee
TC CLOUD
IT-Telecom convergence Interoperability
TC DECT
Digital Enhanced Cordless Telecommunications
TC EE
Environmental Engineering
EP eHEALTH
Co-ordination of activities in the Health ICT domain
TC ERM
EMC & Radio Spectrum Matters
TC ESI
Electronic Signatures & Infrastructures
TC HF
Human Factors
TC INT
IMS Network Testing
TC ITS
Intelligent Transport Systems
TC LI
Lawful Interception
TC M2M
Machine-to-Machine Communications
TC MCD
Media Content Distribution
TC MSG
Mobile Standards Group
TC MTS
Methods for Testing & Specification
TC PLT
Powerline Telecommunications
TC RRS
Reconfigurable Radio Systems
TC RT
Railways Telecommunications
TC Safety
Telecommunications Equipment Safety
TC SCP
Smart Card Platform
TC SES
Satellite Earth Stations & Systems
TC STQ
Speech & multimedia Transmission Quality
TC TETRA
Terrestrial Trunked Radio
TC TISPAN
Telecoms & Internet converged Services & Protocols for Advanced Networks
ETSI Partnership Project
EPP 3GPP
Third Generation Partnership Project
3GPP - CT
Core Network & Terminals
3GPP - GERAN
GSM/EDGE Radio Access Network
3GPP - RAN
Radio Access Networks
3GPP - SA
Services & System Aspects
ETSI Special Committees
EMTEL
Emergency Communications
SAGE
Security Algorithms Group of Experts
User Group
Users' consultation on needs & requirements
Industry Specification Groups
AFI
Automatic network engineering for the self-managing Future Internet
INS
Identity and access management for Networks & Services
ISI
Information Security Indicators
LIS
Localization Industry Standards
MOI
Measurement Ontology for IP traffic
MTC
Mobile Thin Client Computing
ORI
Open Radio equipment Interface
OSG
Open Smart Grids
QKD
Quantum Key Distribution
SMT
Surface Mount Technique

Figure 2: The ETSI structure.

Some relevant standards for nSHIELD are:

- 3GPP
- TISPAN
- PLT
- RRS
- RT
- CLOUD
- SAFETY
- ITS
- SAGE
- M2M
- SCP
- eHEALTH
- AERO

In the following paragraphs we are selecting some of the ETSI standards that have an influence on the research activities, architectural choices, Embedded System (ES) designs for the nSHIELD SPD networks and devices. It is important to select these relevant standards from the point of view of:

1. the application scenarios, and
2. key research topics in nSHIELD.

3.1.3.2 The nSHIELD Scenarios

SMN scenario

Some key ETSI standardisation activities and standards that are important for the SMN scenario are selected. The research activities on SDR/Cognitive and micro SPD nodes, and a WSN composed of such nodes are considered for contributions in the following ETSI standards and target projects.

3.1.3.2.1 Reconfigurable Radio Systems

Reconfigurable Radio Systems (RRS) is a generic concept based on technologies such as Software Defined Radio (SDR) and Cognitive Radio (CR). These systems exploit the capabilities of reconfigurable radio and networks for self-adaptation to a dynamically-changing environment with the aim of improving supply chain, equipment and spectrum utilization, as well as SPD functionalities targeted in nSHIELD.

The nSHIELD focus on SDR/Cognitive node and smart transmission is in line with a global interest in RRS solutions. It is being fuelled by the rapidly-growing demand for wireless communications for a wide range of purposes, as for example the SMN. With respect to the forecast of 7 trillion wireless devices serving 7 billion users in 2017, we definitely need more flexible ways to share radio networks and frequencies amongst multiple services and radio networks. RRS technologies offer the solution. With respect to this there is a worldwide interest for the so called "cognitive radio technologies".

CR is quite a new concept and could be said in short as a radio

- with learning capabilities, i.e.
- a radio able to obtain the knowledge of radio operational environment and adjust its operational parameters and protocols accordingly.

It is clear that such an approach has got undoubtedly a lot of benefits in terms of spectrum efficiency and this is much more important when the spectrum is scarce. Thus, there is great interest in CR technologies at European level as well as worldwide. Although CR must not be necessarily based on SDR, it is clear that SDR can be considered as one possible enabler of CR Technology and so the two technologies are definitely complementary from this perspective. The CR and SDR might have some regulatory aspects to consider and this is currently under investigation in different fora, i.e.:

- 3GPP TSG RAN
- CEPT ECC
- Cognitive Networking Alliance (CogNeA)
- European Communications Office (ECO) SE43
- IEEE (SCC41, 802.22 WG)
- ITU-R
- Joint Research Centre (JRC)
- Object Management Group (OMG)
- RSPG
- SDR Forum
- The Mobile Industry Processor Interface (MIPI)
- SAFECOM

3.1.3.2.2 Intelligent Transportation Systems

Figure 3 illustrates an Intelligent Transport Systems (ITS) that includes telematics and all types of communications in vehicles, between vehicles (e.g. car-to-car), and between vehicles and fixed locations (e.g. car-to-infrastructure). However, ITS are not restricted to Road Transport - they also include the use of information and communication technologies (ICT) for rail, water and air transport, including navigation systems.

In general, the various types of ITS rely on radio services for communication and use specialized technologies. Such new technologies are important for nSHIELD. For four application scenarios, we have to demonstrate that the nSHIELD technologies will have an important influence on ITS. These scenarios are rail transportation and SMN.

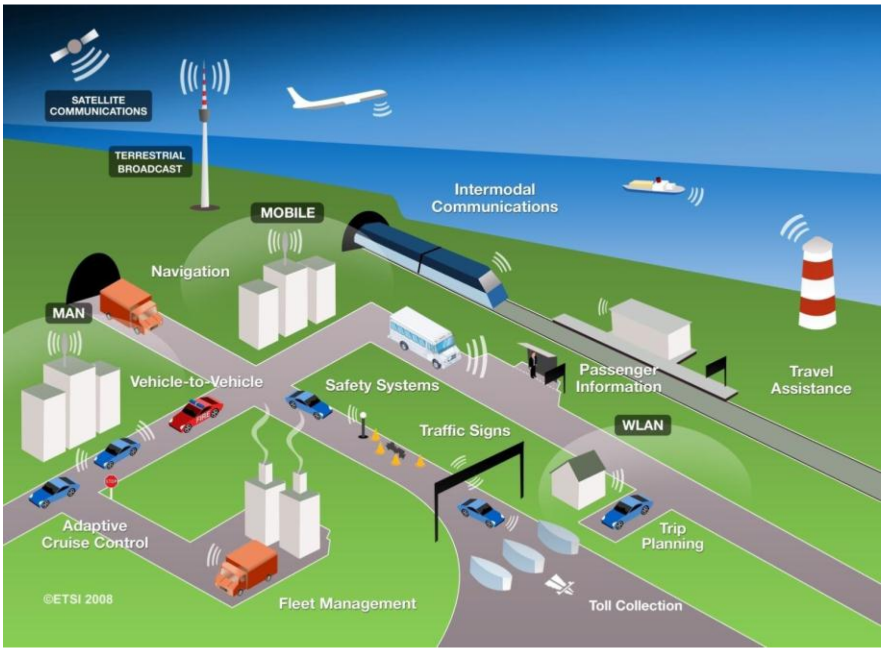

Figure 3: ITS vision (source: ETSI).

Figure 3 illustrates the communication architecture as it is presented in EN 302 665. The right hand side of this figure present the entity "Security" which provides security services to the OSI communication protocol stack, to the security entity and to the management entity. "Security" can also be considered as a specific part of the management entity.

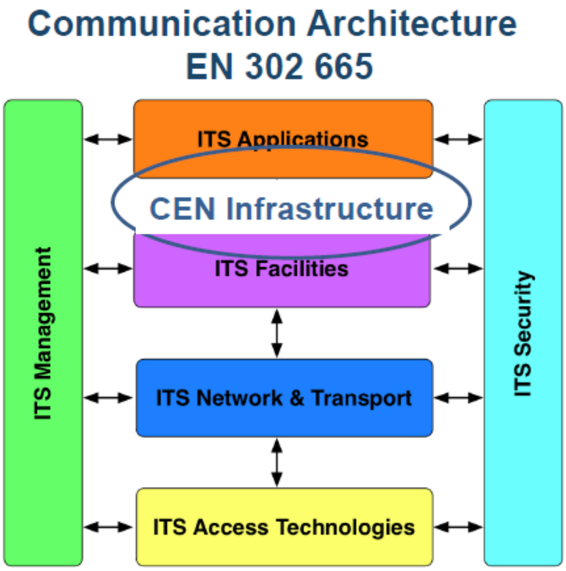

Figure 4: ITS communication architecture as in EN 302 665 (source: ETSI).

3.1.3.2.3 Machine-to-Machine communications

Thanks to Machine to Machine communications (M2M) standardisation activities all applications relevant to personal health monitoring, intelligent tracking and tracing in the supply chain (e.g., rail transportation), smart utility metering, remote control of vending machines, industrial wireless automation, ambient assisted living and mobile networking are made possible. The future telecoms networks may need to be optimised to cater for the new ‘subscribers', who may have very different behaviour from current customers. To achieve this, standardisation is required in order to deliver cost-effective M2M solutions. Many component-level standards already exist. They are addressing various radio interfaces, different meshed or routed networking choices, or offering a choice of identity schemes. Each is optimised for a particular application scenario and there is therefore a degree of fragmentation. Until now, insufficient effort was made in order to bring all these pieces together, and identify the standardisation gaps which exist. This is a challenge that ETSI is now confronting! It is also a challenge for nSHIELD framework which is based on one common network architecture for different applications and scenarios, because we have a strong emphasis on the SPD functionalities, SPD nodes, SPD networks and SPD core services.

Leading industry players participating in ETSI's Technical Committee for M2M (TC M2M) have now developed a set of standards which provide **a complete horizontal service layer for M2M communications**.

The ETSI M2M Release 1 standards enable the integration of different M2M technology choices into one managed platform. ETSI M2M Release 1 is built upon proven and mature standards from ETSI and other bodies such as the IETF, 3GPP, the Open Mobile Alliance and the Broadband Forum. The business benefits are clear: reduced complexity of M2M deployments, reduced deployment time for new M2M services, and ultimately reduced CAPEX and OPEX. The ETSI M2M standards specify architectural components including M2M devices, gateways with associated interfaces, applications, access technologies as well as the M2M Service Capabilities Layer. They also offer security, traffic scheduling, device discovery and lifecycle management features. The ETSI M2M Release 1 standards are published as a set of three specifications which are available for download from the ETSI website:

- Requirements in ETSI TS 102 689
- Functional architecture in ETSI TS 102 690
- Interface descriptions in ETSI TS 102 921

Embedded Devices (EDs) will be widely used in the future M2M. Therefore, it is important to consider the above mentioned documents in an early development phase of nSHIELD, i.e., in preliminary system requirements and specifications, preliminary system architecture and SPD metrics, node, network, middleware and overlay designs.

3.1.3.2.4 Security and Privacy

The increasingly rapid evolution and growth in the complexity of new systems and networks like nSHIELD, coupled with the sophistication of changing threats and the presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of ICT systems and networks. **To minimise exposure to risks, security must be built in from the beginning when designing new architectures, not added on later as an optional feature**. This demand opens the door for ETSI standardisation contributions. The nSHIELD project offers new opportunities for original and innovative contributions.

Therefore, as a response to such challenges, **Information Security standards are essential to ensure interoperability among systems and networks, compliance with legislation and adequate levels of security**. These standards provide the means for protecting the user, creating a more secure and profitable environment for the industrial sector, from SMEs to large global companies, and providing benefits for a diverse range of interest groups that include government organisations, research bodies and universities.

Each year, in January, ETSI organises a Security Workshop in its premises in Sophia Antipolis, France, attracting a large number of experts from all over the world. This is an excellent opportunity for nSHIELD dissemination activity, because these events are highly appreciated for the quality and relevance of the presentations, many of them focusing on standardisation issues. Additionally, the nSHIELD partners have valuable co-operation opportunity, because it helps to set the direction for future standardisation work, in line with the requirements of ETSI Members.

In recent years the discussions have focused increasingly on the broad issue of security innovation, and the role that security standards can and should play in such context. Speakers are selected from a call for contributions, which is announced at [20].

Each of the ETSI Security Workshops so far has featured many expert speakers, representing organisations that include ETSI, CEN, CENELEC, European Commission, ENISA, ITU-T, ISO, NIST as well as the private sector, governments, universities and research bodies, including the European Commission's Joint Research Centre.

Security in RRS

The activity of research and standardisation of RRS security must resolve a broad range of issues, which spans from software assurance, conformance to spectrum regulations and certification. We already demonstrated in the pSHIELD project many important SPD issues for ESs and EDs that will be used as nodes in the SPD network. As a general rule in nSHIELD, RRS must validate the communication security requirements of conventional communication systems like Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization. CIAA (Confidentiality, Integrity, Authenticity and Availability) concept described in pSHIELD will be elaborated with new functionalities that are typical for RRS. This is a consequence of the general conformance to standards and regulations already defined for the wireless communication systems, with which RRS must interoperate.

A major security issue introduced by RRS is the consequence of its reconfiguration capability. Theoretically RRS terminals or nodes should be able to download from the air interface new configuration profiles or software modules. With respect to SW and HW limitation of the nSHIELD nodes, we will have different cognitive and/or SDR features. However, once activated, the new profile or software module will change RRS radio transmission parameters like frequency, power and modulation types or SPD parameters. For example, RRS can use this capability to improve the spectrum usage efficiency and interoperability with the Radio Access Technology (RAT) present in the area, and to enhance SPD features. This capability presents two main security issues:

1. who guarantees that the downloaded profile or software module comes from a trusted source and can be activated on the RRS terminal?
2. who guarantees that the downloaded profile or software module will behave as expected?

One inherent requirement is that ETSI RRS needs to adopt the concept of Software Assurance in Information Technology, requiring

- a certification process to guarantee that the software modules to be downloaded and activated will behave as expected,
- a secure download mechanism, which guarantees the authenticity of the downloaded software. This should be completed by components in the RRS terminal in order to verify the software modules,
- a secure execution environment in the RRS in order to guarantee that only trusted software can be activated and executed,
- a component to ensure that spectrum regulations will be validated regardless of the software modules running on the RRS terminal.

Security in ITS

ETSI's TC for ITS is responsible for the production and maintenance of standards in order to support the development and implementation of ITS communications and services across the network, for transport networks, vehicles and transport users. The ITS approach to security is the following:

- Determine risk
- Minimise risk
- Manage risk
- Offer risk assurance

Security is a combination of technology and process. There are two extremely important issues:

- **Design for Assurance**: Ensuring that security provisions can be measured and evaluated
  - "Common Criteria (CC) for Security Assurance Evaluation (SAE)" published as ISO 15408 and ETSI EG 202 387
- **Privacy by Design**: adopt practices throughout the design, implementation and operation that maximises the privacy
  - identify data leakage
  - address the human element in system deployment
  - address the policies of the system users, maintainers & managers
  - finally consider end of life data disposal

Overview on CC documents

- *ISO/IEC 15408-1: Introduction and general model*

  ISO/IEC-15408-1 provides a general overview of the Common Criteria evaluation model. It defines a range of security terms within the CC context, describes the model itself, identifies what results are expected from an evaluation and, in its normative annexes, and specifies the content of a PP and an ST.

- *ISO/IEC 15408-2: Security functional requirements*

  ISO/IEC 15408-2 specifies a formal set of security functional requirements which together describe the security behaviour expected of a Target Of Evaluation (TOE). These requirements, summarized in annex A, are defined as a catalogue of components and classes which can be extended and specialized to suit particular TOE applications.

- *ISO/IEC 15408-3: Security assurance requirements*

  ISO/IEC 15408-3 describes the evaluation process by defining a set of evaluation classes and specifying the actions of an evaluator. Guidance on meeting the CC evaluation requirements is given in clause 6 of the present document.

ETSI standards in the evaluation of CC

Evaluation in the context of ISO/IEC-15408 is a test of the product against a set of defined security criteria. It is not a test that the product functions completely and correctly but a test that the product meets the security-related claims made for it. As such, this type of testing is similar to the conformance testing which is normally specified for all protocol standards. However, it is possible that interoperability testing (or a combination of conformance and interoperability testing) may be a more appropriate means of evaluating security criteria. Further details of the methods involved in the development of test specifications for both conformance and interoperability can be found in ISO/IEC 9646 and TS 102 237-1.

Privacy

Why ITS privacy is so important?

- V2V broadcast messages cannot be encrypted, thus the content cannot be controlled
- There is no formal agreement between sender and receiver in place
- In the USA, V2V safety applications are considered as a mandatory system
- ITS privacy is not like, say mobile phones:
  - can be turned off
  - privacy agreement between user and provider in place

Privacy objectives:

- Anonymity
  - There should be no pointer to any real-world identity (e.g. VIN, license plate number, owner name, static IP address, etc.).
- Long-term unlinkability
  - It shall not be possible to link transmissions from the same vehicle over a long time period (e.g. link two transmissions broadcast on different days).

ITS privacy in Europe:

- In Europe, ITS must respect and comply to the European Data Protection Directive
- However, it is unclear how to apply European Data Protection Directive to ITS stations in V2V mode
  - E.g., how often do we need to change certificates to satisfy the directive?

Privacy concerns can be found in most network layers

- Payload
- Communication headers
- Security overhead
- Security authorities

Perfect privacy is not possible (if revocation is required). Therefore a reasonable privacy-by-design is required. Both Europe and USA include privacy-by-design. However, neither was tested legally. More research is useful, for instance there is no accepted privacy metric to compare different approaches.

Future work in ITS will extend from the early work to cover media other than 5.9 GHz and therefore incorporate the mechanisms from IP, 3G and other technologies to the security suite of ITS. In the area of malware prevention this will take the work of ETSI TC ESI in particular for the application of signed certificates and apply it to secure distribution of software to the ITS Station (ITS-S).

This short overview on the ETSI TC ITS in domain of security and privacy are relevant for nSHIELD SPD metrics. Taking in consideration the existing ETSI documents on security and privacy is a first step towards new advanced technology solutions targeted in nSHIELD. By identifying the gaps of the existing security and privacy solutions in ITS, it is possible to find out how to implement the new SPD solutions.

Security in M2M

ETSI TC M2M specifies a telecommunication technology independent Service Layer offering a wide set of generic functionalities to facilitate the deployment of vertical M2M applications, such as Smart Metering, fleet management or remote healthcare monitoring applications. TC M2M WG4 is in charge of the related security and privacy aspects.

In 2011 TC M2M published its release 1 deliverables which support mutual authentication, key agreement and optional secure connection establishment between the Service layers of the Devices/Gateways and the supporting network. The security may rely on the Access Network provided mechanisms when trusted, on secure channel establishment at the M2M Service Layer (e.g. using TLS), or on data security provided at the object level. One of the main challenges addressed by the TC M2M architecture relates to the bootstrapping of security credentials to a multitude of objects across various environments, potentially with different constraints in terms of computing resources. This is addressed in M2M release 1 by offering several options suitable for different scenarios.

We can see once again that the ETSI M2M activities in the domain of security and privacy are relevant for nSHIELD SPD metrics. Taking in consideration the existing ETSI M2M documents on security and privacy is a first step towards new advanced technology solutions targeted in nSHIELD. By identifying the gaps of the existing security and privacy solutions in M2M it is possible to find out how to implement the new SPD solutions.

On-going activities

Release 2 of TC M2M specifications may extend this scheme to provide end-to-end (E2E) security to M2M applications, which is not covered in Release 1. This is an excellent chance to introduce an integrated concept of CIAA described in pSHIELD. TC M2M WG4 also provides specific inputs such as threat analysis to support the work in European standardisation mandates where TC M2M is involved.

Next Generation Networks

In the framework of nSHIELD it is planned that the communication services can be delivered over multiple specific technology platforms and received via a broad range of terminals (nodes). It is also in line with ETSI vision that the telecommunication services of the future will be delivered seamlessly over the most appropriate access network, with users roaming between domains and networks unaware of the underlying mechanisms that enable them to do so. **This opens the door to a new range of security and privacy risks**. How we are going to manage these risks in nSHIELD is one of the primary focuses of this project.

What do we need to take in consideration? First, the nSHIELD SPD network of networks (NoNs) cannot be an isolated network from other IP networks. Second, SPD network should be interoperable with other IP networks. Third, it should allow convergence with other IP networks. So, the new converged and access-independent network model - dubbed Next Generation Networks (NGN) - is based on the extensive use of IP, and is designed to accommodate the diversity of applications inherent in emerging broadband technologies. ETSI is already heavily committed to, and is well advanced in, developing the necessary standards to bridge disparate networks and domains and enable them to interoperate. The work on NGN is being managed by Technical Committee TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) and security is one of its core concerns.

Security, privacy and dependability must be built in from the beginning for the nSHIELD architecture. Therefore, we should take in consideration the recommendations form the available ETSI and world standards. For example, TC TISPAN established the security requirements for the subsystems of NGNs in its first version (NGN Release 1) of the general network and service specifications for the convergence between the traditional public switched telephone networks (PSTNs) and the new IP-based networks. In addition, TC TISPAN has produced a set of Security Design Guides which should be followed in the design of any new component of the network. This work references the guidelines on the use of the CC for the evaluation of IT security (ISO/IEC 15408). The publications deal with the issue of the application of the CC framework in the ETSI standardisation process and the development of protocols and architecture standards. They describe the way to map the CC framework drivers onto the process of defining a new standard, from the *a priori* definition of the purpose, the environment and the acceptable level of risk, to the actual definition of the subsystems, modules and protocols that constitute the standard.

Finally, behind RRS, ITS and M2M standardisation activities of ETSI, the NGNs security, privacy and dependability issues becomes more and more important in the scope of nSHIELD framework. Therefore, nSHIELD approach to SPD functionalities, SPD metrics, and SPD core services can be isolated form the ETSI standards, systems and architectural solutions. Our goal is to find way out how to implement new nSHIELD innovative technologies in NGNs. This is possible if and only if one nSHIELD SPD networks can converge with NGNs and if such a network will allow interoperability with the NGNs.

On-going activities

TISPAN WG7 has work in progress in various areas for the security of the NGN, by updating previously published deliverables and working on the following new ones: WG7 works in close collaboration with TC LI to publish a specification on Data Retention (DR) for the NGN. As already done for Lawful Interception, this document on Data Retention will include a mapping to the handover capabilities defined in TC LI for DR. WG7 started a new TR on Smart Metering TVRA and Security Requirements. Measures need to be in place to ensure public acceptance of smart metering data security and privacy safeguards, so that consumers can be confident that their data is secure. Due account will be taken of work in other Standard Developing Organisations (SDOs) and ETSI TCs.

Other security issues

Over the years, ETSI has produced numerous standards, specifications and reports covering generic security aspects including [21] - [34]:

- a comprehensive glossary for security terminology ([21] and [26])
- a guide for the selection and application of basic security mechanisms ([28] and [32])
- a guide for ETSI Technical Committees on the inclusion of security features in their Technical Specifications and Reports ([24] and [25])
- a guide to specifying requirements for cryptographic algorithms ([22], [23], [29],[31] [30] and [31])
- a report providing guidance to the availability and use of methods for the development of ETSI security standards ([34]).

In addition, to maintain coherence and co-ordination within ETSI, the Institute has produced documents offering an overall assessment of work done in the field of security ([27] and [33]).

3.1.3.2.5 ETSI recent and future events

- Year 2012:
  - **Conference:** International ETSI Model-Based Testing User Conference (MBTUC) 2012
    25 – 27 September , 2012, Tallinn, Estonia
  - **Plugtest**: RCS VoLTE Interoperability Event 2012
    1-12 October, 2012, Slovenia / China

- **Workshop**: 3rd ETSI TC M2M Workshop
  24-25 October 2012, Sophia Antipolis, France
- **Plugtest**: Global IPv6 Transition Test Event
  12-15 November 2012, Beijing, China
- ETSI Workshop on Energy Efficiency
  20-21 June 2012, Genoa, IT
- Business Opportunities in ICT Standardisation: an ETSI Workshop for SMEs 11 April 2012, Madrid, ES
- EU-US Electronic Signature workshop
  9 February 2012, McLean, USA
- 4th ETSI TC ITS Workshop
  7 - 9 February 2012, Doha, Qatar(FR)
- 7th ETSI Security Workshop
  18 - 19 January 2012, Sophia Antipolis (FR)

- Year 2013:

  - **Workshop**: 8th ETSI Security Workshop
    16 - 17 January 2013, Sophia Antipolis, France

  - **Workshop**: 3rd ETSI Workshop on Future Networks
    19 -21 March 2013, Sophia Antipolis, France (tbc)

3.1.4 Object Management Group (OMG™) – CORBA

The Common Object Request Broker Architecture (CORBA) is a widely-accepted, standardized system integration framework based on distributed object technologies. CORBA is focused on facilitating general computing environments and does not explicitly address the needs of responsive (fault-tolerant, real-time) computing. Therefore, the question remains how to extend today's CORBA implementations for support of responsive computing.

An increasing number of applications are being developed using distributed object computing (DOC) middleware, such as CORBA. Many of these applications require the underlying middleware, operating systems, and networks to provide dependable end-to-end quality of service (QoS) support to enhance their efficiency, predictability, scalability, and reliability.

The Object Management Group (OMG) has addressed many of these application requirements individually in the Real-time CORBA (RT-CORBA), Fault-tolerant CORBA (FT-CORBA) and security CORBA (CORBASec) specifications. Though the implementations of RT-CORBA are suitable for mission critical commercial or military distributed real-time and embedded (DRE) systems.

The usage of FT-CORBA with RT-CORBA implementations is not yet suitable for systems that have stringent simultaneous dependability and predictability requirements.

Security, Privacy and Dependability are the attributes that will make an nSHIELD compliant embedded system a winner in the market. In order to achieve this result nSHIELD should respect worldwide accepted standard as CORBA. Moreover nSHIELD shall support the improvements that CORBA should have as the simultaneous use of FT-CORBA, RT-CORBA and CORBASec. In fact, problems as Semantic Incompatibilities between RT-CORBA and FT-CORBA Features, lack of Standards to handle Partial Failures, lack of Standard QoS Semantics could be ideally resolved using these three standards simultaneously. As today, these three CORBA specifications are incompatible. The nSHIELD consortium shall interact with the OMG with an exchange of information in order to address the incompatibility.

The need to develop dependable middleware to support distributed real-time embedded systems (DRE) has therefore motivated research on policies and mechanisms for fault-tolerant CORBA

Distributed real-time and embedded (DRE) systems are playing an increasingly important role in many application domains, including telecommunication networks (e.g., high-speed central office switching), telemedicine (e.g., remote surgery), manufacturing process automation (e.g., hot rolling mills), and aerospace (e.g., avionics mission computing). Although there are many types of DRE systems, they have one thing in common: the right answer delivered too late becomes the wrong answer. Providing the right answer at the right time is therefore imperative for mission-critical DRE systems. nSHIELD effort at adding dependability to DRE systems focuses on developing and deploying standard CORBA middleware that can provide timeliness and performance guarantees to applications even when crash faults occur. nSHIELD consortium plan is to collect more empirical data in order to amortize the unpredictability in detection and recovery after a fault event. [8]

3.2 Interaction with other relevant standardization bodies and industrial fora

3.2.1 Global Platform

GlobalPlatform is a cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models [4].

As one of the technologies identified in the technology assessment stage of the project is the secure element technology, nSHIELD will deal with the work around this technology taking into consideration the potential relationship with GlobalPlatform specifications. Therefore the effort done during the project will be addressed towards the application of existing GlobalPlatform standard specifications as well as the improvement of these specifications.

3.2.2 Open Mobile Alliance

The Open Mobile Alliance (OMA) is designed to be the centre of mobile service enabler specification work, helping the creation of interoperable services across countries, operators and mobile terminals that will meet the needs of the user. To achieve this, the OMA addresses a holistic approach to the value chain of mobile services and applications, and drives service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms [4].

As indicated above, one of the technologies selected during the technology assessment process in the first phase in technical work package of the project is the secure element technology and specifically the planned work is focused on the mobile field. Therefore identifying the main specifications in this area and applying as well as improving the existing specifications aims to be one focal point for nSHIELD project.

3.2.3 Trusted Computed Group

Trusted Computing Group (TCG) [35], a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.

Given the fact that nSHIELD addresses issues dealing with trusted computing building blocks and software interfaces across multiple platforms, contributions to TCG will arise. In particular nSHIELD could give a substantial contribution on Trusted Platform.

3.2.4 ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Therefore identifying the main specifications in this area and applying as well as improving the existing specifications aims to be one focal point for nSHIELD project.

3.2.5 ITU-T Study Group 17

Within ITU-T, Study Group 17 coordinates security-related work across all study groups. One key reference for security standards in use today is the ITU-T Recommendation X.509 for electronic authentication over public networks. X.509, a cornerstone for designing applications relating to public key infrastructure (PKI), is used in a wide range of applications; from securing the connection between a browser and a server on the web, to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible.

Often working in cooperation with external SDOs and various ICT industry consortia, the study group deals with a broad range of standardization issues. To give only a few examples, SG 17 is currently working on cybersecurity, anti-spam, identity management, telebiometrics and IPTV security. Additionally, SG 17 is coordinating standardization work covering e-health, cloud computing and SmartGrid security, open identity trust framework, Near Field Communication (NFC) security, and Child Online Protection.

Development of the X.1500 CYBEX ensemble of techniques is a significant step towards enhancing cybersecurity globally. It provides a suite of techniques to facilitate the global information exchange demanded by Computer Incident Response Teams (CIRTs), and is a comprehensive collection of around forty draft ITU-T Recommendations.

Another achievement of SG17's is Recommendation ITU-T X.805, which will give telecom network operators and enterprises the ability to provide an end-to-end architecture description from a security perspective. Key players from telecom network operators, manufacturers and governments have defined the specifications that will alter the way companies look at their networks. The Recommendation will allow operators to pinpoint all vulnerable points in a network and mitigate them.

Most of nSHIELD’s activities in WP3 and more importantly WP4 relate to the fields of interest of SG17. The work within nSHIELD relating to secure communication, identity management and network monitoring as well as the improvements of existing protocols and mechanisms in these areas may bring significant contributions to the current standards and procedures for both the telecommunication organizations and government activities.

3.2.6 ISO/IEC Standard for Face Recognition

Facial recognition is a biometric-based technology that allows to automatically recognizing a person through a set of photographs of his/her face. The information acquired during the process can be adopted for further identification purposes and enables several applications, such as e-Passport, credit card payments, access control, identification etc., where security is an important aspect.

The reliability of a facial recognition system depends on the characteristic of the photographs of the face, which are influenced by several factors that, in turn, have an impact on the quality of the recognition process. The process adopted for photographs acquisition, the acquisition device and the biometric characteristics of a person play a major role in the performance of a facial recognition system.

Two standards have been introduced to regulate and normalize the data and the data acquisition process adopted during face recognition: ISO/IEC 19794 and ICAO.

ISO/IEC 19794 biometric standards describes interchangeable formats for several types of biometric data, provides guidelines for face image capturing and image quality and introduces a standard scheme for codifying data describing human faces within a CBEFF-compliant data structure. Furthermore, in order to enable applications that run on a variety of devices, including embedded systems, and to improve face recognition accuracy and reliability, the ISO/IEC 19794 specification describes also additional requirements that must be satisfied during data acquisition: scene constraints (lighting, pose, expression, etc.), photographic properties (positioning, camera focus etc.) and digital image attributes (image resolution, image size, etc.).

ICAO (International Civil Aviation Organization) specifies the guidelines on how photographs of face should be taken with a particular focus on the photograph that are used for travel documents.

These standards have been specifically conceived for computer analysis of face images in the following application areas:

- automated face identification (one-to-many searching),
- automated authentication (one-to-one matching),
- human identification of distinctive features used to verify identity and
- human verification of computer identification results.

The ISO/IEC 19794 standard defines four types of face image in order to introduce different categories that satisfy the needs of several application contexts. Each category must satisfy the requirements defined by the standard:

- Basic: this is the fundamental face image type that specifies on which all the other types are based. It defines a record format including header and image data. It doesn't specify a mandatory scene and is suitable for storage of the facial info, and is applicable to portraits for passport, driver license, etc...
- Frontal: it consists of an extension to the Basic type to conform to requirements appropriate for frontal face recognition. Two variants of the Frontal Face Image Type are defined:
  - Full Frontal: A Face Image Type that specifies frontal images with sufficient resolution for human examination as well as reliable computer face recognition. This type of face image type includes the full head with all hair in most cases, as well as neck and shoulders.
  - Token Frontal: specifies frontal images with a specific geometric size and eye positioning based on the width and height of the image. It requires less detail, which makes it suitable for less demanding applications.

The Full Frontal Type is adopted for face recognition in the user scenario that will be developed in this project.

The standard introduces categories of factors that affect the facial recognition systems performance as concerning the environment and the user (subject). In the acquisition and capture process of a face, elements such as variation of lighting and extreme or weak illuminations as well as camera characteristics (sensor resolution) play a role in performance. In example, current facial recognition standards for e-Passports allow for limited facial expressions and behaviour like closed eyes and subject position.

During the analysis of facial image quality different aspects have to be considered:

- This process must be performed on full frontal images with a resolution of 180 pixels of the width of the head or roughly 90 pixels from the eye to the centre.

- Lighting and background influences the quality and, in order to enhance machine-assisted face recognition performance, the photographs must be taken with a background with a grey plain smooth surface.
- No unnatural colour should be introduced. Grayscale photographs should be produced from common incandescent light sources. Colour balancing techniques should be used for colour photographs (high colour-temperature flask with standard film or tungsten-balanced film with incandescent lighting).

The behaviour of the person must satisfy specific indications regarding the behaviour of eyes (i.e., closed eyes are not admitted), closed or open mouth, face expression (i.e., smiling or neutral), head pose (i.e., frontal or rotated in any direction), presence of glasses, hair over eyes, hats or coverings, etc...

Finally, the standard defines also the best practices for face image data acquisition, in example:

- close-up of the head and shoulders so that the face takes up 70-80% of the photograph,
- in sharp focus and clear,
- the person should look directly into the camera,
- the person should have a natural skin tones,
- use appropriate brightness and contrast,
- use a plain light-coloured background,
- use a uniform lighting and not show shadow or flash reflections on the face
- avoid the presence of red eyes, etc..

The above specifications will be used as guidelines to develop the Human Identification Scenario based on Face and Voice Recognition.

3.3 Integration, interoperation and open source implementation

3.3.1 Real-time and Embedded Systems Forum

The Real-time and Embedded Systems Forum [36]. defines, coordinates, integrates and prioritizes real-time and embedded systems standards utilizing various existing architectural approaches. The Forum also defines test suites and certification programs for products adhering to these standards to enable the proliferation of conformant real-time and embedded systems.

This Forum is a focal point for real-time and embedded systems developers and customers, as well as other industry standards groups, and is working on:

- Profiles and Certification

  The main activities in this work area have been to establish a set of test and certification programs

- Security and MILS APIs

  Secure systems and real time, embedded systems are subject areas with many requirements, guidelines, and standards. Historically, real time systems designers have not included information security/assurance in their requirements. The forum interest area is the intersection of real time and security.

- Safety/Mission Critical Applications

Work with Commercial-Off-The-Shelf (COTS) component developers and system integrators to remove barriers for the use of COTS in safety-critical systems.

The Open Group is working with both COTS component developers and system integrators to remove barriers for the use of COTS in safety-critical systems. As a first step, The Open Group is preparing a Recommended Practice for the documentation and related services that a COTS vendor should provide with a product targeted to the safety-critical marketplace.

- Open Architecture

  The initial activity of this Working Group will be to develop a “coordinated' Open Architecture for Real-time and Embedded System environments that would be mutually beneficial for the various architecture approach(es) to include but not limited to the following -- DoD Joint Integrated Open Architectures, Navy Open Architecture, Air Force Viable Combat Aircraft Joint Council on Aging Avionics, Modular Open Systems Approach Interoperability Initiative, Army Weapon Systems Common Operating Environment and various open architectures from corporations and system integrators.

This forum is focused in real time ES and they are working, among other issues; they are working on secure systems for safety application. Both aspects will be studied in the scope of nSHIELD and also dissemination activities will include standardization of embedded systems (software) interfaces or services in a number of different domains (Real Time embedded systems, Data Distribution Systems etc.)

3.3.2 USB Implementers Forum

USB Implementers Forum Inc. [37], is a non-profit corporation founded by the group of companies that developed the Universal Serial Bus specification. The USB-IF was formed to provide a support organization and forum for the advancement and adoption of Universal Serial Bus technology. The Forum facilitates the development of high-quality compatible USB peripherals (devices), and promotes the benefits of USB and the quality of products that have passed compliance testing.

Some of the many activities that the USB-IF supports include to specify protocols by which a host computer may interact via and interface with Integrated Circuit(s) Cards (ICC) or Smart cards [38]. Taking into account that one point of interest of nSHIELD project is working with TPM and Smartcard for Trust ESs, the effort done during the project nSHIELD will be addressed towards the use of existing protocols as well as the improvement of these specifications.

3.3.3 EMSBC, European Multilaterally Secure Computing Base

European Multilaterally Secure Computing Base (EMSCB) [39], [40], aims at developing a trustworthy computing platform with open standards that solves many security problems of conventional platforms. The platform deploys, (a) hardware functionalities provided by Trusted Computing; (b) a security kernel based on a microkernel; and, (c) an efficient migration of existing operating systems.

In the sense of multilateral security, the EMSCB platform allows the enforcement of security policies of different parties, i.e., end-users as well as industry. Consequently, the platform enables the realization of various innovative business models, particularly in the area of nSHIELD interest, while averting the potential risks of Trusted Computing platforms concerning privacy issues. The source code of the EMSCB platform will be published under an open source license.

TOPAS works on providing the necessary framework for creating trusted – or trustworthy – personal devices, devices that are as familiar to their users as their mobile phones are and that can be used in security-relevant or sensitive application scenarios. The major objective of TOPAS is the development of a framework of Mobile Trusted Platforms that can be used on a variety of mobile and embedded systems, cost-effectively providing trusted computing technologies to these platforms, irrespective of the security features of the underlying system. nSHIELD work on the node side could contribute to this platform.

4 Conclusions

This document provides an overview over standard institutes being relevant for the nSHIELD project. It presented the standards and regulations for security, privacy and dependability. Having identified European directives following standards from CEN, CENELEC and ETSI the document provides then a short overview over the relevant norms and regulations.

The document then identified the standardization bodies and industrial fora, ranging from ISO/IEC via, IEEE, ETSI, CEN, CENELEC to the Object Management Group. A second focus in this chapter was the identified areas for interaction with the standardization bodies and industrial, as well as the connection towards open source implementations.

A number of nSHIELD partners have connections to standardization either as part of their group activities, as part of their industrial networks or as part of their implementation and validation activities. As an example, the Norwegian partners have co-founded the Internet of Things Value Network, where they consult in the steering board with other industrial members such as Telenor, Sintef, Statoil and Standards Norway. Through Standards Norway an analysis of the IoT standardization in ETSI, CEN and CENELEC is performed with the goal of identification of areas suitable to contribute.

A contribution to standards will then either come from collaboration with other industrial partners, or through direct involvement based on collaborative decisions on where to focus.

5 References

[1] http://www.cenelec.eu/

[2] ISO Press release, http://www.iso.org/iso/pressrelease.htm?refid=Ref1223

[3] Heru Susanto, Mohammad Nabil Almunawar & Yong Chee Tuan. Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Engineering and Computer Science. IJENS Publishers. 2011.

[4] GlobalPlatform, http://www.globalplatform.org/

[5] Open Mobile Alliance, http://www.openmobilealliance.org/default.aspx

[6] "ASSC - Evaluation of RTOS Systems". assconline.co.uk. March 1997. http://www.assconline.co.uk/documents/ASSC_Evaluation_of_RTOS_Systems_Report.pdf. Retrieved 2008-07-27.

[7] René L.C. Eveleens (2November 2006). "Integrated Modular Avionics - Development Guidance and Certification Considerations". National Aerospace Laboratory. http://ftp.rta.nato.int/public//PubFullText/RTO/EN/RTO-EN-SCI-176///EN-SCI-176-04.pdf.

[8] “Towards Real-time Fault-Tolerant CORBA Middleware”. Aniruddha S. Gokhale, Balachandran Natarajan Douglas C. Schmidt (Vanderbilt University) - Joseph K. Cross (Lockheed Martin Tactical Systems)

[9] IEEE standard and working Group: http://www.ieee.org/index.html

[10] Erika McCallister, Tim Grance, andKaren Scarfone, “Guide to protecting the confidentiality of personal identifiable information (pii)”, National Institute for Standards, NIST SP800-122, April 20120

[11] Were Oyomno, “Usable Privacy Preservation in Mobile Electronic Personality”, PhD thesis, Lappeenranta University of Technology, August 2012

[12] T. Erickson, “From Pim to Gim: Personal Information Management in Group contexts”, Commun. ACM, 49:74 -75, January 2006

[13] S. S. Al-Fedaghi, “How sensitive is your personal information?”, Proc. Of the 2007 ACM Symp. On Applied Computing, SAC’07, pp 165-169, ACM, New York, 2007

[14] E. Wolf, “Data Privacy and Product Liability in ITS as well as in Co-operative Systems”, Presentation to the CEN/TC278/ETSI TC ITS 3. WG Meeting 25-27. May 2010 in Berlin

[15] The historical dimension of privacy is well described in Wikipedia: http://en.wikipedia.org/wiki/Privacy (assessed 14. Juli 2012)

[16] Andrea DiMaio, ”Forget Privacy, It Is Just an Illusion”, http://blogs.gartner.com/andrea_dimaio/2009/09/28/forget-privacy-it-is-just-an-illusion/

[17] The European Union Data Protection Directive 95/46, http://www.dataprotection.ie/viewdoc.asp?docid=89 (retrieved 15 July 2012)

[18] ETSI security workshop, ”Security as a Business opportunity”, 16-17 Januar 2013, http://www.etsi.org/SECURITYWORKSHOP

[19] http://www.aviation-ia.com/standards/index.html

[20] http://www.etsi.org/SECURITYWORKSHOP

[21] ETSI ETR 232 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[22] ETSI TCRTR 037 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks"

[23] ETSI ETR 235 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks".

[24] ETSI TCRTR 038 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy"

[25] ETSI ETR 236 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy"

[26] ETSI TCRTR 028 (Network Aspects (NA)): "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

[27] ETSI TCRTR 029 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards".

[28] ETSI TCRTR 042 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[29] ETSI TCRTR 030 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

[30] ETSI ETR 234 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

[31] ETSI EG 200 234 (Network Aspects (NA)): "Telecommunications security; A guide to specifying requirements for cryptographic algorithms".

[32] ETSI ETR 237 (Network Aspects (NA)): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[33] ETSI SR 002 298: "Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"".

[34] ETSI TR 102 780: "Methods for Testing and Specification (MTS); Security; Guide to the use of methods in development of ETSI security standards

[35] Trusted Computing Group http://www.trustedcomputinggroup.org/

[36] The Open Group, http://www.opengroup.org/rtforum/

[37] USB Implementers Forum , http://www.usb.org

[38] USB approved Class Specification Documents http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf

[39] Towards Trustworthy Systems with Open Standards and Trusted Computing, http://www.emscb.com/

[40] Towards Trusted Computing for Embedded Devices, http://www.iaik.tugraz.at/content/research/trusted_computing /topas/