Pilot SHIELD

pilot embedded Systems
archItecturE for multi-Layer Dependable solutions

SEVEN FRAMEWORK
PROGRAMME

Project no: 100204

pSHIELD

pilot embedded **S**ystems arc**HI**tectur**E** for multi-**L**ayer **D**ependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems / Rail Transportation Scenarios

Real world requirements for SPD-based system

For the
pSHIELD-project

Deliverable D6.4

Partners contributed to the work:

ASTS, Italy
CS, Portugal
SESM, Italy
THYIA, Slovenia
SE, Italy
ETH, Italy
HAI, Greece

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

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Mariana Esposito	ASTS		
Francesco Flammini	ASTS		
Gareth May-Clement	CS		
Fabio Giovagnini	SESM		
João Cunha	SESM		
Przemyslaw Osocha	SESM		
Spase Drakul	THYIA		
Gordana Mijic	THYIA		
Marco Cesena	Selex Elsag		
Paolo Azzoni	Eurotech		
Nikolaos Pappas	HAI		
Reviewed by			
Name	**Company**		
Spase Drakul	THYIA		
Approved by			
Name	**Company**		

Modification History

Issue	Date	Description
Draft A	17/11/2011	First ToC proposal for comments
Draft B	20/01/2012	First draft
Final	28/01/2012	

Contents

Figures

Tables

This Page is intentionally left blank

1 Executive summary

The aim of this document is to guaranteeing the proposed Security, Privacy and Dependability (SPD) Node prototypes and pSHIELD network architectures in WP3, WP4 and WP5 to be future proof-of-concepts and to support real world requirements for industrial operations. Prototyping in industrial systems might address new and extended pSHIELD system requirements, which not have been addressed in the SPD focused requirement work in WP2. This document will summarize the experiences from the demonstration, including:

- Recommendation for real-life requirements from industrial implementation;
- Lessons-learned for the adaptation of lab prototypes towards quasi-autonomous Operations;
- Analysis of industry-readiness for pSHIELD-based monitoring.

Based on the real-world experiences and developed requirements and specifications in WP2, this document will further summarize recommendations for further industry-related developments of SPD node, network and its functionality.

The structure and content of the document are the following:

- Chapter 1 – Purpose of the document and its structure
- Chapter 2 – Brief introduction
- Chapter 3 – Real requirements for Nano/Micro Personal Node Prototypes
- Chapter 4 – Real requirements for FPGA node prototype
- Chapter 5 – Real requirements for Semantic model prototype
- Chapter 6 – Real requirements for Hardware and Software implementation of the prototypes

2 Introduction

In this document will be described the recommendations and lesson learned for a future standardization an industrial readiness of the prototypes. Based on these real-world experiences and requirements, the document will further summarize recommendations for further industry-related developments of SPD functionalities for the pSHIELD SPD nodes and network. The basic idea is to describe the hypothetical/verified limits for a real life implementation for the proof; the lesson learned for the adaptation of the prototype from the lab implementation to the real demonstration and the actual/future readiness for standardization and industrial implementation.

3 Nano/Micro Personal Node Prototype

3.1 Recommendations for real-life requirements from industrial implementations

3.1.1 Pervasive computing in pSHIELD

Pervasive Computing (PC) also called Ubiquitous Computing (UC) or together Ubiquitous and Pervasive Computing (UPC) is maturing from its origins as an academic research area to a commercial reality. In ubiquitous or pervasive ambient environment, simple and complex services are provided to users, according to their contexts, at anytime, anywhere, and using any available device. Dynamic composition of services for such environment plays an important role, because it composition aims to provide a variety of high level services[1]. Variety of PC nodes and concepts are proposed to accomplish with the UPC requirements. A key aspect of pervasive computing involves embedding sensing, networking and computation into everyday objects and everyday life processes. UPC is the trend towards increasingly ubiquitous connected EDs (Embedded Devices) in the environment. It is a trend about a convergence of advanced electronic, wireless technologies and the Internet. **UPC devices** are not PCs (Personal Computers) but very tiny and invisible EDs, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods that are communicating **through increasingly interconnected networks**. Among the emerging technologies expected to prevail in the UPC environment of the future are wearable computers, smart homes and smart buildings. The tools expected to support these are: application-specific integrated circuitry (ASIC), speech and gesture recognition, perceptive interfaces, smart matter, field programmable gate area (FPGA), system on a chip (SoC), and micro electromechanical systems (MEMS).

The pSHIELD SPD nodes require a Middleware to interface between the networking kernel and the end-user applications running on these ED devices. This pSHIELD middleware will mediate interactions with the networking kernel on the user's behalf and will keep users immersed in the pervasive computing space. The middleware will consist mostly of firmware and software bundles executing in either client-server and/or P2P mode (hybrid nature of the pSHIELD network). User interfaces are another aspect of middleware.

Recommendation no. 1: The pSHIELD system architecture based on the four functional layers (node, network, middleware and overlay) is conceptually designed for the development of software components that are reusable across the **pervasive computing applications**.

To achieve this is important to consider the variations and properties like **mobility**, **adaptability**, **composability**, and **context awareness** that may be required for different pSHIELD applications types. However, that various requirements and variations may not always be known a priori and hence developing all the multiple variants may not always be possible or feasible. **The term "composability" is widely used in pSHIELD, but for SPD is a property of a software component meaning that it may easily and systematically be combined with other components**. Composability of software components in pervasive computing is an important issue and has been given little attention. Therefore, in this document we will summarise the consortium effort for NMPS nodes tailored for ubiquitous connected EDs in the selected application environment to achieve a convergence in the pSHIELD SPD IP-based network, i.e., a hybrid heterogeneous network (HHN) of SPD & Legacy Nodes, and SPD & Legacy Networks.

[1] K. Tari et al. ," Context-aware Dynamic Service Composition in Ubiquitous Environment," IEEE ICC 2010 proceedings.

3.1.2 Wireless sensor networks

The pSHIELD network architecture for the railway application scenario, the concept of four functional layers with SPD functionalities and core services is a **homogenous network** as in Figure 2.2 of the Technical Annex. By introducing more implicational scenarios as in nSHIELD and Legacy ES nodes and Legacy ES Networks, the final architecture becomes a **hybrid heterogeneous network** (HHN). It is heterogeneous in the sense of coexistence different technologies (IEEE 802.15.4, IEEE 802.11, UMTS, etc., multi-frequency, multi- technology, multi-layer, multi-architecture) that are connected with unified control and optimisation, and it is hybrid in the sense of a network that is between a centralised and pure decentralised architecture. Figure 1 illustrates a WSN composed of Nano, Micro/Personal and Power Node which can be used also as a Gateway.

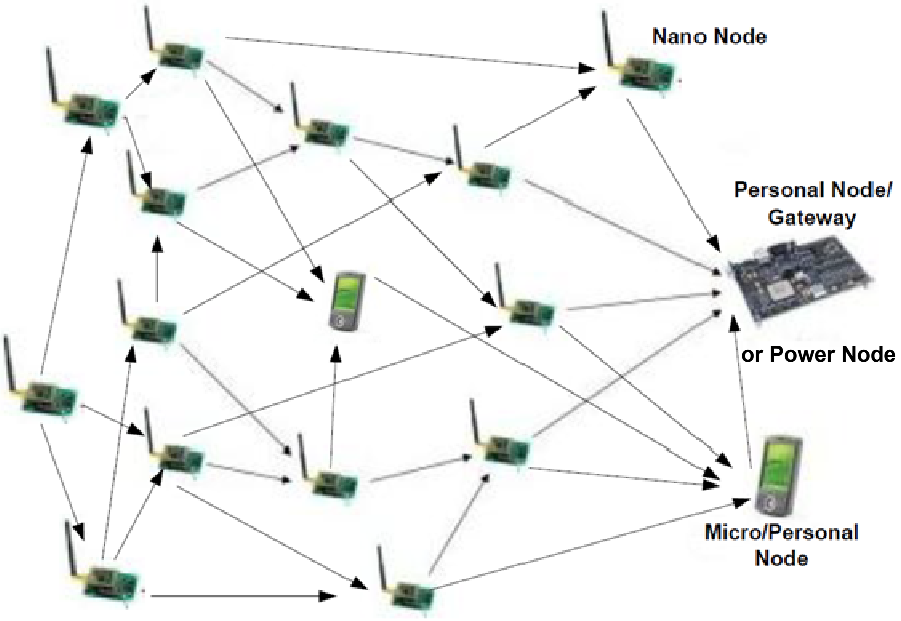


Figure 1 WSN composed of NMP and power nodes.

For example, in the pSHIELD network it can be designed to track wagons that pass through certain geographical areas up to the destination. Therefore, the network may switch between being a monitoring network (inside the wagons, or trains) and a data collection network (outside, railway road or railway track). During the long periods of inactivity when no monitored wagons are present, the network will simply perform the monitoring function. Each NMP or power node will monitor its sensors waiting to detect an alarm. Once an alarm event is detected, all or part of the network, will switch into a data collection network and periodically report sensor readings up to a GW that tracks the wagon. Due to this multi-modal network behaviour, it is important to develop a single architecture that can handle these application scenarios as well as other scenarios.

The final deliverables D2.1.2 (system requirements and specification) and D2.2.2 (system metrics) constrained the implementation architectural design of the NMP node on a system level with some particularities for each functional layer (node, network, middleware and overlay). D2.1.2 provides a set of system requirements specification starting with the application scenario and followed by the functional layers. D2.2.2 gives us two fundamental and complementary concepts for defining SPD metrics. However, for the pilot project we are concentrating upon the research effort on the WSNs because they are excellent candidates for many application scenarios. Therefore, the SPD metrics addressed in this document are related to WSNs and its nodes.

Recommendation no. 2: One standalone SPD-WSN composed of SPD nano, micro/personal nodes and/or legacy nodes that have pSHIELD node adapter with SPD functionalities represent the smallest possible pSHILED SPD network called sub-SPD-WSN.

3.1.3 Middleware

The sensor nodes for WSNs differ so much in terms of HW platforms. Writing an OS that runs on all these possible sensor platforms is impossible. To hide the underlying platform differences and to decouple the OS from HW platform a middleware is needed. **The concept of middleware in distributed systems is often taken to mean the software layer that lies between the operating system and the applications on each site of the system. It facilitates scalability, interoperability, deployment, and development of applications**.

Recommendation no. 3: The SPD-WSN should have middleware as software layer that lies between the operating system and the applications on each site of the system**.**

In the last decade numerous works on middleware for mobile devices (smart phones, tiny/mote nodes) are performed and successfully implemented. Most of those devices use operating systems like Windows CE, Palm OS, Symbian OS, Tiny Linux, etc. In this document we focus on middleware for NMP nodes, which are much smaller than those devices. The recent development of sensor node middleware is showing that we have quite a large number of middleware for WSNs. Most of the middleware we have studied are built on top of TinyOS. There are other OSs like Contiki, Mantis, SOS, and t-kernel. It is important to note that the scope of middleware for WSN is not restricted to the sensor network alone, but also covers external networks connected to the WSN (such as Internet) as well as the applications interested in querying sensor data through such external network. Standards such as 6LoWPAN (which used IEEE 802.15.4) and Web Services running directly on the sensor node allow integrating them into the **Internet of Things** (IoT). However, nodes which are capable to run the internet stack directly are either very expensive or not very energy-efficient. There have been several efforts to implement the Internet Protocol Stack on small energy-constrained devices. The LoWPAN and 6LoWPAN protocols try to port the IPv4 and IPv6 Protocols on small devices. This enables running services on the application layer directly on sensor nodes. The **Web service technology** is often used to connect and access sensors and actuators through the Internet. The recent middleware approaches use different technique. For example, such middleware are Sensorpedia (Web 2.0 based), TinyDB (Database oriented), Mate (Virtual Machine based), Agilla (Mobile Agent), TinyLime (tuple space) and TinyCubus (cross-layered).

Recommendation no. 4: The SPD-WSN should allow Web services and access its NMP sensors and actuators through a SPD node that act as Gateway to connect SPD-WSN on IP-based network.

Taking in consideration that pSHIELD SPD network is composed of SPD and Legacy Nodes it is obvious that we have a complex HHN structure where the standard OSI layers are defining the overall network requirements in sense of the HW & SW components. On the physical layer (PHY) different NMP nodes will coexist in the same pSHIELD network. Above PHY different protocol stacks for different Legacy NMP nodes are increasing the complexity of the overall pSHIELD network design. Figure 2 illustrates a standard Internet Layer Structure and Middleware for WSNs composed of SW components that adapt the PHY layer to the application layer.

Recommendation no. 5: The SPD-WSN may contain one or more legacy nodes that are not using pSHIELD node adapter.

The SPD-WSN composed only of NMP-SPD nodes or legacy nodes represent a homogenous sub-SPD-WSN or sub-WSN respectively.

Recommendation no. 6: The SPD-WSN may be designed as a hybrid heterogeneous network if it is composed NMP-SPD nodes and legacy nodes with or without pSHIELD node adapters with centralised and decentralised homogenous sub-SPD-WSNs or sub-WSNs.

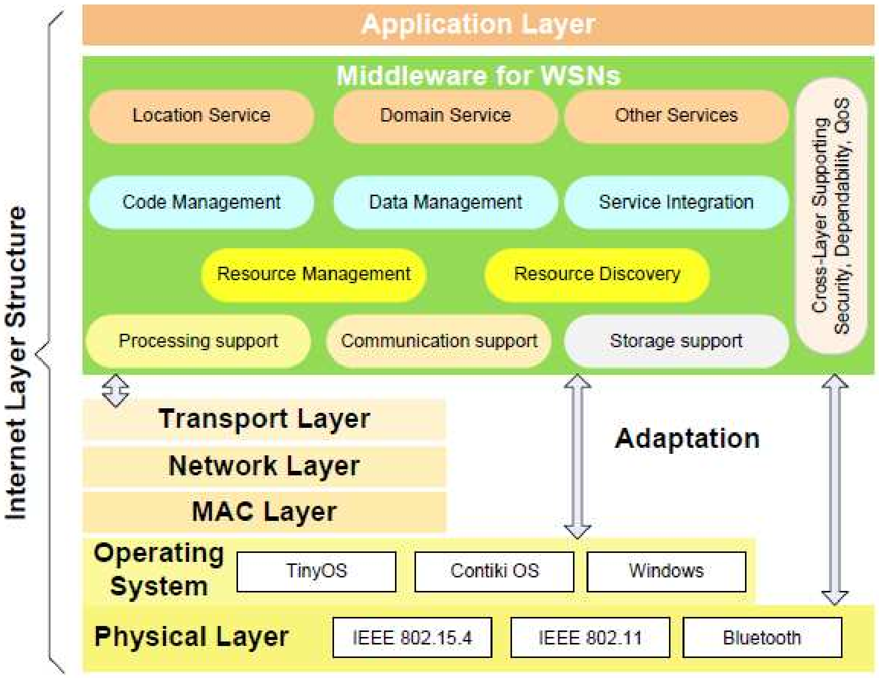


Figure 2 A reference model for middleware in WSNs.

Based on the requirements for NMPS nodes for WSNs and the main challenges in the development of adaptable middleware (as it is shown in Figure 2) a base for comparison of the following features is:

- **Code Mobility**: it evaluates the support of code mobility, both for update and installation of new services in a node;
- **Flexibility**: it evaluates the support for network scalability and support for manage incoming nodes in the network, as well as manage for the network topology;
- **Node Mobility**: it evaluates the support for mobile nodes in the network;
- **Node Heterogeneity**: it evaluates the capacity of the middleware address the needs of both low-end nodes, with few and constrained resources, as well as more sophisticated sensors, with more powerful computer platforms and advanced resources;
- **Application Knowledge**: it evaluates the ability of the middleware to respond the needs of specific applications or group of applications;
- **Data Fusion**: it evaluates the support for data aggregation and fusion by the nodes that are in the way of data moving from the phenomenon occurrence to the end user that requested the information;
- **QoS**: it evaluates the support for QoS control that can be provided by the middleware.

Recommendation no. 7: The SPD-WSNs should have code mobility, flexibility, node mobility, application knowledge, data fusion and QoS features.

By comparing some adaptable middleware[2] like DAVIM, ATLAS, AGILLA, IMPALA, SINA, TinyCubs, MiLAN, SensorWare, TinyLime, and AWARE, the conclusion that can be drawn by this analysis is that **there is a need to integrate the support for each of the described feature a common middleware platform in order to offer the required support for new emerging applications**.

[2] Pignaton de Freitas, "A Survey for Adaptable Middleware for Wireless Sensor Networks, Technical Report, 2008.

There have been also some efforts to architect middleware for WSNs using SOA (RUNES, P2PComp, etc). Service Oriented Architecture (SOA) can deal with aspects of heterogeneity, mobility and adaptation, and offers seamless integration of wired and wireless environments.

The OSGi (Open Services Gateway Initiative) is focused on the application layer. It is open to almost any protocol, transport or device layers. The OSGi mission is multiple services, wide area networks, and local networks and devices. The OSGi advantages are platform and application independent. The central component of the OSGi specification effort is the services gateway. Service semantics for WSNs is another important issue, in addition to the service definition, so that services can be coordinated in the space.

Hydra platform[3] is a new concept that is realized in such a way that between physical and application layer is a middleware. The main goal was to develop a middleware that is 'inclusive' which means that it will be possible to enable any device to be detectable and usable from a Hydra application. The concept is based on the work of Rozanski and Woods[4] , and the Hydra architectural descriptions are in line with the IEEE 1471 standard. For the NMP prototype platform design concept is described in D3.2. The Hydra middleware as in Figure 3 is a core technology that has a transparent communication layer, equally supporting centralised and distributed architectures. The Hydra middleware takes security and trust into account and allows building model-guided web services. It runs on wired or wireless networks of distributed devices with limited resources. The embedded and mobile service-oriented architecture will provide fully compatible data access across heterogeneous platforms, allowing true ambient intelligence for networked ESDs. Adding extended security, privacy, trust and new dependability modules may satisfy requirements for having a middleware that will be SPD composable with the rest of the pSHIELD system architecture and network. The Hydra middleware consists of large number of software components – or managers – that handle various tasks needed to support cost-effective development of intelligent applications for networked embedded devices.

Recommendation no. 8: Hydra middleware is an excellent candidate middleware technology for SPD-NMP Nodes that composed a SPD-WSN.

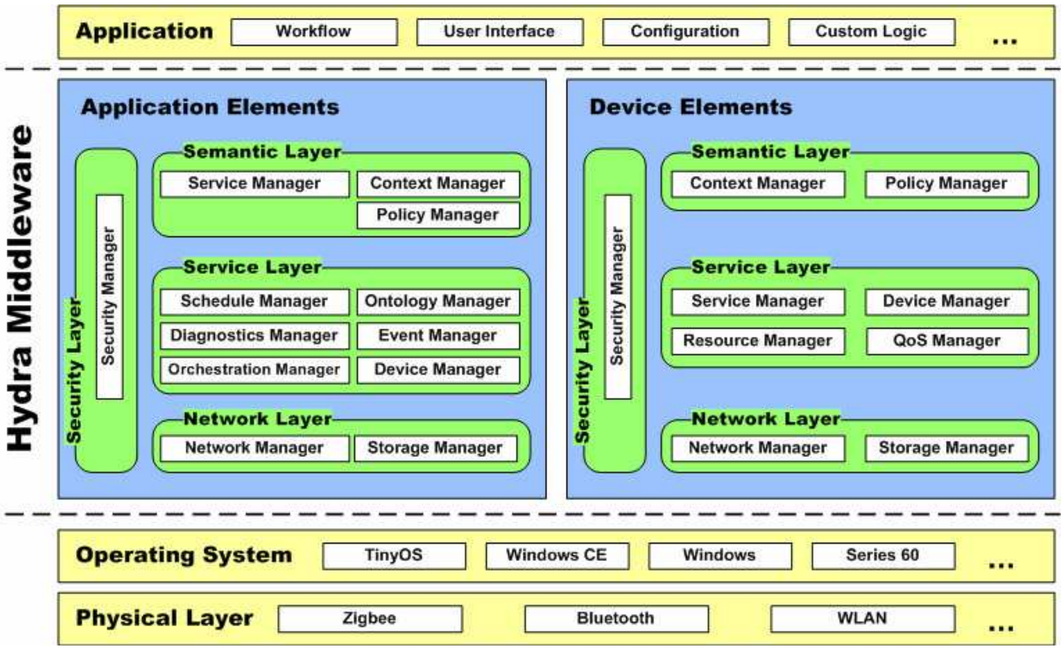


Figure 3 The Hydra middleware layer[5].

[3] http://www.hydramiddleware.eu/news.php

[4] Rozanski, N. and Woods, E. , “Software systems architecture: working with stakeholders using viewpoints and perspectives,” Pearson Education.

[5] Hydra project , D3.4, “Initial architectural design specification,” http://www.hydramiddleware.eu/articles.php?article_id=90

The biggest advantage of the Hydra middleware relies on the fact that allows developers to incorporate heterogeneous ESDs into their applications. This middleware can be incorporated in new and existing networks of distributed ESDs, which operate with limited resources: computing power, energy and memory. Additionally, Hydra-middleware provides easy-to-use web service interfaces for controlling any type of physical device irrespective of its network interface technology. Additionally, this **middleware is based on a semantic Model Driven Architecture for easy programming and incorporate service discovery, P2P communications and diagnostic**. In Hydra framework any physical devices, sensor, actuators or subsystem can be considered as a unique web service.

What we will need from Hydra middleware for the pSHIELD SPD nodes? **A lightweight version of this middleware, to be the Legacy Middleware Layer on top of which the pSHIELD middleware Adapter can host a set of Innovative SPD Functionalities: proper software modules must be added.** This solution is in line with the recent IP stacks that are lightweight enough to run on tiny, battery operated ESDs. This is also in line with emerging application space of smart objects that require scalable and interoperable communication mechanisms that support future innovations as the application space grows. This strategy is also aligned with the future application scenarios the **Internet of Things and Human** (ITH). **Smart objects** are small computers with a sensor and actuator and a communication device, embedded in objects. To support the large number of emerging applications for smart objects, the underlying networking technology must be inherently scalable, interoperable, and have solid standardization base to support future innovation.

Recommendation no. 9: The SPD-WSN middleware should allow semantic web services and ontology with an overlay SPD Layer that is responsible for cross-layer SPD functionalities and QoS.

3.1.4 Securing embedded systems

Figure 4 illustrates the security pyramid[6] with five primary abstraction levels for an embedded system.

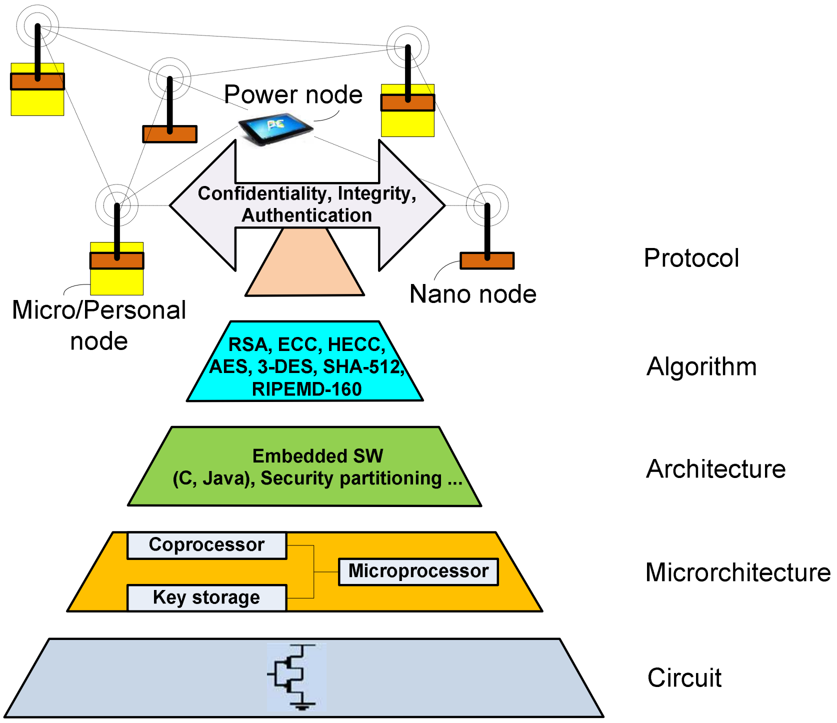

Power node
Confidentiality, Integrity, Authentication
Micro/Personal node
Nano node
Protocol
RSA, ECC, HECC, AES, 3-DES, SHA-512, RIPEMD-160
Algorithm
Embedded SW (C, Java), Security partitioning ...
Architecture
Coprocessor
Key storage
Microprocessor
Microrchitecture
Circuit

Figure 4 Embedded security pyramid.

[6] D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede. Securing Embedded Systems. In *IEEE Security and Privacy Magazine 4*, pages 40–49, 2006

The five abstraction levels are:

- **Protocol level** includes the protocols to be performed on embedded devices. For achieving security CIAA concept can be implemented.
- **Algorithm level** includes cryptographic primitives (such as Public Key, Symmetric Key crypto algorithms and hash functions) and application-specific algorithms used at the protocol level.
- ***Architecture* level** includes secure hardware/software partitioning and embedded software techniques to prevent software hacks.
- **Microarchitecture** deals with the hardware design of modules (the processors and coprocessors) required and specified at the architecture level.
- ***Circuit* level** requires implementing transistor level and package-level techniques to thwart various physical-layer attacks.

Protocol level is application specific and includes the design of protocols to be performed on EDs. The PKC (public key cryptosystems) are based on RSA[7] or DSA[8]. ECC (Elliptic Curve Cryptography) and Hyper-ECC (HECC) are based on different algebraic structure[9]. After 20 years of intensive investigation on both, theoretical and practical aspects it is evident that ECC and HECC offer equivalent security as RSA, but for much smaller key size! This result in smaller HW and lower power consumption that is extremely important for NMPS nodes. However, it is not enough to have strong cryptographic algorithms. It is also important their implementation that must be secured. The attacks techniques are related to the PHY implementation. For example, the attack can be active or passive. Active attack is performed in such way to alters HW or SW by changing the operating conditions (power supply, temperature, etc.) Passive attack is based on monitoring side-channel information (power supply, EM radiation).

With this short introduction on pyramid security approach for ESs is clear that all abstraction level must be secured. Of course, this is not limited only to security. The same strategy can be applied for Privacy and Dependability. This is a complex SPD approach, which can be extended to a general pyramid SPD approach for the future ESs. For the pilot pSHIELD project we focus mainly on the security aspects for ESs.

Recommendation no. 10: The networked SPD and legacy nodes of a WSN should be designed with SPD features on the circuit level, micro-architecture, and architecture, algorithm and protocol level.

3.1.5 Multidimensional metric space

This section considers the **SPD metrics** as in D2.1.2 and D2.2.2 with key security & dependability attributes: availability, reliability, safety, confidentiality, integrity and maintainability and the **system performance metrics** that are important for WSN applications such as computational time, memory size, energy consumption and cost. Additionally, authenticity attribute is very important for WSN.

The key metrics for wireless sensor networks are grouped for **SPD functions**

- security,
- privacy, and

[7] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978.

[8] A. Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[9] V. Miller. Uses of elliptic curves in cryptography. In H. C. Williams, editor, Advances in Cryptology: Proceedings of CRYPTO'85, number 218 in Lecture Notes in Computer Science, pages 417–426. Springer-Verlag, 1985, and
N. Koblitz. Elliptic curve cryptosystem. Math. Comp., 48:203–209, 1987, and N. Koblitz. A family of Jacobians suitable for Discrete Log Cryptosystems. In S. Goldwasser, editor, Advances in Cryptology: Proceedings of CRYPTO'88, number 403 in Lecture Notes in Computer Science, pages 94–99. Springer-Verlag, 1988.

- dependability,

and **basic functions**:

- lifetime,
- coverage,
- cost and deployment,
- response time,
- temporal accuracy, and
- effective sample rate.

These functions can be considered with the key aspects: threats, attributes and means in the main concept taxonomies: security, dependability, fault-tolerance, reliability and survivability (see D2.2.2 and D3.2). The importance of these functions is briefly discussed below. Many of these evaluation metrics are interrelated. For example, it may be necessary to decrease performance in one metric, such as sample rate, in order to increase another, such as lifetime. Taken together, this set of metrics form a multidimensional metric space (MMS) that can be used to describe the capabilities of a WSN and its nodes. The SPD capabilities of a prototype platform are represented by this MMS. A specific application deployment can be represented by a subset in this MMS. A system prototype platform can successfully perform the application if and only if the application requirements subset lies inside the capability of MMS.

Recommendation no. 11: The Multi-dimensional metric (MMS) space for NMP-SPD nodes of a SPD-WSN is composed of SPD (security, privacy, dependability) and basic functions (lifetime, coverage, cost and deployment, response time, temporal accuracy and effective sample rate).

Further details on security considerations, SPD metrics and design constrain are provided in D3.2.

3.1.6 Power supply source

As time goes by, Embedded Systems (ES) have improved more and more due to the systems integrated on a single chip are becoming more complex.

The first designs were slower and less energy efficient than current ones. For this reason, these versatile components had an urgent need for a better power supply design.

Current devices operate at lower voltages and higher currents than first models. Consequently, power supply requirements may be more demanding, requiring special attention to features deemed less important in past generations.

One of the basic requirements of a power supply for ES is to generate the necessary supply voltages in the best possible quality and a favourable electrical current which lets them make full use of their capabilities.

3.1.6.1 Power supply components

One of the phases of pSHIELD project is the design of intelligent ES platforms. Complexity is different depending on the kind of node:

- ***Nano node***: is the simplest model and consists of a small device with limited resources in terms of hardware and software. Nano nodes are small wireless sensors which are massively distributed in the environment. Due to this and also to their simplicity, these models don’t represent a guarantee in terms of SPD so they are feasible targets for attacks.

- ***Micro node***: goes a step further than “Nano node” in terms of hardware and software resources, network access capabilities, mobility, interfaces, sensing capabilities, etc.

Table 1 Power consumption of possible models of nano nodes.

Model	Description	Consumption	Input Voltage
GPS-330R	GPS receiver module (Interfaz USB)	< 45mA < 171mW	3.8V ~ 8V
iW-GPS-01	GPS receiver module (Interfaz USB)	< 111.5mW	3.3V
WRL-00582	Bluetooth module	<150mW	3.3V ~ 6V
AMBZ420	ZigBee module	<150mW	2V ~ 3.6V
SL030	RFID module	< 140mW	2.5V ~ 3.6V

Table 2 Power consumption of possible models of micro nodes.

Model	Description	Consumption	Input Voltage
eSPOT board	SunSPOT	70mA ~ 120mA	3V
eDEMO board	SunSPOT	400mA	3V
HTC 7 Trophy[10]	Smartphone	3mA ~ 236mA	-
Sony Ericsson Naite	Mobile phone	1.6mA ~ 221mA	-

To protect the systems against external attacks, it is important to design the properly power supply. These will focus on three key points:

- Study how to provide a continuous power supply source, without any cut in time or, at least, how to keep the system running during a period of time long enough to solve the problem with the main source or to send a warning to alert the person in charge.
- Design the appropriate protections to avoid system damages, including different operation modes to plug or unplug critical and non-critical sections of the nodes.
- Monitor the power consumption.

3.1.6.2 Power supply protections

Both micro and nano nodes, need a protection circuit to avoid problems related to over voltages, overloads, short circuit or over temperatures. Besides, it is important to include a mechanism to plug/unplug critical sections or disconnect any damaged sub-system.

For this proposal, a protection board has been designed. Figure 5 shows the schematic with all necessary components to achieve this goal.

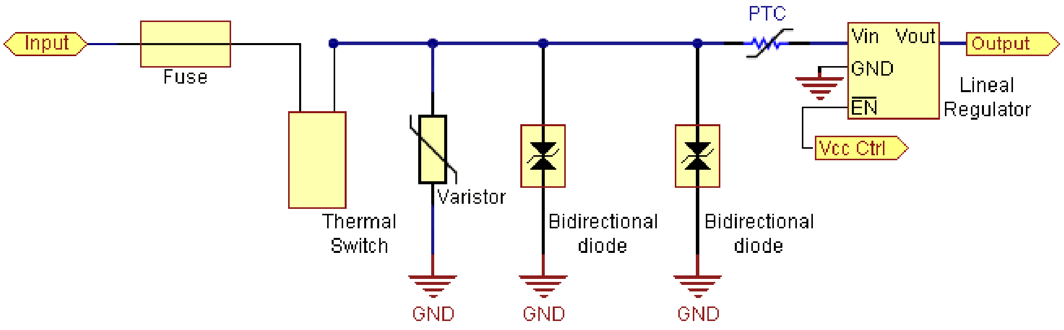


Figura 5 Protection circuit board – Nano and micro nodes.

[10] Power consumption in standby mode and 3G talking mode (HTC 7 Trophy and Sony Ericsson Naite)

- The ***Fuse*** is useful to protect the system against excess of current flow caused by an overload or a short circuit. When the current exceeds the rating of the fuse, an excess of heat is produced and the fuse blows out. From that moment on, all the components of the circuit are protected against over current.

- The ***Thermal Switch*** is a protection necessary to avoid damages when the system is working out of the defined operating temperature range. It is a thermostat which has an internal contact that will be opened every time the temperature exceeded the limits.

- The ***Varistor*** provides protection against high voltage transients as well as other surges produced by lighting, switching, electrical noise on AC or DC line, etc. These components can absorb high transient energies and can suppress positive and negative transients.

- The ***Bidirectional Transient Voltage Suppression Diode*** provides high overvoltage protection thanks to its instantaneous response to transient over voltages. This protection is needed to avoid damages related to electrostatic discharges or electrical over stress.

- The ***Linear Regulator*** maintains a constant DC output voltage and continuously holds the output voltage at the design value, regardless of changes in load current or input voltage (it is assumed that load current and input voltage are within the specified operating range)

- ***Vcc Ctrl*** is a signal that lets the system plug/unplug the sub-systems connected to the output power. Power protection board could include as many protection circuits as needed. Thus, it could be possible to maintain different power inputs and disconnect those damage sub-systems or the ones that could be working in a suspicious mode.

3.1.6.3 DC protection board

Two different protection boards have been manufactured. The first one is for a wireless platform which could have up to five different sub-systems connected. It will include not only the necessary protections to avoid damages into the circuit but also the hardware necessary to let the microprocessor controls the power supply of different sub-systems. To achieve this goal, five protection circuits, like the one showed in Figure 6, have been integrated in the protection board. To monitor power consumption, a current sense amplifier has been included in the design.

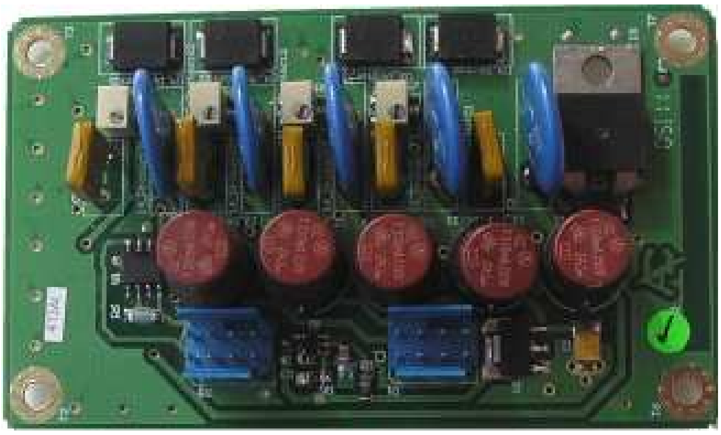


Figure 6 DC Protection board – power control and monitoring.

The second protection board (Figure 7) contains only the protections needed to avoid damages into the circuit. Both designs try to be a starting point in the design of a secure power supply for both pSHIELD and nSHIELD nodes.

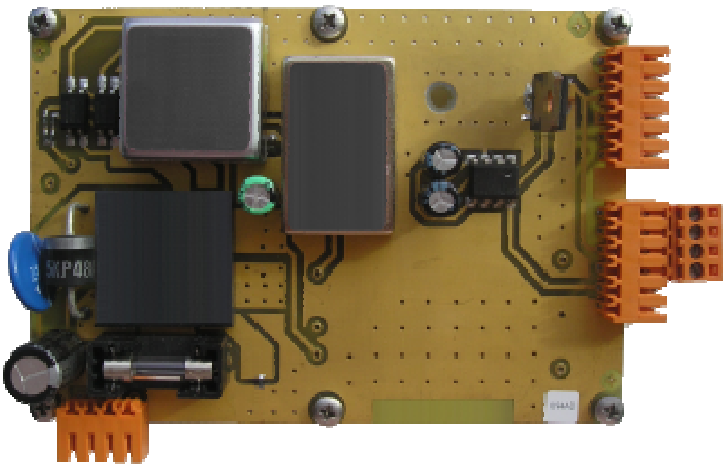


Figure 7 DC Protection board.

Recommendation no. 12: NMP-SPD nodes should have power-supply circuits with security and dependability features.

3.1.7 Elliptic curve cryptography for NMP nodes

A WSN is a wireless ad-hoc network consisting of resource-constrained sensor devices (limited energy source, low communication bandwidth, small computational power) and one or more base stations (Gateways). The Gateways (GWs) are more powerful and collect the data gathered by the sensor nodes so it can be analyzed. Routing is accomplished by the nodes themselves as any ad hoc network through hop-by-hop forwarding of data. Common WSN applications range from battlefield exploration and emergency rescue operations to surveillance and environmental protection.

Security and cryptography on WSNs meet several open problems even though several years of intense research. Given the limited computational power and the resource-constrained nature of the sensing devices, the deployment of cryptography in sensor networks is a difficult task. Aranha et al. s paper [2] presents the implementation of elliptic curve cryptography in the MICAz Mote, a sensor platform to develop optimizations specifically:

(i) the cost of memory addressing;

(ii) the cost of memory instructions;

(iii) the limited flexibility of bitwise shift instructions.

This work presents efficient implementations for arithmetic of binary field algorithms such as squaring, multiplication, modular reduction and inversion at two different security levels. These implementations take into account the characteristics of the target platform. The implementation of field multiplication and modular reduction algorithms focuses on the reduction of memory accesses and appears as the fastest result for this platform.

Finite field arithmetic was implemented in C and Assembly and elliptic curve arithmetic was implemented in Koblitz and generic binary curves. Here are obtained the fastest binary field arithmetic implementations in C and Assembly published for the target platform. Significant performance benefits where achieved by the Assembly implementation, resulting from fine-grained resource allocation and instruction selection. The performance of implementations is illustrated with timings for key agreement and digital signature protocols. Results strongly indicate that binary curves are the most efficient alternative for the implementation of elliptic curve cryptography in this platform.

Optimizations produced a point multiplication at the 160-bit security level under 1/3 of a second, an improvement of 72% compared to the best implementation of a Koblitz curve previously published and an improvement of 61% compared to the best implementation of binary curves. When compared to the best implementation of prime curves, is obtained a performance gain of 57%.

Therefore, ECC is becoming a powerful cryptographic scheme. Because of its efficiency and security is a good alternative to cryptosystems, like RSA and DSA, not just in constrained devices, but also on powerful computers. ECC is very important in the field of low-resource devices such as smart cards and Radio Frequency Identification (RFID) devices because of the significant improvements in terms of speed and memory compared to traditional cryptographic primitives (e.g. RSA). Memory is one of the most expensive resources in the design of embedded systems which encourages the use of ECC on such platforms. Security, implementation and performance of ECC applications on various mobile devices have been examined and it can be concluded that ECC is the most suitable PKC scheme for use in a constrained environment.

The remote client authentication can be implemented by the traditional public-key cryptography. The computation ability and battery capacity of mobile devices are limited, so traditional PKC, in which the computation of modular exponentiation is needed, cannot be used in mobile devices. Elliptic curve cryptosystem (ECC), compared with other public-key cryptography, has significant advantages like smaller key sizes, faster computations. Thus, ECC-based authentication protocols are more suitable for mobile devices than other cryptosystem. However, like other public-key cryptography, ECC also needs a public key infrastructure (PKI) to maintain the certificates for users' public keys. When the number of users is increased, PKI needs a large storage space to store users' public keys and certificates. In addition, users need additional computations to verify the other's certificate in these protocols.

Recommendation no. 13: Elliptic Curve Cryptography should be implemented on energy-constrained NMP-SPD nodes.

3.1.7.1 ECC in software trusted platform module

Trusted computing discussed earlier is an emerging concept that deals with information security concerns in a wide variety of computing systems. Trusted computing standards are driven by the computing and communications industries through the Trusted Computing Group (TCG). Hardware and software improvements to the target system are required for the usual approach to trusted computing, including the addition of a separate chip called the TPM that is attached to the target system.

The TPM provides capabilities for secure storage; secure reporting of platform configuration measurements, and cryptographic key generation. In addition the TPM chip implements tamper-resistance techniques to prevent a wide range of physical and hardware-based attacks.

Trusted computing has applicability to a wide range of embedded systems. Recent efforts to adapt trusted computing standards to resource-constrained environments include the TCG's Mobile Phone Working Group and the Trusted Mobile Platform Alliance. The hardware enhancements, including the addition of the TPM chip, may impose an overhead in the context of cost and size in resource-constrained embedded systems and this is not acceptable. For such systems, one option is to use a software-based TPM (SW-TPM), which implements TPM functions using software that performs in a protected execution domain on the embedded processor itself in order to enable the adoption of trusted computing techniques. It is also important to ensure that the computational and energy requirements for SW-TPMs are acceptable since many embedded systems have limited processing capabilities and are battery-powered.

In terms of protection against physical and hardware attacks SW-TPM is not completely equivalent to a conventional TPM chip. **SW-TPM can be executed within protected or isolated execution domains that are provided by embedded CPUs (*e.g.*, ARM TrustZone), and can utilize on-chip storage in order to provide a reasonable degree of tamper-resistance.** The question that arises is whether the computational and energy requirements to perform the TPM functions are acceptable. This is subject for the future study targeted for nSHIELD.

Recommendation no. 14: TPM or SW-TPM should be implemented on NMP-SPD nodes in order to guaranty enhanced security mechanisms in SPD-WSN.

3.1.7.1.1 SW-TPM implementation

The SW-TPM security features are very useful in many embedded systems! Some embedded systems cannot be augmented with a conventional TPM chip because of the area and cost constraints. Here, the feasibility of a SW-TPM is explored, which performs the same functions as a hardware TPM, *i.e.*, supports all the three roots of trust, as well as other cryptographic capabilities. Executing the SW-TPM in a protected execution domain of the CPU (*e.g.*, ARM Trust-Zone), and using on-chip memory, provides resistance to software attacks, including compromises of the OS, and a limited number of physical attacks.

The implementation of SW-TPM is adapted from the public domain TPM emulator, which provides basic TPM functions, such as RSA cryptography and HMAC and SHA-1 hashing functions, and provides several TPM commands.

The emulator has been changed as follows:

- **Random number generation**: A hash-complemented Mersenne Twister (MT) random number generator is used, *i.e.,* we run the output of MT through SHA-1.
- **ECC**: SW-TPM supports ECC in the binary field GF(2^m). ECC on this embedded platform is used because of its small key sizes compared to RSA for offering the same security robustness. Hence, it requires less resources such as processor cycles and energy. ECC-enabled SW-TPM supports key generation and validation, digital signature generation and verification, encryption, and decryption. Supported ECC key sizes are 224 bits (equivalent to 2048-bit RSA keys), 192 bits (not equivalent to RSA key), and 160 bits (equivalent to 1024-bit RSA keys).
- **AES_CBC cryptography**: SW-TPM supports the Advanced Encryption Standard (AES) algorithm, running in Cipher Block Chaining (CBC) mode. This engine is specifically used for ECC encryption and decryption, and for decrypting AIK credentials.

Recommendation no. 14: SW-TPM with ECC should be implemented on NMP-SPD nodes in order to guaranty enhanced security mechanisms in SPD-WSN.

More details on SW-TPM implementation are provided in D3.2.

3.1.8 NMP node: prototypes

This section provides details for the NMP node prototypes with small energy-constrained sensor nodes that form a WSN. Development platform will be designed in such a way to facilitate security enhancements discussed in previous sections 4, 5, 6 and 7. As it is already explained in previous sections to achieve security enhancements in WSNs is not an easy task for resource-constrained NMPS nodes.

For the application scenario, i.e., rail transportation of dangerous materials the best suited proof of the concept prototype is capability of a NMPS node to **maintain information integrity, confidentiality, authenticity and system integrity** by using symmetric or asymmetric key cryptography.

In the past decade lot of research work is dedicated for security enhancements like TinySec, SPIN, TinyPK, SERP, etc. Most of the work is related to the security and integrity of data transmission and less research effort is dedicated on protecting sensor nodes themselves. It is especially important for attacks initiated from wireless channels, which convert sensor nodes to malicious nodes by reprogramming them through radio channels. The malicious nodes can attack the WSN. For examples,

- take over a node and listen to the data being transmitted through the node,

- introduce corrupt data into the network,
- destroy the node by depleting the node resources,
- consume the energy of the WSN trough intentional broadcast.

A possible solution is monitoring integrity in WSNs. For that we need secure communication channels, which introduce additional security concerns. Aside from that, the main concern in WSN is integrity of NMPS nodes, since the widespread use of shared secrets, if any, in communication protocols is based on the assumption that nodes are not compromised. In literature, we can find different approaches for data and system integrity in WSNs. There is no solution that guaranty security for WSNs because they can be composed by different types of sensor nodes, networks and application scenarios. The same is true for privacy, trust and dependability attributes. Therefore, our SPD goal for the NMPS node prototypes is to take in consideration the following design constrains:

I. For RT scenario, which belongs also to critical infrastructure, high security of WSNs composed of secured NMPS nodes is compulsory.

II. NMPS nodes are energy and resources-constrained.

III. Secure ES firmware, secure boot, secure upgrade mechanisms, and TCG technologies are needed for enhancing security.

Recommendation no. 15: NMP-SPD nodes networked in a SPD WSN should guaranty at least confidentiality, integrity, authenticity and system integrity.

3.1.9 Development platform

Development platform has two separate prototypes:

1. NMPS node platform
2. TPM platform

The choice of the processor and memory performance is very important since the program memory sized defies performance (MIPS) and computational time (ms). Selection of all other components for both platforms is constrained with constrains I, II and III.

3.1.9.1 NMPS node prototype

Before we decided which type of tiny sensor node will well suited with the pSHIELD requirements we investigated many suitable solutions. Fig illustrates the most recent sensor platforms that can be used for NMPS node (generic sensing type or gateway). For video applications the current sensor node platforms are showing lack of processing power and memory sizes. Therefore, low-resolution image sensors are considered for NMPS node. Additional goals for the NMPS node are:

- The node should have the memory-performance size 100-1000 KB and 10-100 MIPS.
- WSNs will multi-tier type. For example Tier “0” is has nano nodes, tier “1” micro/personal nodes, and tier “2” more powerful micro/personal nodes as gateways, and tier “3” has power nodes.
- The NMPS nodes should be able to connect: low-resolution camera, passive infrared (PIR), acoustic/ultrasound, temperature, pressure, humidity, etc.
- It should have sufficient low power consumption when is used with a battery.
- It should allow a wide range of applications.

- USB interface for programming the applications and data retrieval.
- Separate USB interface will be for radio module.
- To connect the image sensor and other sensors an expansion connector is used.

Figure 8 illustrates the prototype architecture that we investigated. The expansion interface unit is used to connect and evaluated different NMPS node elements like sensors, TPM modules, etc. For example we investigated the image sensors: Agilent ADMC-1670 CIF, ADNS-3060 concurrently by using two independent UARTs and a shared SPI bus. In addition a reference camera from CoMedia C328R with VGA resolution from 80x60 to 640x480 is examined.

AT91SAM7S family offers RAM size of 8 – 64 kB and FLASH memory 32 – 256 kB. For an application if more RAM is necessary, a FRAM memory chip can be used. This is limited to 32 kB, but offer unlimited write/erase cycles ond no wait states when writing. For example, if a 2MB FLASH device was specified for 100.000 write/erase cycles with one 100 kB frame written every 10 seconds, the devices would be expected to fail after ~230 days.

Recommendation no. 16: One NMP-SPD node should be composed of sensors (analog and digital), camera(s), and a TPM and/or SW-TPM unit.

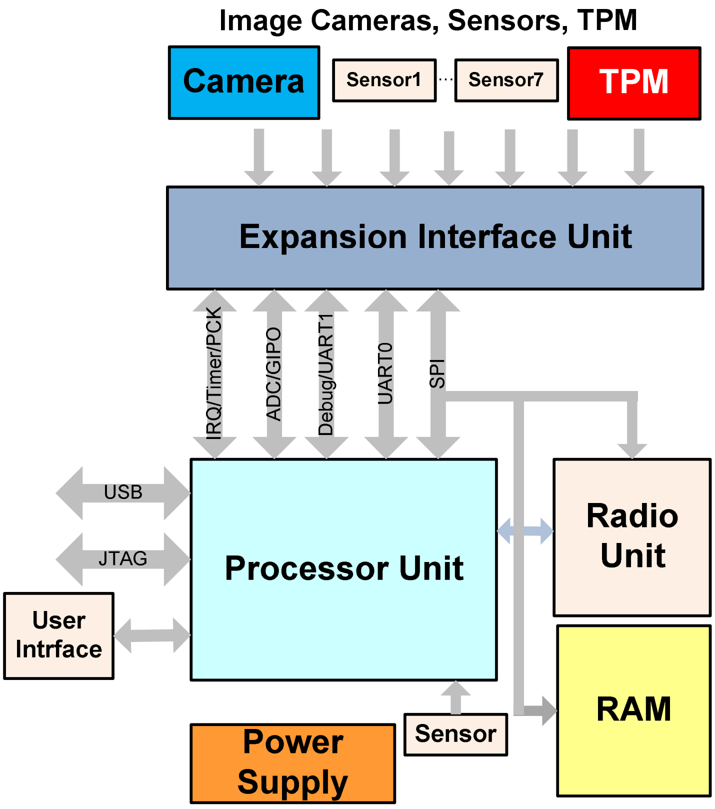


Figure 8 NMPS node prototype architecture.

More details for NMPS node design and possible design choices are provided in D3.2.

3.1.9.1.1 Design and implementation of a trusted NMPS node

3.1.9.1.1.1 TPM unit

The pSHIELD project aims to include trusted features in the sensor node design. TCG proposed TPM modules to enhance security of the devices. In section **Errore. L'origine riferimento non**

è stata trovata. we introduced security architecture for a sensor node. This can be made by an ASIC design, but it is not targeted for a prototype design in pSHIELD. The way forward was to design a separate TM module. The contribution for trusted NMPS node of this deliverables includes the following:

1. Design of a trusted TPM platform for NMPS nodes, which include standard TPM chip. It is needed for cryptography (e.g., PKC, or ECC) and remote attestation in WSNs.
2. Extensive evaluation of trusted TPM unit in terms of cryptography algorithms, computation time, power consumption, cost, etc.
3. A proof-of-concept to use such trusted NMPS node for different applications where security enhancements are required (key management, secure SW update, secure remote attestation, etc).

The objective of a TPM is to provide a hardware-based root of trust for a device. For example, TPM has

- **Cryptography Operation Engine (COE)**:
  - TPM is programmed with a unique RSA key pair and the private part never leaves nonvolatile protected memory
  - RSA engine for signature generation and message decryption
  - Secure Hash Algorithm (SHA) Engine
  - Random Number Generation (RNG)
- **Platform Configuration Register** (PCR):
  - Stores integrity-sensitive messages in regard to platform environment
  - Located in nonvolatile protected memory (temper-proof)

More details are provided in D3.2 document.

3.1.10 Security enhancements: performance evaluation

In D3.2 are summarized the performance of a NMPS node platform equipped with a TPM unit. As part of our study in section 7 in D3.2, the possible final implementation of RSA or ECC for NMPS node is still under investigation. However, the reported results are encouraging that such cryptography can be used successfully for energy-constrained sensor nodes. The results show that the TPM chip can reduce the computational time of RSA encryption by a factor of 8000. Integrity of a node can be verified by an attestation protocol, which used TPM as was proposed in the previous section. By to enable a WSN operator to react to tempering attempts, information about the node integrity needs to be exchanged through the network. If such information is exchanged overtly, attacker may be aware of the fact that the network is being monitored. Analyses of exchanged information may even reveal how often such information is exchanged and if no appropriate cryptography countermeasures are taken, it may also be possible to tell what information is exchanged. The problem is that every integrity protocol needs a secure channel between devices. Recently was proposed a “covert channel” for hidden transportation of integrity monitoring messages. The current work presented in this deliverables will be extended toward a new approach for enhancing security regarding the system integrity.

3.1.10.1 Attack models

With respect to the possible attacks explained in section **Errore. L'origine riferimento non è stata trovata.** there are different attack models. Here, we are mostly concerned for integrity. Therefore, we can define the following attack models.

1. The attack initiated from a radio signal which try to reprogram sensor node with malicious intent.

2. The physical attacks which completely take over sensors by plugging in wired cables.

For example, through radio channel can be modified the functional modules of a sensor. The second model is relevant for changing middleware or OS, which are hard coded in the HW. By reprogramming sensor nodes through radio signals is possible in the following cases:

- Listen to the data being transmitted through a node
- Introduce corrupt data into the WSN
- Act as sink and discard all the data passing through the node.
- Deplete the node of its resources
- Keep transmitting garbage data; thereby deplete energy of entire network or occupancy the communication channel.

The first assumption is that an attacker has a powerful PC computer with powerful computational resources. The attack may be an external or internal. Injecting malicious packets into the network, replay previously intercepted packets, or impersonate other nodes is an external attack for eavesdropping the information. DoS are external attacks were explained in section 4 in D3.2. The attacker can compromise some nodes to attack the rest of the network (internal attack). Compromised sensor nodes are considered as legitimate nodes in the WSN before they are detected and removed. However, despite nodes are being compromised, the cryptographic information stored in TPM could not be learned because TPMs are temper-proof HW. For the purpose of secure bootloading the microcontroller is configured via the fuses so that, on reset, control is transferred to the initialisation code within bootloader segment. Then the initialisation code performs a TPM clear state reset, which clear all TPM configurations including PCR value. We can use a remote attestation protocol to test the system integrity of a node and to defend against over-the-air malicious code injection attacks.

We shows that by utilising commercial TPM HW techniques is possible to design a trusted NMPS node that provide essential security services such as message confidentiality, integrity, authenticity and system integrity based on RSA or ECC cryptography techniques. The results shows that such node can provide services within the computational, memory and energy limits that apply to pSHIELD WSN nodes. HW approach offer secure storage of the private key and support for system configuration checking. We have demonstrated there is possible to achieve remote attestation, symmetric key management, secure SW update, etc.

Recommendation no. 17: The performance of networked NMP-SPD nodes should be evaluated on a SPD-WSN network by using pre-defined attack models tailored for the application-specific scenario.

3.1.11 Conclusions

This deliverables summarizes the SPD attributes and functionalities for NMPS nodes that composed a pSHIELD sub-WSN. One of the main aims of this document was to provide an extended view of the SPD concerns in ESs design and implementation for the pSHIELD system. It is essential to consider the fundamental and often application-specific characteristics of ESs and the particular requirements developed in D2.3.2.

Our goal was to provide various mechanisms for ensuring and maintaining the security and dependability of sensed network data under the aforementioned adversary model. Specifically, we have the following goals:

- **Security**: To enhance data confidentiality, integrity authenticity and system integrity.

- **Privacy**: To enhance privacy because, WSNs are “tools” for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network.
- **Dependability:** To enhance data availability against sensor failures and sensor compromises, i.e., minimizing the effect brought by individual sensor failures and compromises.
- **Lightweight**: The NMPS node security design should be lightweight as always in order to fit into the inherent resource-constrained nature of the sensor nodes.

Based on a layered design approach proposed for the pSHIELD system/network and SPD service composition the existence of SPD nodes is essential. Therefore, a considerable effort was made for designing NPM SPD node prototypes. In D3.2, we firstly reviewed the weakness of previous proposed SPD schemes and pointed out the major concerns for security of WSNs via formal proof. In particular we highlighted possible WSN applications we a focus on RTCI scenario, their network architecture, their hardware specifications and their security vulnerabilities. We also outlined the major threats associated with WSNs. In the literature survey, we emphasized also the work to date conducted by researchers in the areas:

1. NMP Node Technologies
2. Wireless Sensor Networks
3. Firmware, Secure SoC, and Trust
4. Power Supply Protections
5. ECC for NMP Nodes
6. NMP Node: prototypes
7. Confidentiality, Integrity, Authenticity, and System Integrity in WSNs

Securing a WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability on which we focus our work for proof-of-concept. We showed that efficient software updating is in many ways one of the most challenging features to provide on a WSN. It requires reliability large amounts of data to be reliably disseminated to the nodes, sophisticated mechanisms to minimize the cost of this dissemination, and aggregated status to be returned to a host. It may also require tracking of software failures and recovering from its failures in a network-wide manner. It must provide support to handle network partitioning, node failures, software failures, data transmission failures and other intermittent and persistent faults.

3.2 Lessons-learned for the adaptation of lab prototypes

3.2.1 NMP node capabilities

A **pSHIELD Node** is an Embedded System Device (ESD). When a Legacy ESD equipped with several legacy node capabilities will be used in the pSHIELD network it requires a pSHIELD Node Adapter (pSNA). A pSHIELD node is deployed as a hardware/software platform, encompassing intrinsic, innovative SPD functionalities, providing proper services to the other pSHIELD networks and middleware adapters to enable the pSHIELD composability and consequently the desired system SPD[11]. There are three kinds of **pSHIELD node** deploying each different configuration of Node Layer SPD functionalities of the pSHIELD framework, and

[11] “Security and Dependability of Embedded Systems: A Computer Architects’ Perspective” Jörg Henkel, University of Karlsruhe, Karlsruhe, Germany; Vijaykrishnan Narayanan, Pennsylvania State University, USA; Sri Parameswaran, University of New South Wales, Australia; Roshan Ragel, University of Peradeniya, Sri Lanka VLSID '09 Proceedings of the 2009 22nd International Conference on VLSI Design EEE Computer Society Washington, DC, USA ©2009

comprising different types of complexity: **Nano nodes, Micro/Personal (NMP)** nodes and **power nodes**.

The technological advancements in computing hardware and software enables a new generation of small ESDs to perform complex computing tasks. Extremely small sensor devices provide advanced sensing and networking capabilities. In parallel, many operating systems targeting these types of devices have been developed to increase their performance. The method for designing pSHIELD NMP Nodes is twofold:

1. To design completely **new NMP nodes** that are **complaint with the pSHIELD system** design.

2. To keep legacy node technologies as they are compliant with their standards, developed for many applications including those that are targeted in pSHIELD, which means to assume a heterogeneous infrastructure of networked ESDs like IEEE 802.15.4, IEEE 802.11, etc. An ordinary sensor technology (not all, since we need those that are designed for ES) permits to consider an augmentation of SPD functionalities at different levels of the hardware and firmware modules. This means an enhanced **legacy NMP node** with physical layer and protocol stack composed of existing and new SPD technologies added by pSNA. As result of this integration a new types of networked SPD ESDs will be created. pSHIELD and new SPD ESDs will compose a heterogeneous SPD network infrastructure too.

Developing a nano, micro/personal node equipped with some Legacy functionalities and with the pSNA we obtain a composable pSHIELD Node. **It means new SPD ESDs it has all desired SPD functionalities and services for the pSHIELD application scenario selected**. Additionally to that, the pSHIELD Node keeps almost all desired functionalities of a standardised sensor technology with additional SPD features that make it composable into the pSHIELD framework. The architectural design of the pSHIELD Nodes will relay on the ISO/IEC 9126 standard that has 6 top level characteristics: functionality, reliability, usability, efficiency, maintainability and portability.

Selection of the operating system for the demonstrator is an important design constrain, since we need to decide in which sensor platform will be realized SPD functionalities. The only requirement that we posed for this operating system is related to it possibility to be designed for embedded devices. There are two candidates for that: **TinyOS** and **Contiki**. Additionally, **Hydra platform** is a new concept that is realized in such a way that between physical and application layer is a middleware.

3.2.2 NMP node capability gaps

The NMP nodes need to support various security solutions in order to deal with one or more of the SPD requirements described in D2.1.2, D2.2.2, and D2.3.2. These requirements present significant bottlenecks during the node design process, which are briefly described below.

- **Processing Gap:** Existing embedded system architectures are not capable of keeping up with the computational demands of security processing, due to increasing data rates and complexity of security protocols. These shortcomings are most felt in systems that need to process very high data rates.

- **Battery Gap:** The energy consumption overheads of supporting security on battery-constrained embedded systems are very high. Slow growth rates in battery capacities (5–8% per year) are easily outpaced by the increasing energy requirements of security processing, leading to a battery gap. Various studies show that the widening battery gap would require designers to make energy-aware design choices (such as optimised security protocols, custom security hardware, and so on) for security.

- **Flexibility:** An embedded system is often required to execute multiple and diverse security protocols and standards in order to support (i) multiple security. Furthermore, with security protocols being constantly targeted by hackers, it is not surprising that they keep continuously evolving. It is, therefore, desirable to allow the security architecture to be flexible (programmable) enough to adapt easily to changing requirements.

- **Tamper Resistance:** Attacks due to malicious software such as viruses and trojan horses are the most common threats to any embedded system that is capable of executing downloaded applications. These attacks can exploit vulnerabilities in the OS or application software, procure access to system internals, and disrupt its normal functioning. Because these attacks manipulate sensitive data or processes (integrity attacks), disclose confidential information (privacy attacks), and/or deny access to system resources (availability attacks), it is necessary to develop and deploy various HW/SW countermeasures against these attacks. Tamper resistance measures should, therefore, secure the system implementation when it is subject to various physical and side-channel attacks.

- **Assurance Gap:** As systems become more complicated, there are inevitably more possible failure modes that need to be addressed. Increases in embedded system complexity are making it more and more difficult for embedded system designers to be confident that they have not overlooked a serious weakness.

- ***Cost*:** One of the fundamental factors that influence the security architecture of an embedded system is cost. To understand the implications of a security related design choice on the overall system cost, consider the decision of incorporating physical security mechanisms in a single-chip cryptographic module.

So, decision for a generic NMP node SPD compliant architecture is a multi-technology, multi-functional, and multi-target top-down process with respect to the application scenario. In opposite, it is a bottom-up process with respect to heterogeneity of different underplaying technologies. The best-fit of these two design processes is a merge of top-down and bottom-up approach into a unique SPD approach for a HHN on which different interoperable technology will coexist.

3.2.3 Trusted SoC design

By using ARM trust zone, a small on-chip security system is presented in Figure 9 below to execute the pSHIELD SoC SPD design objectives. It clearly depicts the permanent secure place and dynamic secure place that are accessible through AXI2APB bus system which has the capability to switch from secure process and non-secure process. Trust Zone Memory Adapter (TZMA) will secure a region within an on-SoC memory such as SRAM where the secure location will be in the lower part of the memory region.

Figure 9 proposes security architecture for sensor node using ARM11 with Trust zone features. Trust zone Address Space Controller (TZASC) will reject any non-secure transaction to a region that is configured as secure. Therefore external memory also can be partitioned into secure and non-secure region. Compared to previous works, the proposed security architecture has extended the security infrastructure throughout the system design. Instead of protecting assets in a dedicated hardware block, this architecture has made the valuable assets secured in the most protected location. On top of the hardware design, a suitable security protocol such as secure boot will also be configured to complete the security design. Secure boot with the root of trust located in On-SoC ROM will provide a chain of trust for all the secure world software and hardware peripherals and some of the normal world software. With secure boot, the integrity of the OS image, software and peripherals on the platform can be verified to be truly unadulterated. Communications right after the secure boot process can be confirmed coming from a trusted sensor node.

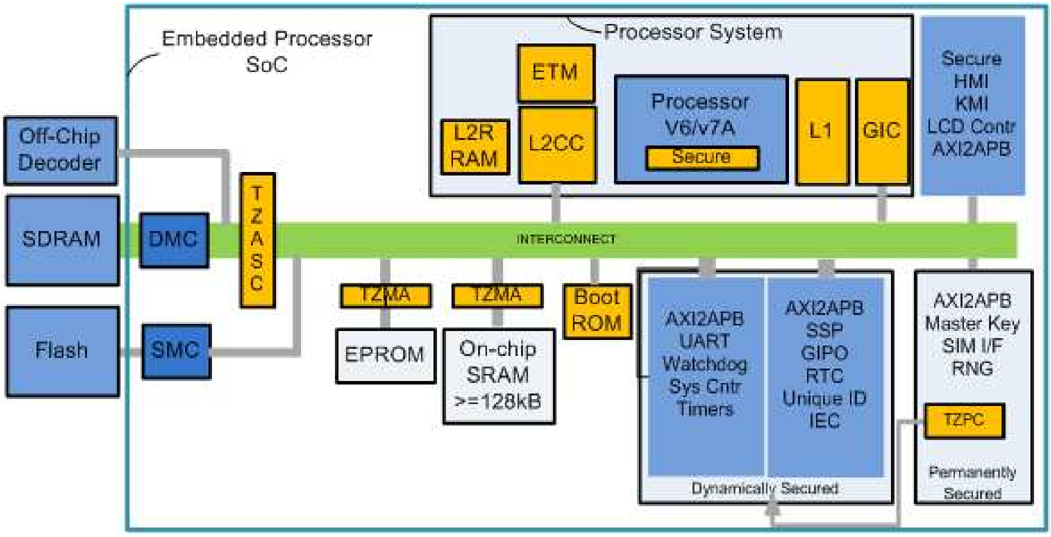


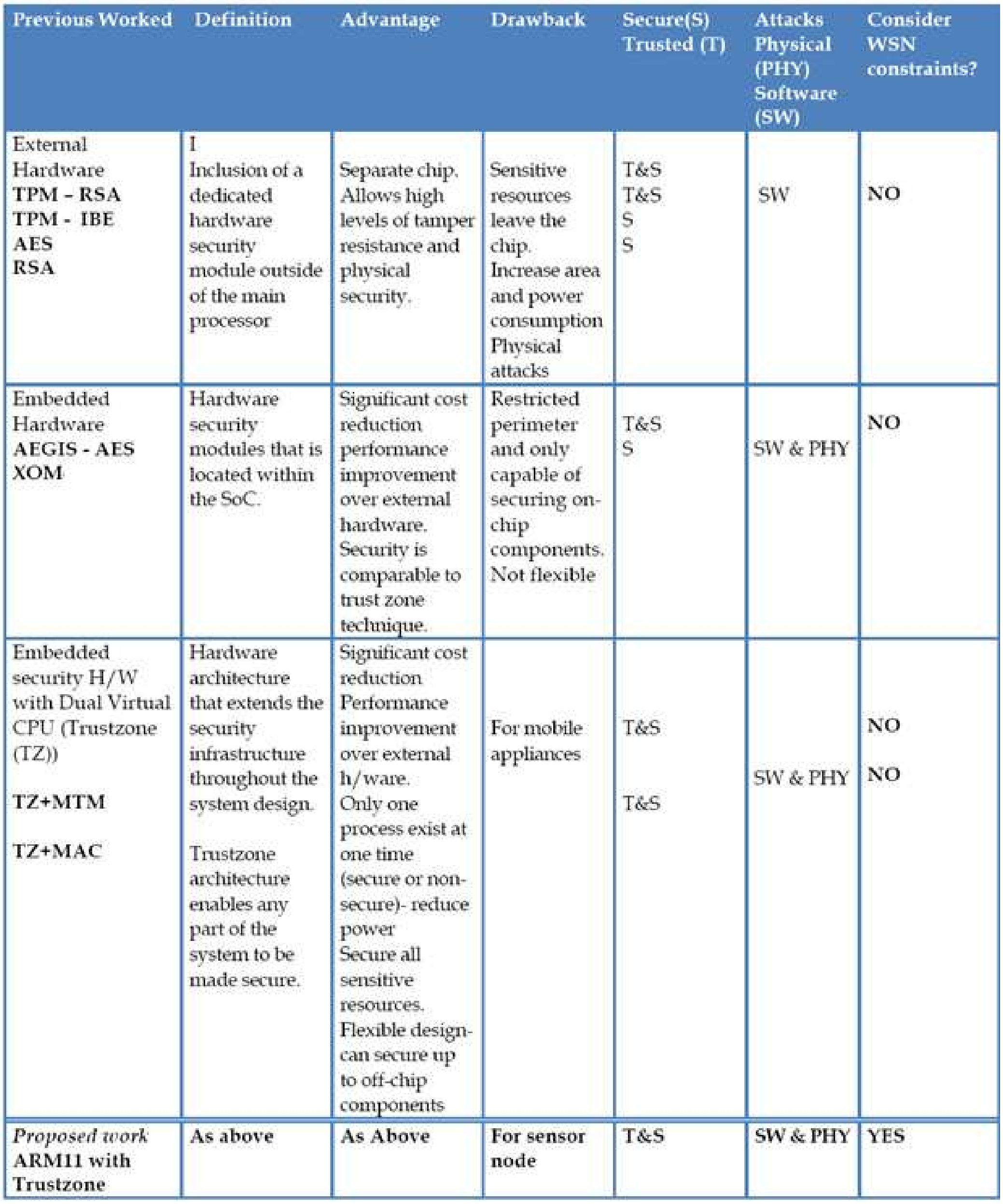
Figure 9 Security architecture for sensor node using Arm11 with Trust zone features.

Table 3 shows the advantage of the security mechanism proposed[12]. While in AEGIS for example two processors are needed to run secure and normal process, in trust zone the dual virtual CPU will execute one of the processes (secure or non-secure) at one time thus eliminate extra processing work and reducing the chip size. Moreover, AEGIS works is does not consider WSNs constraints. The security aspects discussed in this section are intended for highly secure applications dealing with very important information like financial information, noncritical military communications, medical data, and CIP. Two dominant features are the placement of sensitive resources such as the crypto keys within the embedded system and the denial of extra or dedicated processor core for security purposes. This is also in line with the pyramid approach discussed earlier. This implementation ensures no sensitive resources leaves the chip and therefore blocks most types of attacks. Additionally, that it also saves the silicon area and power consumption and also allows high performance security software to run alongside with the normal world operating environment. For example, the choice of ARM11 as the main processor for the sensor node is in line with the constraint faced in sensor node development as it is rated as the most efficient processor in MIPS/Watt[13].

[12] Y. M. Yussof et al., “Untegrity enhancement un Wireless Sensor Networks,” InTech, December 2010.

[13] Vieira, M. A. M., C. N. Coelho, Jr., D. C. da Silva, Jr. & J. M. da Mata (2003): Survey on wireless sensor network devices. In Emerging Technologies and Factory Automation, 2003. Proceedings. ETFA '03. IEEE Conference.

Table 3 Comparison study on trusted implementation for WSNs.



Previous Worked	Definition	Advantage	Drawback	Secure(S) Trusted (T)	Attacks Physical (PHY) Software (SW)	Consider WSN constraints?
External Hardware **TPM - RSA** **TPM - IBE** **AES** **RSA**	I Inclusion of a dedicated hardware security module outside of the main processor	Separate chip. Allows high levels of tamper resistance and physical security.	Sensitive resources leave the chip. Increase area and power consumption Physical attacks	T&S T&S S S	SW	**NO**
Embedded Hardware **AEGIS - AES** **XOM**	Hardware security modules that is located within the SoC.	Significant cost reduction performance improvement over external hardware. Security is comparable to trust zone technique.	Restricted perimeter and only capable of securing on-chip components. Not flexible	T&S S	SW & PHY	**NO**
Embedded security H/W with Dual Virtual CPU (Trustzone (TZ)) **TZ+MTM** **TZ+MAC**	Hardware architecture that extends the security infrastructure throughout the system design. Trustzone architecture enables any part of the system to be made secure.	Significant cost reduction Performance improvement over external h/ware. Only one process exist at one time (secure or non-secure)- reduce power Secure all sensitive resources. Flexible design- can secure up to off-chip components	For mobile appliances	T&S T&S	SW & PHY	**NO** **NO**
Proposed work **ARM11 with Trustzone**	**As above**	**As Above**	**For sensor node**	**T&S**	**SW & PHY**	**YES**

3.2.4 Power harvesting methods

One possibility to overcome power limitations created by the use of batteries as power sources is to get the energy from the environment to either recharge a battery or even, to directly power the electronic device. Not all technologies are suitable to be integrated in pSHIELD nodes. The scenario is one of the most relevant factors to be considered before selecting the suitable energy harvesting method. The node with low power consumption is the nano node. A GPS, GSM or GPRS module could be an example about this type of device. The expected power consumption is about 150mW in full operating mode and less than 1mW in sleep mode. The micro node is more complex than nano node so higher power consumption is expected. A sun spot or a mobile phone could be considered as micro nodes. In general, these low-efficient technologies are useful only for low energy devices, although the improvements carried out during last years have allowed to increase the application fields.

- ***Solar power*** is a clean energy source that needs the sunlight to provide heat and electricity. It is the most popular technology because it could be converted to thermal energy to heat spaces, water or other fluids and it is also possible to get electricity through solar cells or solar power plants. The low efficiency is owing to the irregular sunlight that depends on the location, time of day, time of year and weather conditions. For this reason, a wide area is required to collect the energy at a useful rate.

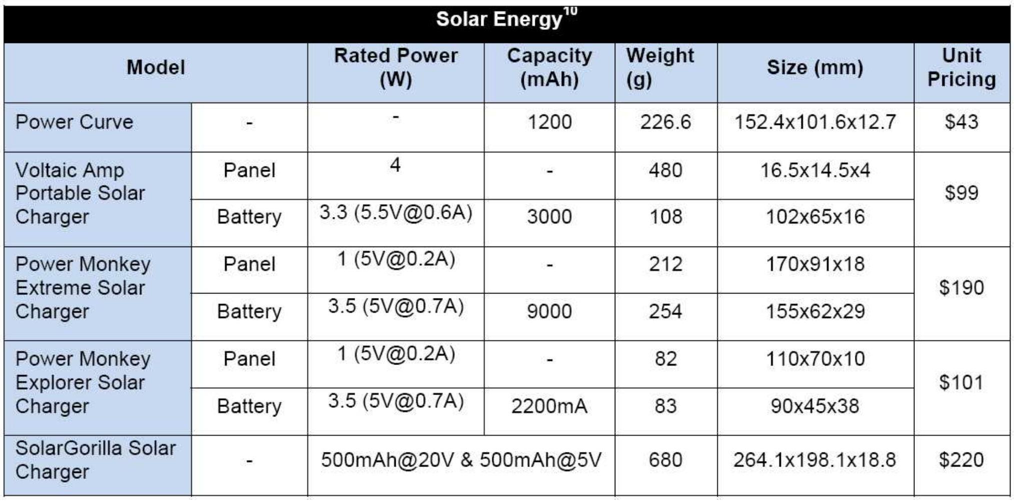
- ***Thermal energy*** converts the waste heat energy variations from the environment (persons, animals, machines, etc.) into electrical energy. The efficiency of this method depends on the difference of temperature between the hot source and the environment. The greater the difference, better the efficiency is.

- ***Wind power*** is one of the most old renewable energy sources where the wind is used to generate mechanical power or electricity. Although it is one of the lowest-priced technologies available today, it requires a higher initial investment and may not be a competitive technology if the environment has not a good wind conditions.

- ***Pressure variations energy*** comes from atmospheric pressure and/or thermal variations. It should be noted that this method is not widely used because there are not advances implementing large-scale systems.

- ***Vibrations*** are present almost everywhere (buildings, transports, industrial environments, etc.) so it is a potential power source. To scavenge power from vibrations, some devices are needed like electromagnetic, electrostatic, and piezoelectric generators that transforms mechanical motion into electricity.

Table 4 Power Source – solar energy.

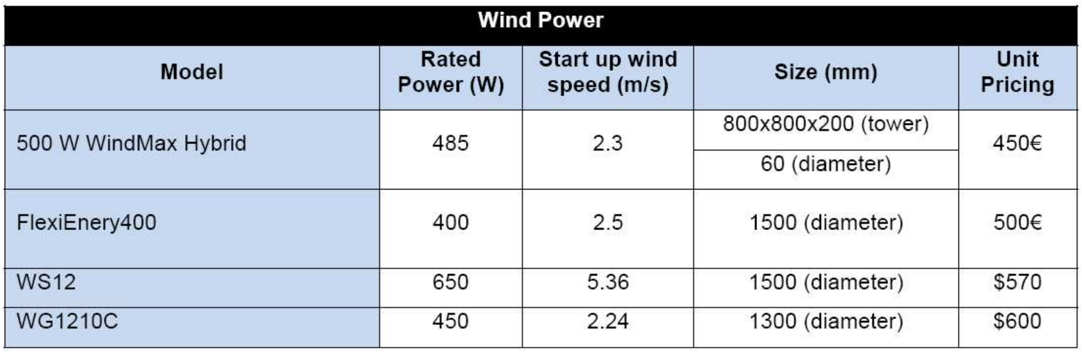


Solar Energy[10]						
Model		**Rated Power (W)**	**Capacity (mAh)**	**Weight (g)**	**Size (mm)**	**Unit Pricing**
Power Curve	-	-	1200	226.6	152.4x101.6x12.7	$43
Voltaic Amp Portable Solar Charger	Panel	4	-	480	16.5x14.5x4	$99
	Battery	3.3 (5.5V@0.6A)	3000	108	102x65x16	
Power Monkey Extreme Solar Charger	Panel	1 (5V@0.2A)	-	212	170x91x18	$190
	Battery	3.5 (5V@0.7A)	9000	254	155x62x29	
Power Monkey Explorer Solar Charger	Panel	1 (5V@0.2A)	-	82	110x70x10	$101
	Battery	3.5 (5V@0.7A)	2200mA	83	90x45x38	
SolarGorilla Solar Charger	-	500mAh@20V & 500mAh@5V		680	264.1x198.1x18.8	$220

Table 5 Power source – vibrations.

Vibrations
The harvesters convert unused mechanical vibration into useable electrical energy to power wireless sensor systems. The PMG FSH is designed with highly efficient drive circuitry for charging an external storage device up to 4mA at 5V while reporting power levels via a standard 3-pin IEC connector. The PMG FSH output can be monitored via the 3-pin IEC interface to provide power output status to a Wireless Sensor Node. The PMG FSH features a high power output up to 20mW.

Table 6 Power source – wind power.



Wind Power				
Model	Rated Power (W)	Start up wind speed (m/s)	Size (mm)	Unit Pricing
500 W WindMax Hybrid	485	2.3	800x800x200 (tower) 60 (diameter)	450€
FlexiEnery400	400	2.5	1500 (diameter)	500€
WS12	650	5.36	1500 (diameter)	$570
WG1210C	450	2.24	1300 (diameter)	$600

3.2.5 ECC vs. RSA execution times for SW-TPM commands

The execution time and energy consumed by SW-TPM on the NMP node is presented here in order to understand what we learned for adaptation of lab prototypes future implementation. The presented results are for the original RSA-based SW-TPM and for the proposed ECC-based SW-TPM reported in D3.2.

For commands categorized as the storage and key management commands, and TPM_Sign, measurements are performed for different key sizes. For commands that process user data, the data size is varied. The results of these experiments are reported in Table 7. The command executed is presented in Column 1. Columns 2-3 give the key size (*K*) and data size (*D*). For commands that do not involve cryptographic operations *K* (*D*) is indicated as N/A. Column 4 gives energy measurements in milliJoules (mJ), and column 5 reports the execution times for the TPM commands in milliseconds (msec.).

The results indicate that commands involving RSA operations, particularly private key operations, which require manipulation of large numbers, and a resource-consuming modular exponentiation, impose a high execution time overhead. For instance, the TPM_MakeIdentity command, which involves 2048-bit RSA key generation and validation, as well as encryption of the private AIK using the SRK, in addition to other cryptographic functions, takes 29.63 sec. and consumes 70.94 J of energy. Similarly, large execution times and energy consumptions are required for TPM_TakeOwnership, TPM_CreateWrapKey, TPM_Unseal, *etc*. This overhead is reduced by using ECC: execution time and energy requirements for the TPM_MakeIdentity command are reduced to 2.43 sec. and 5.86 J, respectively. By using ECC, an average reduction of 6.51X and 6.75X can be achieved for execution time and energy, respectively, across all commands.

Table 7 Energy and execution time for TPM commands

Command	K(bits) ECC/RSA	D(bytes)	PDA measurements	
			Energy (mJ)	Time (msec.)
Authentication commands				
TPM_OIAP	n/a	n/a	0.61	0.21
TPM_OSAP	n/a	n/a	2.38	0.82
Capability commands				
TPM_GetCapability **(Key info.)** **(Manufacturer info.)** **(PCR info.)**	 n/a n/a n/a	 n/a n/a n/a	 0.10 0.10 0.20	 0.04 0.04 0.07
Cryptographic commands				
TPM_GetRandom	n/a	20	0.55	0.19

TPM_Sign	224/2048	20	450/2210	191/902
	224/2048	50	492/2221	204/926
	224/2048	100	531/2394	216/960
	160/1024	20	210/806	90/343
	160/1024	50	242/930	114/388
	160/1024	100	319/1006	131/409
	192/512	20	321/626	136/265
	192/512	50	350/656	148/274
	192/512	100	361/760	153/305
Identity commands				
TPM_ActivateIdentity	224/2048	n/a	598/12824	348/5239
TPM_Makedentity	224/2048	n/a	5859/70943	2425/29634
Measurements commands				
TPM_PcrRead	n/a	n/a	17.32	6.69
TPM_PcrExtend	n/a	n/a	32.28	12.46
TPM_Quote	224/2048	n/a	762/2475	381/1239
Ownership commands				
TPM_ReadPubek	224/2048	n/a	0.31/3.10	0.12/1.22
TPM_TakeOwnership	224/2048	n/a	5619/66777	2391/28619
Start-up commands				
TPM_init_data	224/2048	n/a	1.71/25.39	0.69/10.52
TPM_Startup	224/2048	n/a	0.48/1.46	0.19/0.58
Storage and key management commands				
TPM_CreateWrapKey	224/2048	n/a	5558/42582	2322/16938
	160/1024	n/a	4128/12133	1813/4594
	192/512	n/a	4419/8395	1880/3025
TPM_EvictKey	224/2048	n/a	8.36/37.08	3.31/14.78
	160/1024	n/a	6.70/16.62	2.71/6.62
	192/512	n/a	6.72/7.73	2.79/3.10
TPM_GetPubKey	224/2048	n/a	640/10592	229/4388
	160/1024	n/a	471/1504	157/567
	192/512	n/a	516/852	172/453
TPM_LoadKey	224/2048	n/a	810/14547	336/5367
	160/1024	n/a	593/4557	261/1796
	192/512	n/a	737/2092	301/841
TPM_Seal	224/2048	20	1103/3751	463/1476
	224/2048	50	1125/3785	472/1564
	224/2048	100	1313/4271	530/1761
	160/1024	20	769/1898	322/796
	160/1024	50	806/2195	334/967
	160/1024	100	819/2965	342/1178
	192/512	20	1001/1019	420/427
	192/512	50	1026/1063	431/481
	192/512	100	1093/1326	444/551
TPM_Unseal	224/2048	256	1444/14056	585/5520
	160/1024	256	952/4679	391/1880
	192/512	256	1279/1778	525/714
TPM_Unbind	224/2048	256	1459/10480	576/4103
	160/1024	256	974/4269	384/1699
	192/512	256	1284/1616	524/699

Macromodels that capture the energy for the commands TPM_Sign and TPM_Seal as a function of the key size *K* and data size *D* are presented in the Table 8. Values of *K* are up to 2048 (224) bits for RSA (ECC), and *D* assumes values up to 144 Bytes. From the macromodels, and the numbers reported in Table 7 can be concluded that energy and execution time requirements vary more considerably with the key size rather than with the data size (especially with RSA cryptography).

Table 8 Energy macromodels for the TPM_Sign and TPM_Seal.

Command	**Crypto type**	**Energy model ($C + A*D + B*D^2 + X*K + Y*K^2$ (mJ))**

TPM_Sign	ECC	$31.269 + 1.434{*}D - 0.004{*}D^{2} + 0.642{*}K + 0.011{*}K^{2}$
	RSA	$29.994 + 10.389{*}D - 0.061{*}D^{2} + 0.349{*}K + 0.00029{*}K^{2}$
TPM_Seal	ECC	$6.415 + 0.067{*}D - 0.012{*}D^{2} + 3.980{*}K + 0.005{*}K^{2}$
	RSA	$5.766 + 10.033{*}D - 0.142{*}D^{2} + 2.435{*}K + 0.00026{*}K^{2}$

The presented results are based on the average of several executions (16) of each command, in order to account for uncontrollable variables, such as the randomness of the keys, and to minimize measurement error for commands that require small running times.

It is also important to place the overheads in the context of actual applications not only for evaluating the requirements of SW-TPM in isolation. Trusted extensions for several applications are proposed and the impact of using SW-TPM on their execution time and energy consumption is studied as lesson learned for the future NMPS node prototypes.

3.2.6 Microcontroller/Microprocessor comparison

First of all, choose of a microcontroller unit (MCU) based on several requirements such as low power consumption, rich on-chip peripherals, RAM and ROM, etc. Table 9**Errore. L'origine riferimento non è stata trovata.** shows the comparison of the MCUs.

Table 9 MCU comparison.

MCU	RAM (kB)	FLASH (kB)	Active (mA)	Sleep (µA)	Sensor Nodes
Atmega128 (Atmel)	4	128	8	20	DSY25, EberNet, BT node, Iris, MicaZ, Mica2
AT91SAM7128 (Atmel)	32	128	30	10	Evaluated
Atmega644/V (Atmel)	4	64	0.4	0.1	TelG Mote
STM32W108B* STMicroelectronics	8	128	6@12MHz	<1	pSHIELD NMPS node
PIC Modern (Microchip)	4	60	2.2	1	CIT Sensor node, Particle 2/29, GWnode
80C-51 (Philips)	2	60	15	3	ECO, MITes
MSP430F14x (TI)	2	60	1.5	1	Telos, BSN node, Pluto
MSP430F16x (TI)	10	48	2	1	eyesIFXv2, Tmote Sky

(*) STM32W chip has integrated IEEE 802.15.4 radio at 2.4.GHz.

Table 9 illustrates that Atmega644P/V has the lowest consumption for both active and sleep modes. The operating voltage is 1.8V. It uses an advanced RISC architecture where most of the 131 instructions only require one clock cycle to be executed and up to 20 Million Instructions per Second (MIPS) at 20MHz. It also provides all the basic peripherals for microcontroller with additional USART port, Timer and PWM modes. 4kB RAM is smaller compared to 10kB RAM (MSP430F16x). Although flash sizes are useful for large application programs, they are not the limiting factor in developing WSN applications. AT91SAM7S128 is a member of a series of low pin count Flash microcontrollers based on the 32-bit ARM RISC processor that runs at up to 55 MHz, providing 0.9 MIPS/MHz. It features a 128 Kbyte high-speed Flash and a 32 Kbyte SRAM, a large set of peripherals, including a USB 2.0 device and a complete set of system functions minimizing the number of external components. STM32W108 family is an excellent candidate for NMPS node since it has 32-bit ARM Cortex-M3 core running at 24MHz, considerably high RAM and FLASH memory with low power consumption and an integrated IEEE 802.15.4 radio at 2.4 GHz! Further information about this chip is provided in the Appendix in D3.2. Since pSHIELD was targeted as pilot project for 12 months duration it was not possible to implement SPD features on this chip. It will be furthermore investigated in the following up project nSHIELD, which is a three year project.

3.2.7 IEEE 802.15.4 chips comparison

For WSNs the selection of the radio is a critical for NMPS nodes, because the performance should not be evaluated for a individual NMPS node. The application requirements define what type of radio is needed. A wideband radio operating at 2.4 GHz and comply with IEEE 802.15.4 standard offer advantages that are important for the pSHIELD scenario. There are several radio modules available in the markets that are in compliant with IEEE802.15.4 standard. Most of the module differences lie on its power profile, device interface and additional features. Several IEEE802.15.4 compliant radio from Atmel, Chipcon, Microchip and MaxStream are listed in Table 10. When very high data rate are required (depends of the application requirement) AT86RF231 is the best choice. XBEE module from MaxStream has 50 mW output power and range from 40 m - 1.6 km. The module also provides a complete solution including the antenna. Other radio chip requires a careful design of an external antenna. The USART device interface is very easy to configure and XBEE has two modes of operation which are transparent and API mode.

Table 10 IEEE 802.15.4 chips comparison

	Atmel AT86RF231	**Chipcon CC2420**	**Microchip MRF24J0MA**	**MaxStream XBEE**
Data rate (kbit/s)	250, 500, 1000, 2000	250	250	250
Rx power (mA)	12.3	19.7	19	50
Tx power (mA/dBm)	14/+3	17.4/0	23/0	45
Power down (μA)	0.02	1	2	<10
Turn on time (ms)	<0.4	0.58	Not available	Not available
Device interface	SPI	SPI	SPI	USART
IEEE 802.15.4 HW support	FCS, CCA, RSSI, ED and LQI	RSSA, LQI	RSSA, LQI	RSSI
Antenna	External	External	Integrated PCB	Integrated Whip

3.2.7.1 Comparison of sensor node platforms

Figure 10 shows some recent sensor node platforms that are positioned with respect to the processor performance (MIPS) and memory size (kB). In the region low-bandwidth are typical sensor nodes and in high-bandwidth are extremely powerful gateway nodes. The Atmega128 (see Table 10) microcontroller is frequently used, but it can’t offer good performance for images. It use 8-bit architecture comparing to AT91SAM7128 which use 32-bit ARM7 processor.

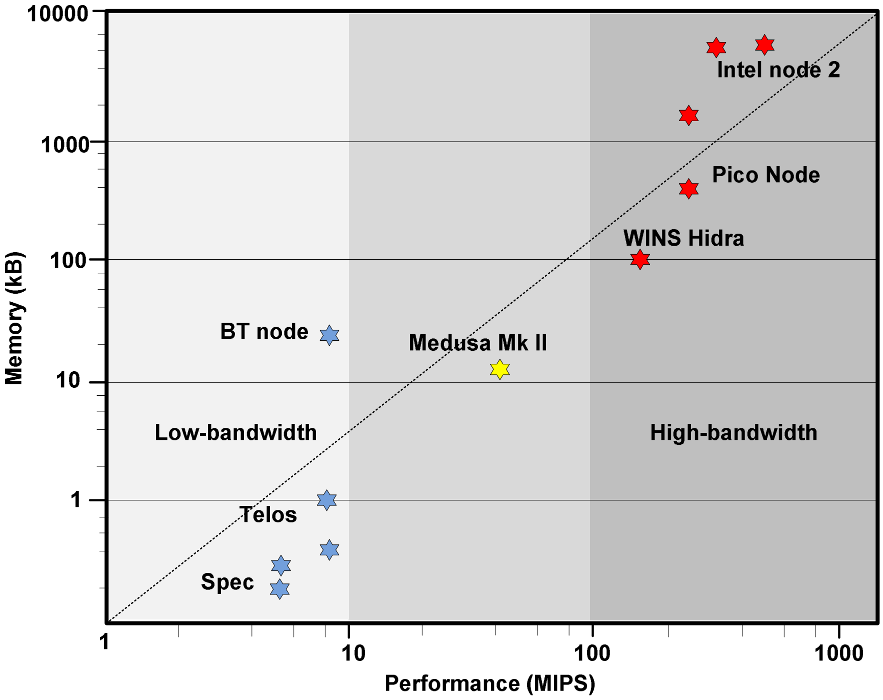


Figure 10 Comparison of sensor node platforms.

Comparing cycles to read/write, Atmega128 require 74 cycles per pixel, which means clocked at 48 MHz it would require 0.12 s. AT91SAM7128 require 56 cycles per pixel, which means clocked at 4 MHz it would require 0.12 s. This reduction for factor 16 in execution time is big advantage at almost the same power consumption. Finally, Atmega128 don't have sufficient memory to store the frames and any result. Intel Mote 2 sensor node platform[14] has more memory and computational capabilities but it has higher power consumption and it is more expensive. For these reasons it is not suitable for large network deployment. However, it is can be used[15] for BAN (Body Area Network). For NMP nodes we need a node between these two extreme, low and high-bandwidth. Medusa Mk II has two microcontrollers[16] and radio TRF1000 (compatible with IEEE 802.15.4), which make it less attractive due to added complexity, which has drawback into cross-layer optimisations. Starting from the above SoA (state-of-art) we were looking for new sensor node platforms suitable for NMP node prototypes.

Before, we decide which processor is suitable for an NMPS node it is important to highlight some restriction regarding the camera. The current generation cameras have a minimum resolution of 1280x1024 (1.3 megapixels). Such camera requires much memory and it is not suitable for NMPS node. In smart phone is used low-resolution camera CIF[17] (352 x 288) and VGA (640 x480). Agilent ADMC-1670 is an excellent candidate with CIF 352 x 352.

Based figure 10 we learned that low-bandwidth node types are suitable for nano-legacy nodes, medium-bandwidth node types for micro-legacy nodes and high-bandwidth node types for personal-legacy nodes.

3.2.8 Experiments

It is known that symmetric key cryptography consumes less energy than RSA (asymmetry keys, encryption key is different from decryption key). For example XTEA encryption consume approximately 10 times less energy compared to HW RSA encryption, and approximately 12.000 times less energy compared to SW RSA encryption. A strategy to adopt will be for nano

[14] http://wsn.cse.wustl.edu/images/c/cb/Imote2-ds-rev2_2.pdf
[15] http://netlab.boun.edu.tr/WiSe/lib/exe/fetch.php/courses:492_final_report_onur_dundar.pdf
[16] http://aceslab.org/sites/default/files/Koushanfar_SensorNetArch_2005.pdf
[17] http://psi.praeger.com/pdfs/whitepapers/PixelsandRecordSpeedandCIF.pdf

nodes to use symmetric cryptography, and for critical applications like the pSHIELD scenario, asymmetric cryptography should be used. For example, asymmetric cryptography can be used to exchange a new symmetric key daily or hourly (this is called rekey process[18],[19],[20],). An application can select to store the session keys in TPM.

An NMPS node A requests a new symmetric key from a NMPS node B, i.e., Gateway (GW). Node A initiates this process hourly or daily by generating a random number Na (nonce) and encrypts the nonce along with the request (Req) command using GW's public key (Pkgw) before transmitting it to the GW. The purpose of nonce is to defend against reply attacks. After receiving Req message from Node A, the GW decrypts the message with its private key Sgw. The GW responds to the Req command by generating a new symmetric session key Kba and encrypts it together with Na using a public key Pka before transmitting it to node A. Node A decrypts the message the from the GW with it its private key Ska and obtains the new symmetric key Kba. Nose A and the GW can then use Kba for future communications as inFigure 11. Therefore, link level secure communications can be achieved by passing the returned cipher over the radio. In the case that the key are stored in Ram or EEPROM it is not secure, because that the information can be extracted from EEPROM and RAM in 1 min. Therefore, storing the key in TPM chip for these infrequent operations is more safely.

Group key establishing cn be achieved by combination of sensor node symmetric session key request operation and sensor node symmetric session key assignment operation. For example if node A wants to communicate with node B and C, node A will request a new group session key from the GW via the session key request operation. After receiving the key request operation from Node A, the GW generates a new symmetric key Kabc. The GW assigns Kabc to the Node B and C via two session key assignment operations before transmitting Kabc to Node A. Finally, Node A, B and C we perform secure communications using the group session key Kabc.

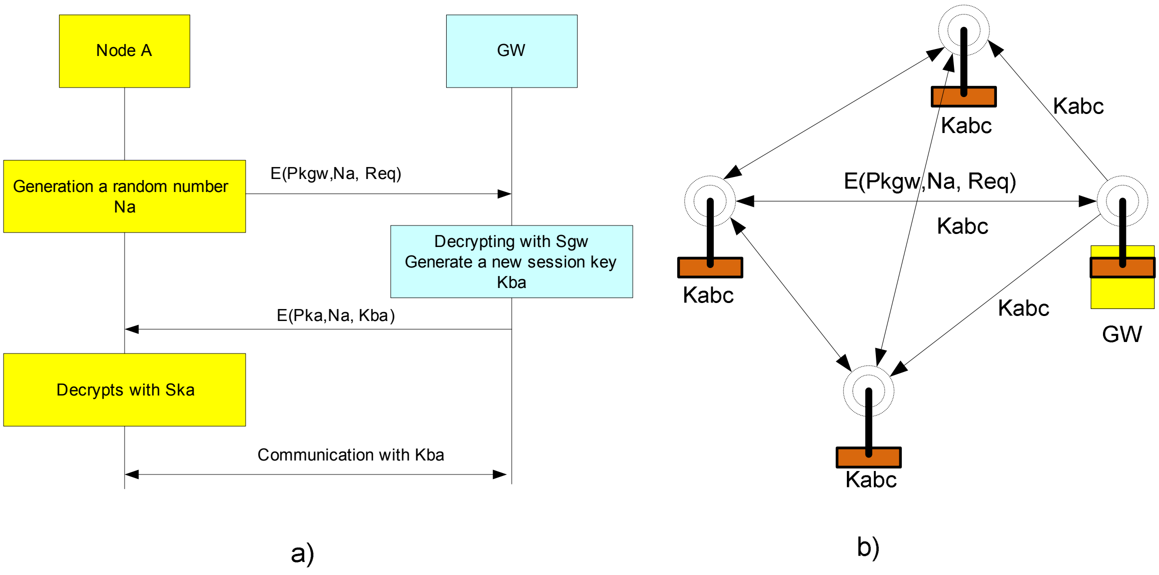


Figure 11 Symmetric session key request operation with trusted NMPS nodes: a) between Node A and GW, b) between Nodes A, B and C grace a secession key Kabc generated by GW on the request from Node A.

[18] http://xtrmntr.org/priikone/docs/ike.pdf
[19] http://conferences.sigcomm.org/co-next/2009/workshops/student/papers/Shen.pdf
[20] http://mcn.cse.psu.edu/paper/zhang/adhoc09.pdf

3.3 Analysis of industry-readiness for pSHIELD-based monitoring

3.3.1 Industry-readiness for NMPS nodes

The pSHIELD NMP sensors will expand real-time monitoring and control capabilities throughout different infrastructures (critical ones, smart grids, smart environments, smart cities, etc.) to support pSHIELD-based maintenance, enhance safety and reliability, and improve efficiency and utilization. The abilities of SPD network to monitor key parameters in areas that could not previously be accessed (or only accessed with significant cost and safety implications) will enable O&M interventions for mitigating damage, optimizing efficiency, and improving management. The research work addresses in pSHIELD demonstrated the following capability gaps:

- SPD capabilities for critical pSHIELD system components characterized by a challenging environment rail transportation of dangerous materials
- Energy-constrained and lower-cost monitoring technologies

A prototype Micro Electro Mechanical Systems (MEMS) and Nano Electro Mechanical Systems (NEMS) NMP sensor with packaged electronics is scheduled to be fabricated and tested in the laboratory. The explosion in MEMS and NEMS has occurred primarily within academic and research community. They have concentrated the biggest part of the research efforts on demonstrating the proof-of-concept for novel MEMS & NEMS devices. The MEMS are not only making things small but also: the microelectronics revolution changed the world because of cost, not size. The MEMS offers a way to make complex electro-mechanical systems at low cost. The cost and the performances must be the driver in order to fully realize the potential benefits of MEMS.

There is a general consensus that “miniaturization” grace to nanotechnologies will dominate the scientific and technological developments in the 21st Century. The expected revenue generated by NEMS and MEMS has been impressive, ~40 million € in 2001, 12 billion € in 2011, and an expectation of 27 billion to ~1 trillion € in 2015. Such revenue increase and forecast for 2015 has prompted governments of leading industrialized nations in the world investing heavily in the research and development of nanotechnology.

The EC assisted by High Level Group (HLG) (THYIA was member) adopted a plan in 2001 for Key Enabling Technologies (KETs) that becomes an industrial policy for Europe 2020. The five vertical KETs and one horizontal are:

1. Nanotechnology
2. Micro and nanoelectronics
3. Industrial Biotechnology
4. Photonics
5. Advanced materials
6. Advanced manufacturing systems

Crossing the “valley of death” in the key enabling technologies in Europe requires the delivery of solutions to the three successive stages implicit in this crossing.

The first stage, called **“Technological research”** consists of taking best advantage of European scientific excellence in transforming the ideas arising from fundamental research into technologies competitive at world level. These should be both shown through proofs of concept and be proprietary, that is protected by patents. It is the patents that will guarantee both the future freedom to exploit these technologies by European industry and their capacity to resist counterfeits and copying. From a more general perspective, an IPR strategy for global markets along with a single and efficient European system for IP protection and enforcement are urgently needed.

The second stage, called **"Product demonstration"** allows the use and exploitation of these KETs to make innovative and performing European product prototypes competitive at world level. This requires firstly putting in place pilot lines having both the KETs technology prototyping facilities to enable the fabrication of a significant quantity of innovative product prototypes arising from these KETs. Secondly, establishing the prototype product validation in terms of its user performance requires both demonstration and deployment operations at appropriate scale, on European sites protecting the technological advance achieved. In both cases, the objective is to make a demonstration at real scale of the relevance in terms of user value and the competitiveness of new product prototypes containing one or several KETs.

The third stage, called **"Competitive manufacturing"** should allow, starting from product prototypes duly validated during the demonstration phase to create and maintain in Europe attractive economic environments in EU regions based on strong eco-systems and globally competitive industries. In particular, production facilities competitive with their US and Asian equivalents in terms of production volumes and therefore price of products. This will allow further strengthening of the capabilities of EU industry to more successfully deploy KETs-based products, face international competition and master solutions to tackle grand societal challenges. In fact, in KETs where economies of scale are of importance, only advanced manufacturing based on the latest technologies and at a significant level will allow:

- The acceleration of the learning curve on new manufacturing technologies and products in order to arrive amongst the first on non-mature markets with a high probability of penetration.
- To absorb the enormous fixed costs of quality production on a volume sufficiently important to attain production costs in line with those of international competitors, notably Asian.
- To retain the production know-how at the top level, this is the only guarantee of a complete mastery of all these crucial KETs steps on European soil.
- To develop an industry for equipment and advanced manufacturing systems generating a source of export revenues, and support the downstream producers of machinery capable to produce the most advanced manufacturing technologies in Europe (machinery, software, services, etc.), as well as the development and improvement of manufacturing systems (technology and processes) in order to build efficient, modern and high technology manufacturing facilities in Europe.
- To master the whole product life cycle, from resource efficient and energy saving production to recycling processes.

The crossing of the "valley of death" in the KETs can therefore be imagined in the following manner in constructing a European bridge comprising three pillars:

- ✓ The technological research pillar focused on key technologies
- ✓ The product demonstration pillar arising from the technologies focused on product prototyping and validation
- ✓ The production pillar, competitive at world level, focused on advanced manufacturing.

The final report for KETs from June 2011 adopted the following recommendation[21]:

Recommendation n°1: Technological priority for Europe

[21] http://ec.europa.eu/enterprise/sectors/ict/key_technologies/kets_high_level_group_en.htm

The High Level Group recommends that an integrated KETs policy should be implemented, that KETs should be visibly prioritised in EU policies and financial instruments and that the European Investment Bank group should pro-actively support KETs initiatives in Europe.

Recommendation n°2: The EU should apply the TRL scale R&D definition

The High Level Group recommends the EU to align its R&D activities on the TRL scale in line with the OECD definition. The Commission should also systematically apply this definition in order to include technological research, prototype product development and demonstration activities within its RDI portfolio.

Recommendation n°3: fully exploit the scope of relevant R&D&I definitions

The High Level Group recommends that the EU should apply R&D&I definitions in its programmes which support the full and simultaneous implementation of the three pillar bridge model along the innovation chain, from basic research, through technological research, product development and prototyping up to globally competitive manufacturing.

Recommendation n°4: Rebalancing of EU RDI funding programmes

The High Level Group recommends that the EU and Member States firmly rebalance their RDI funding in KETs-related programmes towards technological research, the development of prototypes, pilots lines, first-in-kind equipment and facilities and demonstrator activities. In particular in the future CSF, the EU should set indicative targets for the percentage of funding dedicated to basic research, technological research and development activities.

Recommendation n°5: a strategic approach to KETs programmes

The High Level Group recommends that the European Commission defines and implements a strategic, industry driven and coordinated approach to KETs programmes across EC RDI funding programmes and instruments (CSF, ERDF).

Recommendation n°6: An appropriate set of rules to the implement KETs programmes

The HLG recommends that the European Commission adapts its selection criteria and implementation rules in the CSF programme to maximise its impact on the value and innovation chains. In particular, a "value chain correctness" criterion should be added.

Recommendation n°7: Combined funding mechanisms

The HLG recommends that the EU should introduce a tripartite financing approach based on combined funding mechanisms involving Industry, Commission, and national authorities (Member States and local government), when required by the high costs of the KETs RDI projects, and put in place mechanisms to allow the combination of EU funding (CSF, structural funds), to enable the optimum investment in significant KET pilot line and manufacturing facilities across Europe.

Recommendation n°8: KETs state aid provisions

The High Level Group recommends that the EU adapts state aid provisions to facilitate RDI activities and large-scale investment in KETs, in particular through the introduction of a matching clause in the EU state aid framework across the board, increased thresholds for notifications, faster procedures and the use of projects of common European interest.

Recommendation n°9: Globally competitive IP policy in Europe

The High Level Group recommends that the selection criteria and terms of the consortium agreements of EU RDI funding programmes should be amended to ensure that participating consortia have a clear and explicit plan for both the ownership of and first exploitation of IP resulting from the project within the EU. It should explicitly include provisions similar to those of the “Bayh-Dole Act” and “Exception Circumstances”-like provisions to encourage the first exploitation and manufacturing of products based on this IP within the EU.

Recommendation n°10:

The High Level Group recommends that the EU should create a European Technology Research Council (ETRC) to promote individual excellence in technologically focused engineering research and innovation and establish the appropriate framework conditions through the ESF regulation in order to support KETs skills capacity building at regional level.

Recommendation n°11: a European KETs observatory and consultative body

The High Level Group recommends that the European Commission establishes a European KETs Monitoring Mechanism tasked with the mission of performing analysis and a "KETs Consultative Body" comprised of stakeholders across the entire innovation chain to advise and monitor the progress in Europe of the HLG KET recommendations towards the development and deployment of KETs for a competitive Europe.

From the above brief explanation the industrial policy of Europe 2020 is evident that pSHEILD and its follow-up project nSHILED lie in the core technologies of KETs. The consortium strongly believes that there is clear vision how the European industry in the KETs areas will gain a momentum for developing the most competitive technologies for the world market. Therefore, we adopted also an aggressive plan for that. The milestones are:

- 2013: Complete SPD node component-level experimental tests
- 2014: Assemble prototype MEMS NMP sensor nodes
- 2015: Assemble prototype SPD Network of NMP SPD and Legacy nodes
- 2020: A mass production of NMP SPD nodes

The industry-readiness of SPD network for such critical applications should include the following:

- to develop and design warning systems which include: understanding and mapping the hazard; monitoring and forecasting impending events; processing and disseminating understandable warnings to administrative authorities and the population, and undertaking appropriate and timely actions in response to the warnings;
- to build special software packages for all SPD functionalities of interest, which are particularly useful to manage SPD services to administrative authority and the population;
- to facilitate planning, coordination, and implementation of risk-reduction measures;
- to build planning and policy decisions for preparedness, response, recovery, and mitigation at all SPD levels;
- to improve the quality of analysis of hazard vulnerability and capacity assessments, guide development planning, and assist planners in the selection of mitigation measures;
- to provide emergency communication and timely relief and response measures.

Applying Nano and Micro Technologies (NMTs) in the application domains of pSHIELD needs validation of NMP SPD devices under the application environment. The development of advanced MEMS/NEMS technologies for such applications faces a dilemma in successfully "maturing" new concepts. There are standard measures for evaluating the maturity of technologies, known as the Technology Readiness Level[22] (TRL) scale that has now found

[22] https://docs.google.com/viewer?a=v&q=cache:FBs4umuTb64J:www.smdc.army.mil/Contracts/BAA/DoD-TechnologyReadinessLevels.doc+technology+readiness+level+definitions&hl=en&gl=ch&pid=bl&srcid=ADGEESisfn4uj-dQj0txe_R3keWzM1AMlU7t_6ls6w4Y6-l5lBSVO2bOxn-KiORoIT3QQ7Ecx6NMba66G_zfybAbYZKIGhfsKEac5oVXZpUHESoTIDA-cO6iFaaRQGWDXJtK4UW7XzCI&sig=AHIEtbStAYo2KP085cG1n-8i1Vf80rdvhA

widespread use in industry. The TRL scale ranges from levels 1 through 9, with levels 1-3 being at the so-called “Low-TRL”, basic research into demonstrating the proof-of-concept, while levels 4-6 correspond to “Mid TRL” development, which is the reliable demonstration of subsystems based on the new technologies, and finally, levels 7-9 “High TRL” correspond to successful utilization of these subsystems in the selected scenarios.

The current research results performed in pSHIELD are showing that we are reaching low-TRL. A mid TRL development is planned for the period 2012-2016, and high TRL for 2020.

In spite of a strong enthusiasm expressed by scientists and engineers and huge amount of monies that has been invested in MEMS and NEMS it is encouraging for the European industry to make a strong development and industrialisation push toward a faster commercialisation of new technologies. pSHIELD and nSHIELD belong to the fields of nano- and micro-technologies. The sensors (temperature, pressure, acoustic, chemical, optical, magnetic, etc) involve also other technologies: nanotechnology, advanced material, biotechnology, and photonics. The new SPD devices and networks will be also successfully implemented in advanced manufacture systems.

3.3.2 Analysis of the industrial-readiness for NMPS

This section briefly highlights the most challenging aspect for achieving industry-readiness for NMPS devices. One of the major difficulties tasks in NEMS & MEMS is the integration of the micro scale devices components with the required nano- and micro-electronics for signal or function processing. It is also true for SoC in which components produced with nano- and micro-electronics should be integrated into a single chip. 3D integration today offers dramatic technology advantages for the future MEMS and NEMS.

The fabrication of such devices already started and there are made important achievements that are encouraging for pSHIELD & nSHILED technology developments. ESs evolves from isolated devices to always-on networked devices. SPD becomes a paramount issue for the success of new technologies. ESs security cannot be solved at a single layer, but rather is a system problem spanning multiple abstraction layers. In pSHIELD they are node, network, middleware, and overlay layer. The pSHIELD project open the door for new technologies in different application domains that will be fully exploited in the nSHIELD project. Development of the SPD devices should not be a separate process from the SPD networks. These two developments should go in parallel to take advantages of top-down and bottom-up approach. To achieve the goals of pSHIELD and nSHILED is important to take in consideration many important aspects that constrain our final success.

1. The end-user needs are driving our requirements and specifications from the begging. They are application-specific and differ from one application filed to other one.

2. The fundamental pSHIELD concepts and architectural solutions for SPD nodes and SPD networks should be maintained with an enhanced evolution from pSHIELD toward nSHIELD.

3. Innovative SPD system solutions should be patented first and then published to gain a competitive advantage for the European industry.

4. New technologies should be developed by a multi-disciplinary, multi-technology and multi-purpose strategic view by involving all key enabling technologies and other factors that help for a successful implementation of the research results into a mass production (KETs tri-pillar approach).

5. Developers should take care for aligning its R&D activities on the TRL scale in line with the OECD definition.

6. A joint effort of academy and industrial partners should have synergy toward common achievable goals of pSHIELD and nSHILED.

7. Industrial acceptance and market shares should be obtained through a strong participation in different standardization bodies and forums as well as customer involvements from the beginning.
8. Dissemination of the pSHIELD & nSHILED project results should be well planned to establish a world support in the targeted R&D fields.
9. Exploitations of the pSHIELD & nSHILED project results should be well planned to gain market share first in Europe and then worldwide.
10. Impacts of the pSHIELD & nSHILED project results should be based on large scale and long-road map strategy with economical and other societal benefits at European level.

The MEMS and NEMS ESs need to support various security solutions in order to deal with one or more of the security requirements described earlier. These requirements present significant bottlenecks during the ES design process, which are briefly described in section 3.2.2.

Reaching technology / industrial-readiness for NMPS nodes and WSNs with SPD functionalities and services require a multi-dimensional strategy with clear focus on what is achievable on short medium and long term.

4 FPGA Power Node Prototype

The transition from a laboratory proof-of-concept of a power node into an industrial and real market design requires some special concerns in four main areas:

- Security, Privacy and Dependability
- Certifiability
- Hardware and development cost
- Time-to-market

First of all the required level of Security, Privacy and Dependability must be identified, in order to decide upon the design of the system and the quality of the components.

Then, a special concern related to industrial embedded systems is certifiability. This affects not only the whole system design but also the components used not only hardware and software, but also the used IP cores inside the FPGA.

Hardware cost reduction is especially important in the mass-market, where the production of a high volume of units justifies any reduction in hardware components' cost. Regarding Power Nodes, they are expected to be used in the development of specially-designed solutions, so the development cost is the most important factor influencing the final system cost.

Finally, time-to-market is vital to the companies' competitiveness, implying that the products or systems development must be as short as possible.

4.1 Recommendations for real-life requirements from industrial implementations

Regarding the identified concerns related to the development of applications that must compete in the market, and from the experience gained from the development of a Power Node prototype, we have extracted the following recommendations for industrial implementations of SPD Power Nodes:

- The highest required SPD level for the Power Node must be clearly identified. This influences the level of design redundancy for both software and hardware components, increasing dependability. It also influences the choice of encryption algorithms, cryptographic keys management, etc., for increasing security and privacy.
- When a small number of SPD Power Node units are required, the use of FPGAs is recommended due to its flexibility to incorporate the different components of a SPD Node, and reduced development costs. However, a judicious choice of the correct FPGA is mandatory for retaining cost and development time.
- The development of SPD Nodes with a high volume of produced units requires, on the other hand, the use of other technologies, such as ASICs, which reduce cost and increase dependability due to the increase in technology robustness.
- When certifiability of the SPD Node is a concern, special care must be taken in the choice of third-party components (software and hardware), as these should be already certified, facilitating the process of certification of the whole Node.

- The design and implementation of a generic SPD Power Node with a wide range of capabilities and services offered is recommended. These high-capability nodes could be used in a large variety of applications, where each component could be enabled or disabled. These nodes would decrease the development time of the application, reduce costs, and facilitate certifiability. These nodes should also provide easy integration of non-SPD compliant modules.

The previous recommendations and further requirements have been identified from the analysis of the following application contexts:

- security and e-security,
- radar data processing,
- oil&gas marine exploration,
- situational awareness.

Security and eSecurity

Many e-security processes revolve around collecting data and processing it as fast as possible. This data can be gathered by a network of sensors whose nature and type may vary from surveillance cameras to computers that check the traffic in proximity of network nodes. The amount of the data to be analysed could be overwhelming, opening to solution involving high performance computing (HPC).

The analysis of the datasets could be static, near real time or real time.

The more real time the analysis become the higher is the chance to react promptly to a problem (an intrusion, an attack or any other behaviour that put at risk the security domain, real or cyber).

Due to the big size of the datasets involved, the latency introduced by the distance between the data gathering points and the central elaboration system could kill the opportunity react quickly to an event.

To fully benefit from real time analysis, computation has to take place locally, close enough to the “sensors” and it should be supported by computers that are not only powerful but also able to perform a specific function very quickly.

In this sense, the Power Node is an ideal solution because combines computational power, ruggedization and possibility to build specific algorithms into FPGAs.

The Power Node would function as local pre-processing unit, providing enough data crunching power to perform most of the analysis locally, leaving only to filtered and reduced output the need to be transmitted to a control centre or central processing unit via networks.

Radar data processing

Radar is a data-intensive measurement technique often requiring significant processing to make full use of the received signal. However, computing capacity is limited at remote or mobile radar installations thereby limiting radar data products used for real-time decisions. The use of portable rugged high performance computers allows accelerating the processing of high resolution phase-coded radar data that, if processed on-site in sufficient time, can be useful for decisions made during active experiment campaigns.

In some occasion the data is collected in such remote locations to prevent an easy upload to off-site high-performance computing (HPC) resources.

A similar need for portability, performance and ruggedness applies to Synthetic Aperture Radars (SARs). A SAR is a radar system which produces high resolution images using signal processing techniques. To obtain SAR images, a radar mounted on a satellite or an aircraft transmits pulses and receives the echoed signals.

In a typical SAR application, a single radar antenna is attached to an aircraft or spacecraft so as to radiate a beam whose wave-propagation direction has a substantial component perpendicular to the flight-path direction. The beam is allowed to be broad in the vertical direction so it will illuminate the terrain from nearly beneath the aircraft out toward the horizon.

Resolution in the range dimension of the image is accomplished by creating pulses which define very short time intervals, either by emitting short pulses consisting of a "carrier" frequency and the necessary "sidebands", all within a certain bandwidth, or by using longer "chirp pulses" in which frequency varies (often linearly) with time within that bandwidth. The differing times at which echoes return allow points at different distances to be distinguished.

The resolution of the received raw SAR image is very low. However SAR can produce high resolution images using signal processing. SAR signal processing has been implemented on special purpose architectures and on HPC platforms.

Due to the high cost of the special purpose SAR processors, HPC platforms are becoming popular for SAR processing. The most time consuming task in performing SAR signal processing is Frequency Domain Convolution(FDC).

Another major problem in performing SAR signal processing on High Performance Computing platforms is the cost of communication. Partially processed data should be moved between processors for subsequent processing. This implies large communication bandwidth between processors.

To fit these needs the Power Node should be engineering to consider these requirements:

- High processor power,
- Many core architecture,
- High I/O bandwidth,
- Portability and ruggedness (processing may be required locally in harsh or moving environments).

Oil&gas marine exploration

The Oil&Gas industry has always used supercomputers and high performance computers (HPC) in 2 main areas of application:

- oil and gas exploration,
- reservoir management.

The first comprises the processes of looking for new oil and gas reservoirs through marine and ground exploration. In this area of application, HPCs are specifically used to pre-process and process seismic data, whose interpretation can reveal the presence of oil or gas reservoirs.

The second is related to an area of reservoir engineering in which computer models are used to describe fluids (oil/water/gas) and its flow dynamics in the subsurface geologic formations.

Oil&gas exploration is performed in 2 main ways, in the sea and on the ground, following the same process: charges spread on the ground or sea are blown, the sonic waves resulting from the blasts are reflected either by the sea bottom or by the ground and the reflected waves are measured by probes. The probes send large quantities of data to computers installed locally on the boats or on the lorries. The marine exploration requires much more local computational power due to the large data volume collected. Normally, the data collected from the probes is pre-processed (pre-filtered) locally before being taped and sent to a data center for the processing and visual interpretation.

The pre-processing requires computational power, large storage facilities and equipment that can resist to vibrations and saltiness corrosion.

In this context, racks of Power Nodes connected together would fulfil the requirements of resilience and robustness better than the currently adopted solutions, which in most cases are normal data center equipment mounted in shock resistant racks and subject to frequent faults.

The requirements of such embedded high performance system are:

- processor powerful enough to perform large volume data analysis,
- high speed I/O to transfer data to Infiniband based storage,
- high memory bandwidth,
- vibration resistance,
- resistant to corrosion .

Situational awareness

The Power Node would allow the compute technology and performance levels typically associated with HPC to be applied to the most demanding processing problems using open architecture rugged hardware. A key element of these systems is high performance interfaces, such as Serial RapidIO and PCI Express.

One application that serves as an example of how the Power Node brings HPC technology into traditional embedded defence and aerospace applications space is a situational awareness system that combines clusters of Intel processor and leading edge commercial FPGAs to deliver real time visual sensor information into wereable displays. In this HPEC (High Performance Embedded Computing) system, data from the platform's external visual sensors (which may comprise a wide number of different sensor types) is aggregated and, depending on which direction an individual user's vision is oriented, the system can deliver the appropriate visual data to that user's wereable or helmet display with smooth, realistic imagery.

This challenging application requires several teraflops of processing power and many gigabytes per second of bandwidth. To fit the computational power needed within an embedded system, it is required to have high density, speed, fast I/O and generous bandwidth.

This can be accomplished combining latest Intel CPUs, such the Xeon 5600 series, with FPGAs that can handle the algorithms. The bandwidth and the speed in I/O can be achieved by using Infiniband protocol to connect multiple power nodes together and form a cluster that can put up with a very demanding computational workload.

A potential promising development of such application would be in equipping the Power node with GPUs to better handle the sensor data analysis.

4.2 Lessons-learned for the adaptation of lab prototypes

From the construction of the SPD Node prototype and demonstrator, we went through several difficulties and took several decisions, which should be used as lessons for both future prototype implementations and industrial implementations:

- A careful choice of hardware platform (FPGA and development board) is essential. It is thus recommended that the FPGA should have the necessary capabilities to accommodate system requirements, such as partial reconfiguration, a soft core, a hard core, memories, etc.

- The decision about whether using or not an operating system should be made based not only on the application software requirements (e.g. the need for real-time guarantees), but also on the simplicity to use its native features for accessing devices (e.g. TCP/IP stack).

- Proper selection of IP core is of highest importance. The free soft cores offer freedom of indoor modifications and don’t tie to licenses costs, but may lead to increased implementation costs and time due to possible incompatibilities with some particular hardware and the lack of technical support. On the other hand proprietary soft cores, usually provided by FPGA producers, have full technical support and high compatibility with wide range of hardware; nonetheless the cost of licenses must be considered.

- FPGA based Power Nodes are usually robust enough to run TCP/IP based communication, still software and hardware providing TCP/IP stack should be light enough to not overwhelm the node. So communication constraints should be duly defined in advance, before farther progress in node development.

4.3 Analysis of industry-readiness for pSHIELD-based monitoring

It is expected that pSHIELD project follows European industrial standards, and collects the SotA technologies in one consistent specification, thus the result of the project should be a list of clear guidelines for ESs developers and industry in general. Those guidelines ought to be widely accepted and welcome by industry, leading even to proposal of new standards. Concluding, it is perceived that industry is not only ready, but expecting that kind of solutions, since pSHIELD proposes not a revolution, but evolution of currently used solutions, although in more mature and consistent form.

In the area of power node ESs equipped with FPGA chips, the implementation of pSHIELD projects results will allow to lower production costs and to prolong active lifetime of developed devices. It will be obtained mainly by usage of the new approach of FPGAs Run Time Reconfiguration and standardized framework for development of future ESs. The pSHIELD framework architecture allows to speed up and standardize ES solutions development, while run time reconfiguration will allow the modification of devices operating in the field to adjust their work to changing industrial requirements and prolong their operational lifetime.

5 Middleware Prototypes for the demonstration of SPD-oriented composability

In this paragraph will be explained the industrial and real life adaptation of the prototype middleware prototype and composability property.

5.1 Recommendations for real-life requirements from industrial implementations

With the pSHIELD project, partners of the consortium will have the opportunity to participate in the design of an innovative communication platform, conveying information from sensors to centralized infrastructures, for the management of critical operations or situations. The technological framework refers to Embedded Systems and their utilization in an environment with adequately increased SPD levels during operation. A basic notion and desirable feature of pSHIELD regards the possibilities to abstract components from the platform and create pSHIELD subsystems, depending on the needs of specific applications.

This composability is what partners, especially the industrial ones, wish to, firstly, consolidate and later exploit in the form of a SHIELD prototype. pSHIELD product can be incorporated in individual company business plans or form the basis for a common consortium exploitation plan, that will include implementation of applications in specific business areas.

A wide diversity of industrial control activities can be served by ESs and WSNs, including supervision of assembly line, energy management, automation, process control and inventory tracking. The concept of integrating heterogeneous platforms exploiting their composability capabilities, aims at offering optimized resources management, through the “ad-hoc” formation and collaboration of sub-networks, according to each time needs and availabilities. The consortium will investigate the possibility of utilizing the outcomes of pSHIELD in the development of a series of industrial control applications. A brief description of the most important expectations and requirements for such applications, through representative examples, follows.

Logistics is an aspect of industrial life, which HAI believes can be substantially benefited from the use of sensor networks with synthetic capabilities. Tagging on materials allows the sharing of useful information (ID, location) between all involved parties in the procedures of manufacturing, transporting, storing and ordering products. Collaborative sensor networks render these products traceable all along the path between assembly line and customer delivery.

HAI, for example, will investigate the possibility of embodying pSHIELD exploitation perspectives in its current evolving business plan. Prominent application areas in this plan are Infrastructure Security and Border Surveillance, having a lot in common with Urban railways protection and Voice/Facial recognition (two of the selected SHIELD application topics). The development of high reliable security systems applicable in various aspects of social life, are in the front line of priorities. Cameras and sensors can be used to detect hazardous and illegal actions (e.g. border crossings). The devices usually have to be deployed at remote in between distances and far from the operation center, on mountainous or harsh terrains, etc. If they are able to be organized, through their heterogeneity, with great composability, enhanced overall situational control and awareness for authorities could be possible.

5.2 Lessons-learned for the adaptation of lab prototypes

Located in a heavily polluted industrial zone, HAI will rely on the use of wireless sensor networks in the effort to mitigate the conditions for the company itself, the neighbouring industries and the area inhabitants. *Environmental improvement* can be achieved by reducing the release of toxic substances responsible for air and water pollution. Sensor networks can be used to monitor these unwanted releases. A collaborative grid can be formed with the installation of sensors in the nearby plants also, granting the possibility of dynamically configured sensor networks, according to occasional environmental needs.

HAI, being a sizeable organization, is especially interested in an effective *energy management* mechanism. Sensors and actuators can be used, firstly to monitor the indoor conditions and possible losses in the energy balance and subsequently to control the energy distribution or take corrective actions. Composability offers the possibility of different user panels and administrative schemes. For example, an energy management center could supervise the distribution of resources in the plant. Alternatively, in a more generalized format, many involved parties could play a hierarchical role, from the power provider company to a regional or a building block administrator.

5.3 Analysis of industry-readiness for pSHIELD-based monitoring

Another application in the same domain concerns the prevention of natural disasters and their impact in public safety. Cameras and thermal sensors are used for the notification of abnormal conditions and derivation of alarms. The critical operations of fire fighting, involves the communication of a number of authorities, from fire and forest inspection departments to local communities, ministries, police and governmental crisis operation centres. Their effective organization, vital in these situations of high emergency, could be assisted with a composable SPD network platform, allowing each part to have access to the kind of information of its specific interest.

pSHIELD is expected to contribute significantly in the implementation of these business plans, since its values and concepts (security, privacy and dependability in the context of embedded systems) are of great importance in this area. Furthermore, the results of demonstration will depict platform capabilities, limits and commercial potentialities, while simultaneously they will guide us to the future research field and improvements.

6 Hardware prototypical implementation of specific layers

In this paragraph will be explained the industrial and real life adaptation of the prototype developed for the real case scenario, the monitoring of freight train.

6.1 Recommendations for real-life requirements from industrial implementations

The Pshield prototype for monitoring system is based on WSN. The principal real life requirements are related to the use of WSN in a real scenario. In particular this are related to the: lifetime of nodes, security attack of nodes, area coverage by nodes, maintainability cost. Infact the node should be self-powered, this is related also to the energy conservation, that because of the reduced size of the sensor nodes, the battery has low capacity and the available energy is very limited. Despite the scarcity of energy, the network is expected to operate for a relatively long time. In these situations, the quality of the radio communication might be extremely poor and performing the requested collective sensing task might become very difficult.

Also is important the physical security, as networks grow, the vulnerability of network nodes to physical and software attack increases. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Therefore, routing protocols must be resilient against compromised nodes that behave maliciously. Ensuring that sensed information stays within the sensor network and is accessible only to trusted parties is an essential step toward achieving security.

At last the maintenance cost, the initial deployment and configuration is only the first step in the WSN lifecycle. The total cost of management for a system may have more to do with the maintenance cost than the initial deployment cost. Throughout the lifetime of a deployment, nodes may be relocated or replaced due to outages, and discharged batteries. In addition, reintegrating the failed nodes adds further labor expenses. An approach to limit interventions would be to increase the lifetime by adopting a trigger-based sampling strategy: sensors start to acquire data only when given conditions are met. However, this approach introduces a further coordination problem among sensors.

6.2 Lessons-learned for the adaptation of lab prototypes

The monitoring architecture developed in deliverable D6.3, is at this moment an adapted lab prototype, tested in a real scenario. So, for this reason, is done some adaptation and changes from the lab prototype. The future work and actual adaptation are follow:

- For future can be considered a experimentations on a train with more vagons. As matter of fact, the experimentation was done on a single car and It will be useful to use more network and more wagons with ad hoping protocol between sensors, and data fusion from all networks.
- For the installation will be useful to have a manual in order to know the correct position of nodes, for avoid a signal interference and isolation of communication.
- The sensors installed on car can they be provided with an enclosure for protection by bad whether, to avoid tampering or vandalism the can be installed in not visible position or not easy to reach.
- Also is important to know the frequence for wi-fi transmission in order to avoid collision, data loss or delay or electromagnetic interferences.

6.3 Analysis of industry-readiness for Pshield-based monitoring

The first step for the industrial implementation is the adaptation to standard in railway security, for the use of electromagnetic instrumentation, range frequency, survivability and maintainability of instrumentation on vehicle board. 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. This standards concern Electromagnetic compatibility, use of the range frequency, protection of the communication. CENELEC is the European Committee for electro technical Standardization and is responsible for standardization in the electro technical engineering field. CENELEC prepares voluntary standards, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market. The technology sectors are different: vehicles, medical, telecommunication, etc..

There is also a specific sector for the railways, 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. To help achieve this, the EU 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 norm and regulation, relative to the demonstrator, are the follow:

1. EN 50121-3-2 *Railway application – Electromagnetic compatibility – Rolling stock apparatus.*
2. EN 50124-1 *Railway applications – Insulation coordination – Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment*
3. EN 50159-1 *Railway applications – Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems.*
4. EN 50159-2 *Railway applications – Communication, signalling and processing systems - Part 2: Safety related communication in open transmission systems*

The first prepared by the CENELEC committee, deals with electromagnetic issues in the railway domain. It is divided into five parts, addressing different aspects:

Part 1 - A general description of the electromagnetic behaviour of a railway system is given, summarizing the most important phenomena problems.

Part 2 - Emission of the whole railway system to the outside world. A setup is described for electromagnetic field measurements and limits are set. Basic statistical tools are introduced in order to get a representative estimation of the measured quantities.

Part 3 - This part is divided into two subparts, taking a closer look to emissions generated by electric trains, both as a whole and by its elementary parts.

Part 4 - Emission and immunity of the signalling and telecommunications apparatus. Further tests are described in order to assess the electromagnetic-compliancy of signalling devices.

Part 5 : Fixed power supply installations. Emission and immunity tests are described for devices performing power-supply tasks.

In the context of the research project the most important parts are the second and the third one, dealing with radiated emissions tests for rolling stocks as a whole

The second standard talk about the Coordination of isolation in the specific field of traction. The first part covers the basic principles and criteria for selecting and creepage distances refer to the isolation voltage required, the degree of protection circuits and the degree of pollution present. This standard also indicates the values of frequency withstand the complete equipment.

The third 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 fourth 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 important for industrial readiness is the observation of this norms and standard, in particular for the use of frequency of instrumentation and communication. This is fundamental also for the installation of sensors and instrumentation, is useful a manual for the installation in order to identify the ideal position for not obstacle the communication between sensors and the outside communication between control room.

The use at a range frequency is important also for the noise of signal for the railway asset, as matter of fact, it knows that some range of frequency con be a disturbance for train and their instrumentation.

7 Conclusions

This document aims at guaranteeing the proposed architecture components to be future-proof, and to support the real-world requirements for industrial operations. In particular, will summarize the experiences from the demonstration, Nano micro-persoal node, power node and middleware prototype, including: lessons-learned for the adaptation of lab prototypes towards quasi-autonomous operations, analysis of industry-readiness for pSHIELD-based monitoring and recommendation of real-life requirements. Based on these real-world experiences and requirements, the document will further summarize recommendations for further industry-related developments of SPD functionality.

References

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

[2] D. F. Aranha, R. Dahab, J. López, L. B. Oliveira, “ Efficient implementation of elliptic curve cryptography in wireless sensors” Advances in Mathematics of Communications, vol. 4, issue 2, pp. 169-187, 2010.