SHIELD
NEW

# SELEX Elsag WP4

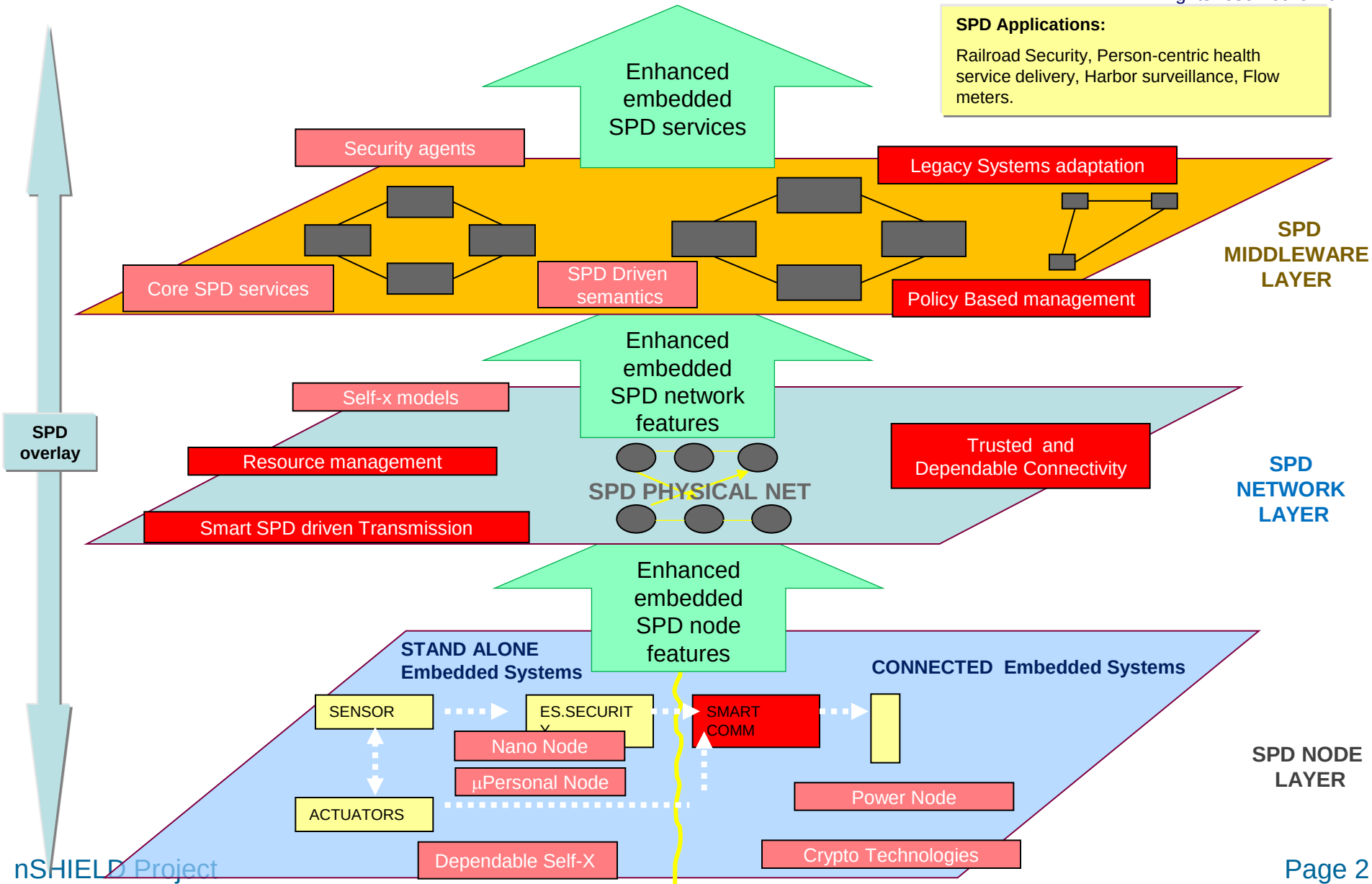
## Pre-Review meeting

## 11th – 12th September 2012

*ARTEMIS 2010 -1*
*Project Proposal No. 269317*
*ASP6: Inter-networked ES for Security and Critical Infrastructures Protection*

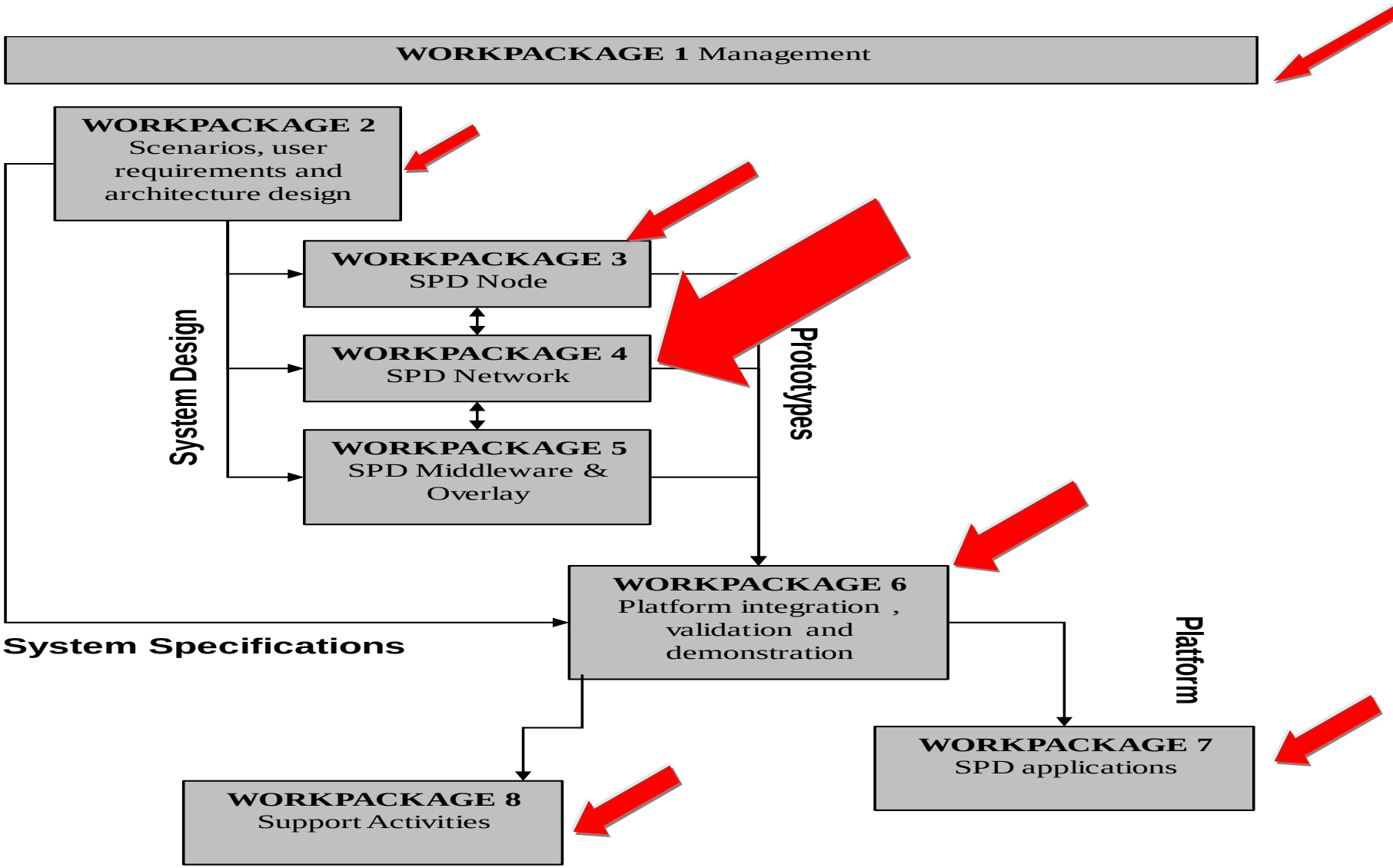
# nSHIELD functional architecture





# nSHIELD: Block Diagram & WP4 partners effort





# WP4 - SPD network – The SCOPE in synthesis



- The main objective of **SPD Network** is to provide Trusted and Dependable Connectivity to Embedded Systems through the implementation of a **reconfigurable radio system** capable:

1. to **maintain awareness** of the operating scenario,

2. to **detect possible threats** and to **counteract** in such a way to ensure communications integrity to the maximum possible extent by **reconfiguring the single nodes** and/or the system itself.

3. To **smart manage the crypto Keys** in order to handle security in lightweight devices and in highly dynamical networks.

# WP4 - SPD network – Basic Concepts



**COGNITIVE ENGINE** defines an optimal configuration according to the environment and the goal (highly reliable communications, efficient use of the radio spectrum, maximize the throughput while keeping the *PER under a threshold, …) being

**AWARE** of its surrounding environment (i.e., outside world), and uses the methodology of understanding by-building to

**LEARN** from the environment, including intrusion detection and

**ADAPT** its internal states to the statistical variations in the incoming RF stimuli, intrusion alerts by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, modulation strategy, key redistribution, data base and intrusion signature updates) eventually in real-time.

***PER: Packet Error Rate**

# WP4 - SPD network – Activities Carried Out



Understanding of the main features needed for making the SHIELD SPD-Based Radio system working, that are:

1. Reconfigurable radio components with waveform parameters (frequency, bandwidth, …)
2. Sensing mechanism to acquire awareness about available/used resources
3. Different IDS approaches (misuse vs. anomaly detection, architecture) taking into account the requirements of sensor networks
4. Cognitive algorithms elaborating the available informations and taking countermeasures decisions against the identified threats
5. Simulator adaptation born for image analytics and to be used for Smart SPD transmission environment simulations
6. Embedded platform adaptation to validate SHIELD cognitive algorithms

# WP4 – SPD network – Achievements



- Analysis of various waveforms
- Adaptation of HW and SW of multi-core platform nShield-OMBRA for the cognitive algorithm validation on embedded system
- Study of the spectrum sensing features for Cognitive Radio
- Adaptation of sensing part of the Cognitive Radio simulator for nSHIELD

# WP4 – SPD network – Achievements



- Selection of the footprint of wireless communication protocols basing on the impact on performances on commercial devices.
- Transmission parameters smart adaptation according to radio resources observation towards trusted and dependable connectivity implementation
- Implementation of a Cognitive Radio Node software simulator able to automatically detect a threat and adjust internal radio parameters to counteract
- Providing security in lightweight and networked embedded devices (novel cryptographic scheme)

# WP4 - SPD network – Work progress of nShield



**nShield** items that started to be:

- **detailed,**
- **implemented,**
- **tested**
- **validated:**

- **Sensing:** awareness (active users, bandwidth, modulation, frequency, …)
- **Cognitive Manager:** decision making, reasoning, cross-layer optimization and resource allocation
- **Radio:** adjust radio parameters according to cognitive manager (dynamically exploitation of available resources, …)
- **Networking:** spectrum-aware routing, cognitive transport protocols
- **Optimize the IDS** architecture regarding distributed or centralized approaches or a combination of both
- **Reputation based IDS** approaches are to be implemented
- **Key Management**
- **Adaptation of the simulator**

# WP4 - SPD network – Task Leader SCOM



- **Objective**:
  - Task 4.1 Smart SPD driven transmission
    - **SE;** SG; THYIA; TUC; UNIGE
  - Task 4.2 *Distributed self-x models*
    - **ATHENA;** *THYIA, TUC, UNIGE, UNIUD, SE*
  - Task 4.3 *Reputation-based resource management technologies*
    - **HAI;** *SE, TECNALIA, INDRA, MGEP, TUC, UNIROMA1*
  - Task 4.4 *Trusted and dependable Connectivity*
    - **ISL;** *SE, SCOM, TECNALIA, HAI, MGEP, THYIA, TUC*

# T4.1 – Smart SPD driven transmission – Leader SE



- Implementation of smart SPD driven transmission techniques to nano-node level
- Identification of new technologies enabling smart SPD driven transmissions
- Validation of various waveforms, both at the physical and MAC layer, through simulation and implementation on ES
- Adaptation of HW and SW of multi-core platform for the cognitive algorithm validation on embedded system
- Identification of spectrum sensing features for Cognitive Radio analysis
- Optimization of sensing part of the Cognitive Radio simulator for nSHIELD

# T4.2 - Distributed self-x models - Leader ATHENA



- Study of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks, aiming to reduce the vulnerability to attacks depleting communication resources and node energy.

- Identification of how the nSHIELD framework will take advantage of physical interoperation for providing reliable and efficient communications even in critical channel conditions. For instance using adaptive and flexible algorithms for parameter dynamic configuration such as adaptive modulation and coding and multiple antennas.

- Basing on channel measurements, provided by the physical layer, we will study how dynamically adapting the modulation, coding and data rate in order to meet the required QoS level (which will quantitatively and qualitatively verified with respect to SPD metrics)

# T4.3 - Reputation-based resource management technologies - Leader HAI



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

- Design and development of innovative resource management methodologies as efficient solutions based on trust and reputation-based schemes for secure routing and intrusion detection systems at the communication level

- Study the capability of authenticate resources and component without a central certification authority but basing on individual certification, allowing a complete interoperability with other platform layers

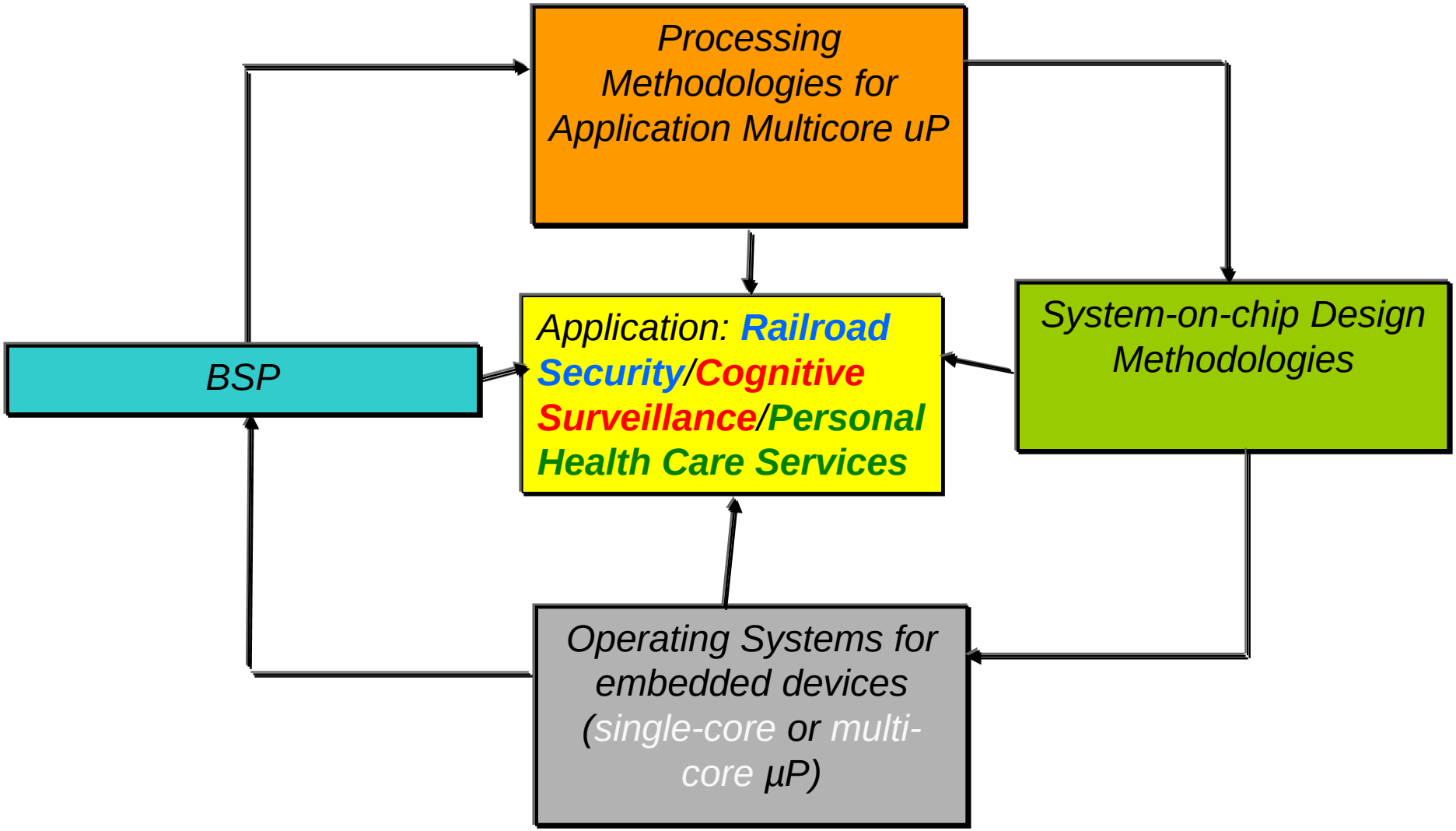
# T4.4 - *Trusted and dependable Connectivity – Leader ISL*



- Study of the requirements for lightweight link-layer secure communication in wireless sensor network scenarios
- Design and development of proper schemes focusing on confidentiality, integrity and authenticity of transmitted data, and relying on the existence of accessible key distribution centre and certification authorities
- Exploitation of features and methodologies developed from T4.1 to T4.3 as key element of Secure Service Chain (SSC), to guarantee secure and dependable transmissions/communications while respecting user privacy
- Integration of the proposed approach with other technologies developed in different nSHIELD's layers to generate added value to the entire system and validated in the selected application scenarios (see WP7)
- Study of the compliance with existing standards and technologies (according to our proposed built-in approach) as well as to the capability of guarantying the proposed architecture to be future-proof, to support the installation, download and upgrade cycle in a continuous improvement perspective

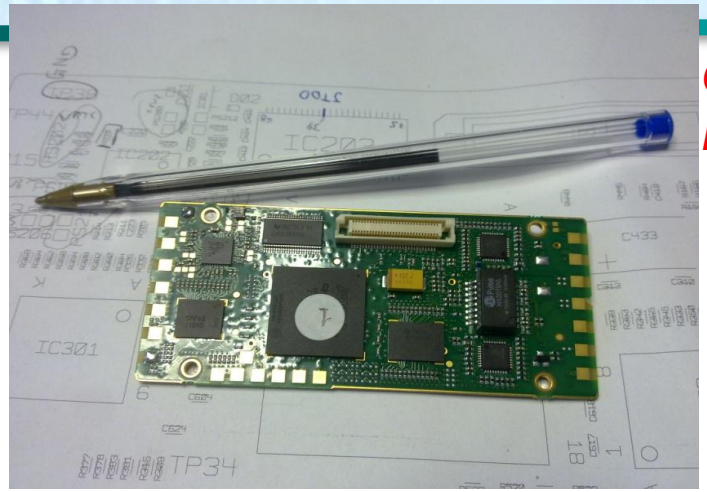
# T4.1 - SPD network – Embedded System OMBRA-SHIELD (Open Multicore Based Reliable Architecture)





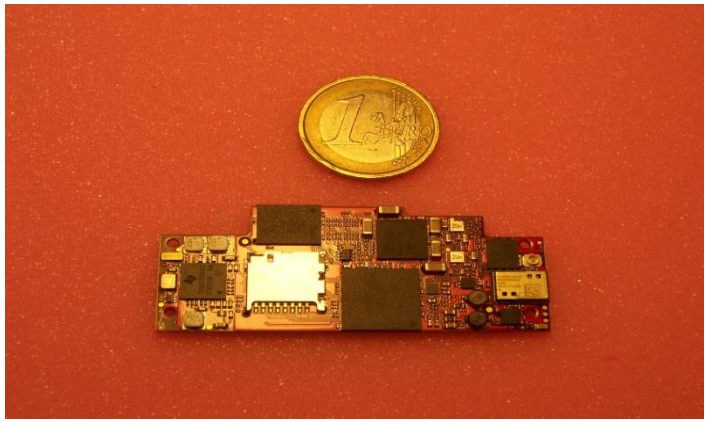
# T4.1 - SPD network – ES Computational Hardware





*Carrier Board OMBRA-nSHIELD*
*Example (40x80mm)*

*PCB Standard - PXA270 uP*
*Size (110x130mm)*
*WCP =~ 350Euro*



***PCB OMBRA-nSHIELD (18x68 mm)***
***OMAP uP, Xilinx FPGA***
***WCP (1K pieces) =~150 Euro***
***Computational Power 5X***