



ARTEMIS JOINT UNDERTAKING
The public private partnership for R&D in the field of Artemis



WP4

Project Review
29-30 September 2011 Oslo

ARTEMIS Call 2009 – SP6100204



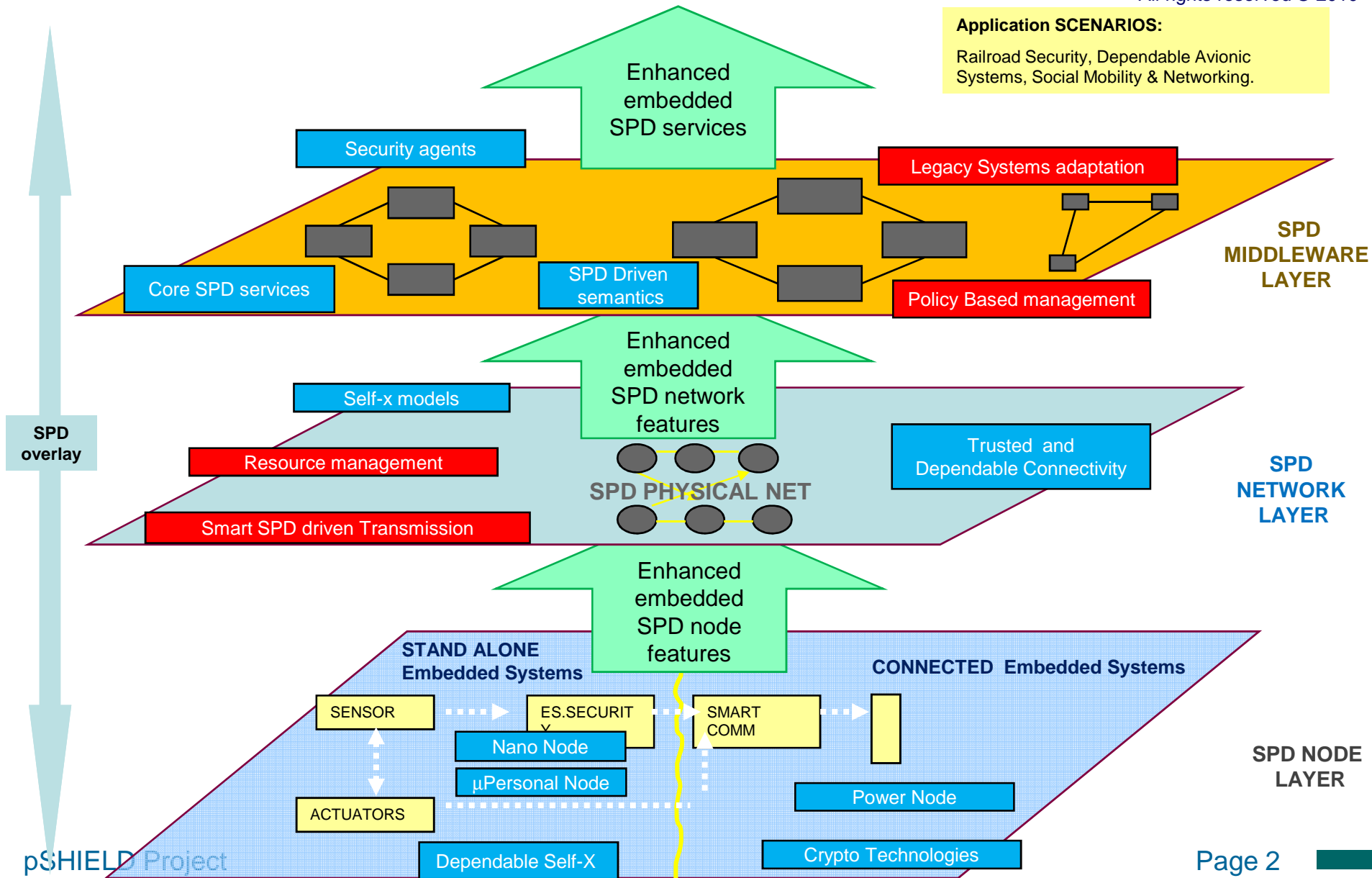
pSHIELD functional architecture



All rights reserved © 2010

Application SCENARIOS:

Railroad Security, Dependable Avionic Systems, Social Mobility & Networking.



- **Objective:**
 - Task 4.1 Smart SPD driven transmission
 - **SELEX Elsag**; THYIA; UNIGE
 - Task 4.2 Trusted and dependable connectivity
 - **MGEP**; ATHENA; CS; ESI; THYIA; UNIGE
- **Activities carried out:**

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

 - reconfigurable radio components with waveform parameters (frequency, bandwidth, ...)
 - sensing mechanism to acquire awareness about available/used resources
 - cognitive algorithms elaborating the available infos and taking countermeasures decisions against the identified threats
 - Simulator adaptation to be used for Smart SPD transmission environment simulations
 - Embedded Platform adaptation to validate pSHIELD cognitive algorithms



- Proposed **new technologies enabling smart SPD driven transmissions**
- **Performance analysis of various waveforms** has been completed to select best candidates for the foreseen applications, both at the physical and MAC layer
- **Realization and 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**
- Adaptation of **sensing part of the Cognitive Radio simulator for pSHIELD**



- Study of the **different IDS** (Intrusion **D**etection **S**ystems) approaches (**misuse** vs. **anomaly detection**, architecture, ...) considering sensor networks requirements
- Study the **real resource footprint** of **wireless communication protocols** (i.e. energy consumption) and its **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
- Research relating to the state-of-the-art technology **providing security in lightweight and networked embedded devices** (cryptographic scheme)
- Studies on the **setup of a general framework for secure communications** within heterogeneous networks comprising resource-limited devices

- **Status of output:**

- D4.1 SPD network technologies prototype (100%) – [M13] internal
 - Innovative approaches for SPD driven transmissions and Trusted and dependable connectivity
 - Spectrum Sensing for SPD driven transmissions and Trusted and dependable connectivity
 - Physical layer Techniques enabling SPD driven transmissions and Trusted and dependable connectivity
- D4.2 SPD network technologies prototypes report (65%) – [M17] public
 - Cryptography Framework
 - Trusted and Dependable Connectivity

Activities planned for the next months:

- Completing the **analysis of some blocks** spanning the ISO-OSI stack
 - **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

- Completing the **adaptation of the simulator**



- **Porting of some cognitive algorithms** on the Embedded OMBRA-pSHIELD platform

- Validation of the algorithms/concepts through simulations and OMBRA-pSHIELD

- Dissemination and Exploitation activities