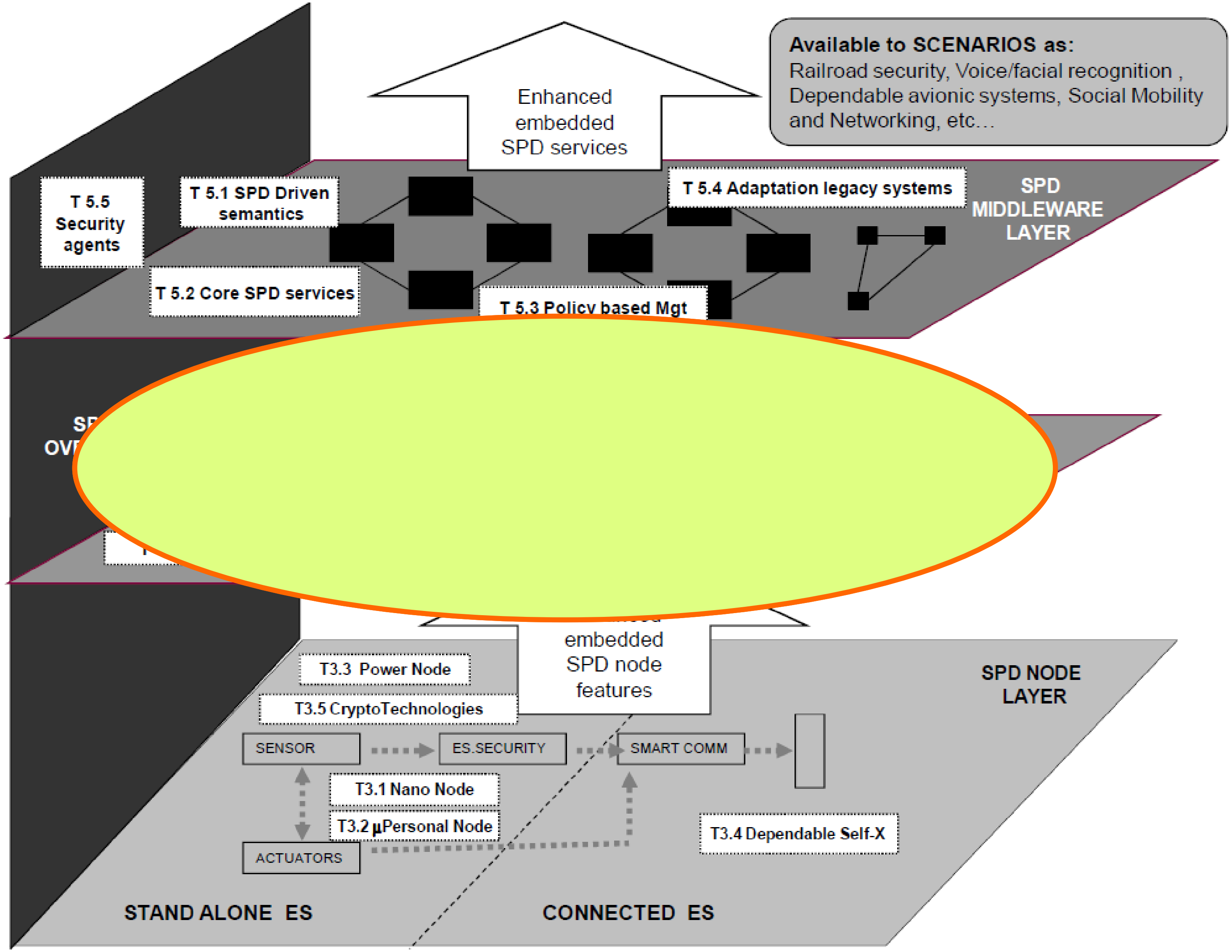
Annual review ROME 2012

nSHIELD

WP4 - Network

ARTEMIS

nSHIELD functional architecture



Enhanced embedded SPD services

Available to SCENARIOS as:
Railroad security, Voice/facial recognition ,
Dependable avionic systems, Social Mobility
and Networking, etc…

T 5.5 Security agents

T 5.1 SPD Driven semantics

T 5.2 Core SPD services

T 5.3 Policy based Mgt

T 5.4 Adaptation legacy systems

SPD MIDDLEWARE LAYER

SP
OV

embedded SPD node features

T3.3 Power Node

T3.5 CryptoTechnologies

SENSOR

ES.SECURITY

SMART COMM

T3.1 Nano Node

T3.2 µPersonal Node

ACTUATORS

T3.4 Dependable Self-X

SPD NODE LAYER

STAND ALONE ES

CONNECTED ES

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:
  - of **maintaining awareness** of the operating scenario,
  - of **detecting possible threats** and **counteracting** in such a way to ensure communications integrity to the maximum possible extent by **reconfiguring the single nodes** and/or the system itself.
  - of **smart-managing the crypto Keys** in order to handle security in lightweight devices and in highly dynamical reconfigurable networks.

Activities Carried Out

- Main features needed for making the SHIELD SPD-Based Radio system working:
  - **Reconfigurable radio components** with waveform parameters (frequency, bandwidth, …)
  - **Sensing mechanism** to acquire awareness about available/used resources
  - **Different IDS approaches** (misuse vs. anomaly detection, architecture) taking into account the requirements of sensor networks
  - **Cognitive algorithms** elaborating the available information and taking countermeasures decisions against the identified threats
  - **Simulator development** for studying and evaluating performances of the Security Aware Framework
  - **Embedded platform adaptation** to implement and validate SHIELD Security Aware Framework

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 starting to be implemented
    - **Key Management**
    - **Adaptation of the simulator**

Work package - objectives

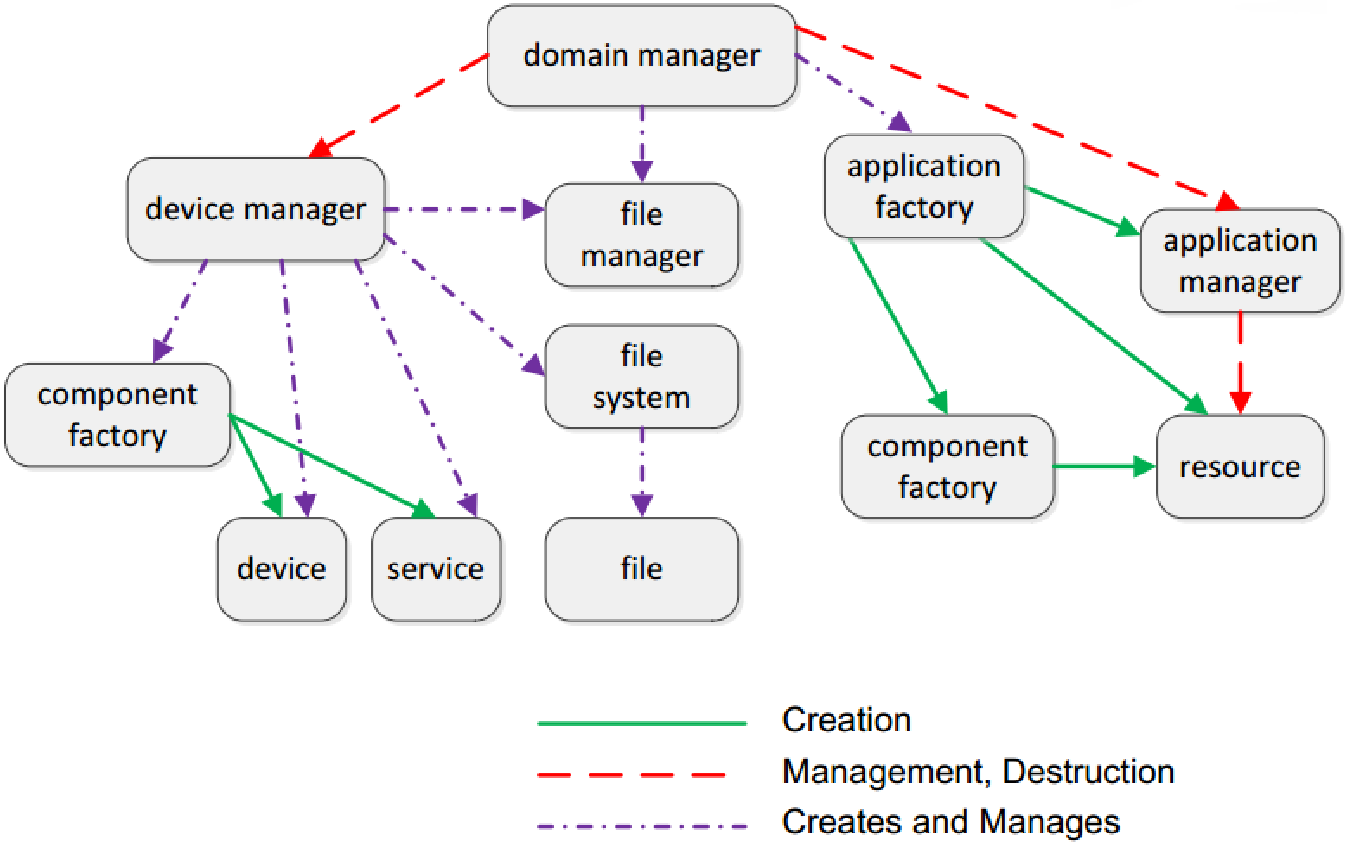
- Task 4.1 *Smart SPD driven transmission*
  - **SE;** SG; THYIA; TUC; UNIGE
- Task 4.2 *Distributed self-x models*
  - **ATHENA;** THYIA, TUC, UNIGE, UNIUD, SE
- Task 4.3 *Reputation-based resource management technologies*
  - **HAI;** SE, TECNALIA, INDRA, MGEP, TUC
- Task 4.4 *Trusted and dependable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

Smart SPD-driven transmission

- Goal: providing reliable and efficient communications even in critical (physical) channel conditions
  - Adaptive and flexible algorithms for dynamically configuring and adapting various transmission-related parameters
- Based on the Software Defined Radio (SDR) or Cognitive Radio (CR) technology
- Shall be SCA-compliant
- Security-aware framework
  - Deployment of different state-of-the-art technologies for detecting and countering reconfigurability-related and cognitive capability-related security issues and attacks

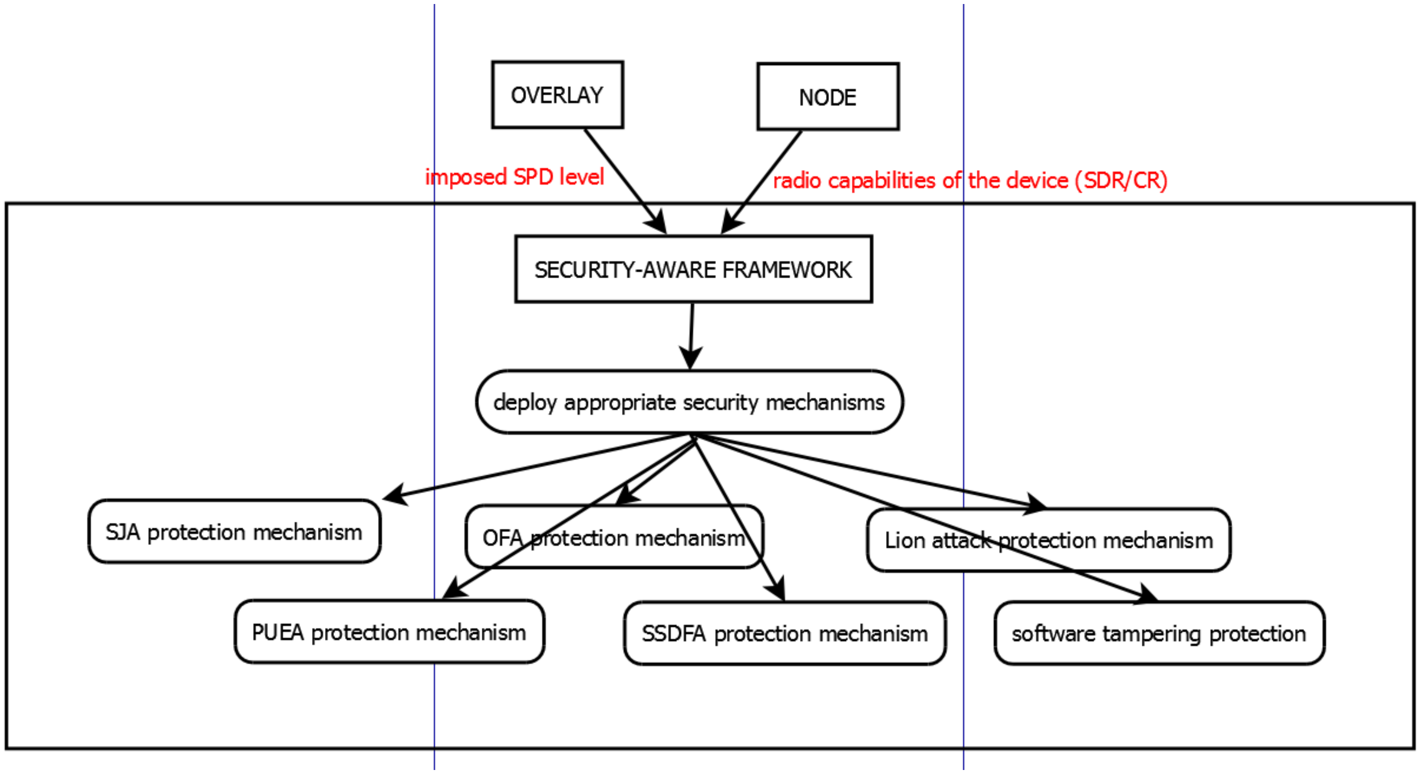
Smart SPD-driven transmission (2)

Software Communications Architecture
(*source: SCA 4.0 specification)*



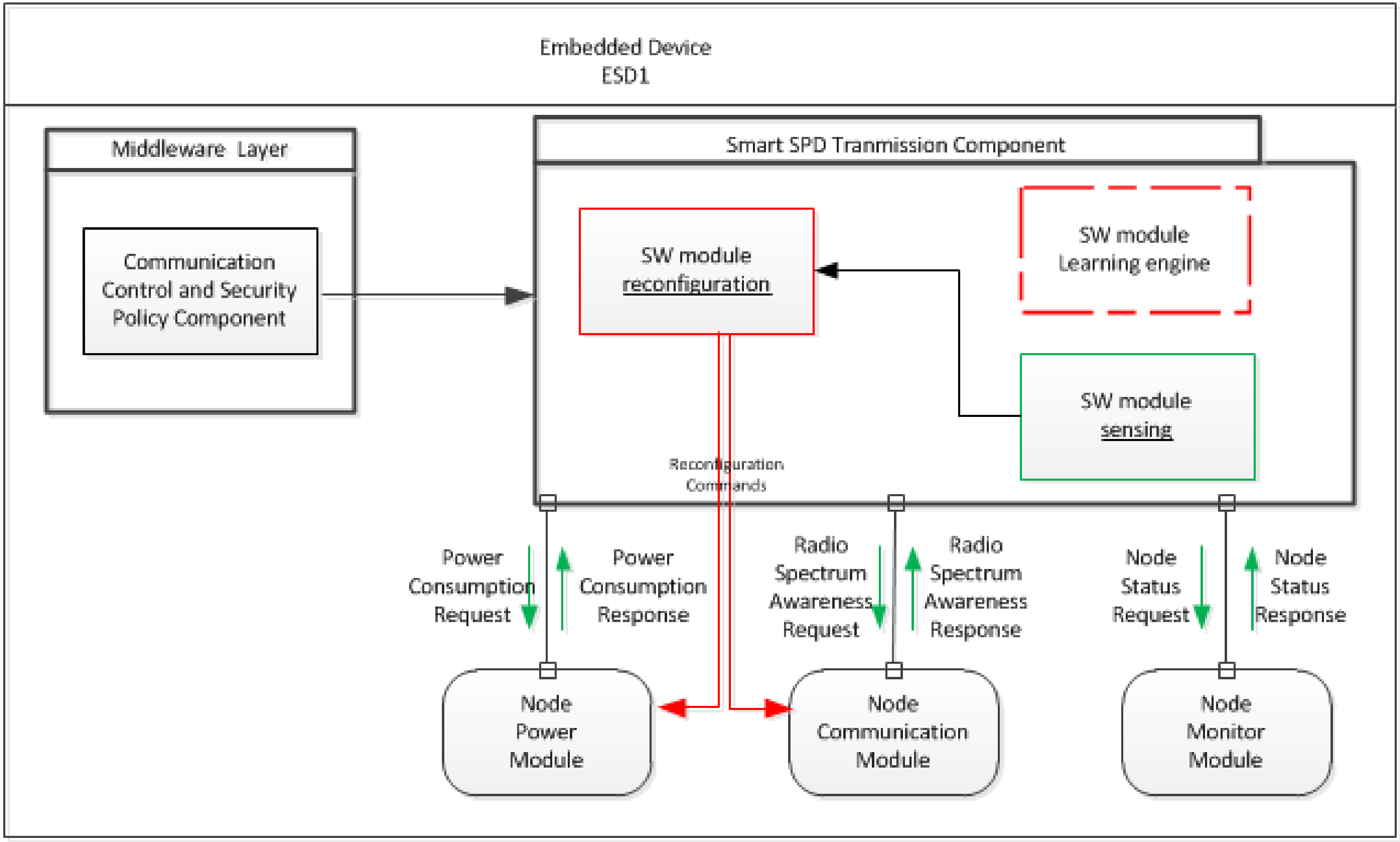
Smart SPD-driven transmission (3)

Security-aware framework (*source: nSHIELD deliverable 2.4*)


OVERLAY
NODE
imposed SPD level
radio capabilities of the device (SDR/CR)
SECURITY-AWARE FRAMEWORK
deploy appropriate security mechanisms
SJA protection mechanism
OFA protection mechanism
Lion attack protection mechanism
PUEA protection mechanism
SSDFA protection mechanism
software tampering protection

Smart SPD-driven transmission (4)

Trusted Network Routing Service
(*source: nSHIELD deliverable 2.4*)



Embedded Device
ESD1

Middleware Layer

Communication Control and Security Policy Component

Smart SPD Tranmission Component

SW module reconfiguration

SW module Learning engine

SW module sensing

Reconfiguration Commands

Power Consumption Request

Power Consumption Response

Radio Spectrum Awareness Request

Radio Spectrum Awareness Response

Node Status Request

Node Status Response

Node Power Module

Node Communication Module

Node Monitor Module

Distributed self-x models

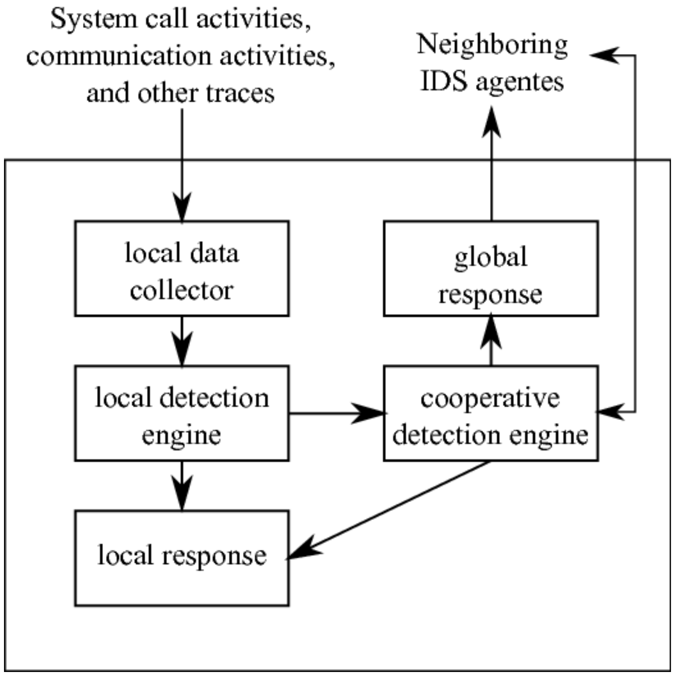
- Goal: Providing network transmission technologies to support the dependable self-x technologies at the node level by means of Cognitive Radio technologies
- Self-x refers to:
  - Self-(re)configuration
  - Self-management
  - Self-supervision
  - Self-recovery
- Evaluation of risks has been performed so far, with the following types of attacks identified and analyzed:
  - Side channel attacks
  - Denial-of-Service (DoS) attacks

Reputation-based resource management technologies

- Goal: Using information of nodes' past behaviours in order to estimate the current trustworthiness level
- Reputation and trust based Intrusion Detection Systems for WSN
  - New distributed approach (vs. centralized in pSHIELD)
    - Agent based detection minimises the communication needs
  - Both anomaly and specification-based detection
    - Anomaly detection using a simpler model (to reduce CPU and power consumption)
    - Coupled with specification based detection to enhance efficiency

Reputation-based resource management technologies (2)

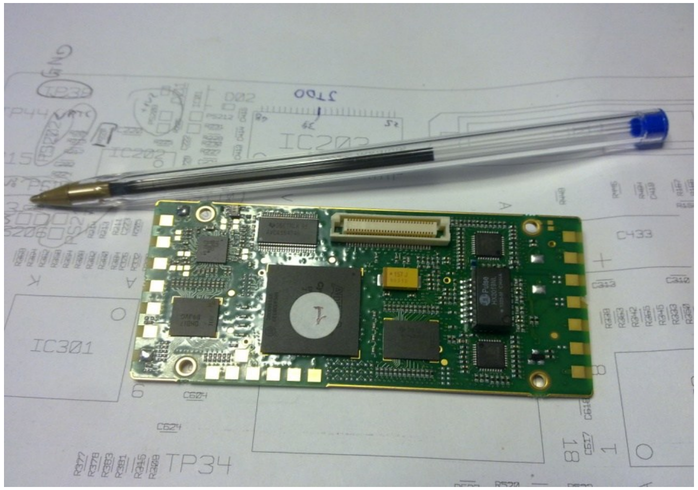
- Distributed detection
- Node monitors local activities
- If not sure about the nature of an activity, node contacts its neighbouring nodes
- Reputation and trust of a node set according to local and neighbouring information
- When anomalous activities are flagged locally, this information is broadcasted to the rest of the nodes


System call activities, communication activities, and other traces
Neighboring IDS agentes
local data collector
global response
local detection engine
cooperative detection engine
local response

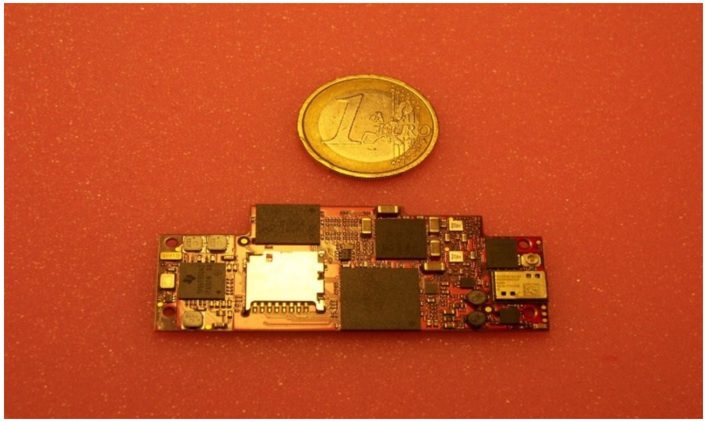
Trusted and dependable connectivity

- Goal: assuring communications integrity to the maximum possible extent
- Regarded at two levels:
  - *Trusted Network Routing Service*
    - Possibility of choosing between different routing schemes, based on the input of the reputation-based scheme
  - *Secure Data Exchange/Communication Service*
    - Encryption schemes to enable protection (and integrity) of data
    - Authentication schemes to verify identity of sender/receiver

ES Computational Hardware

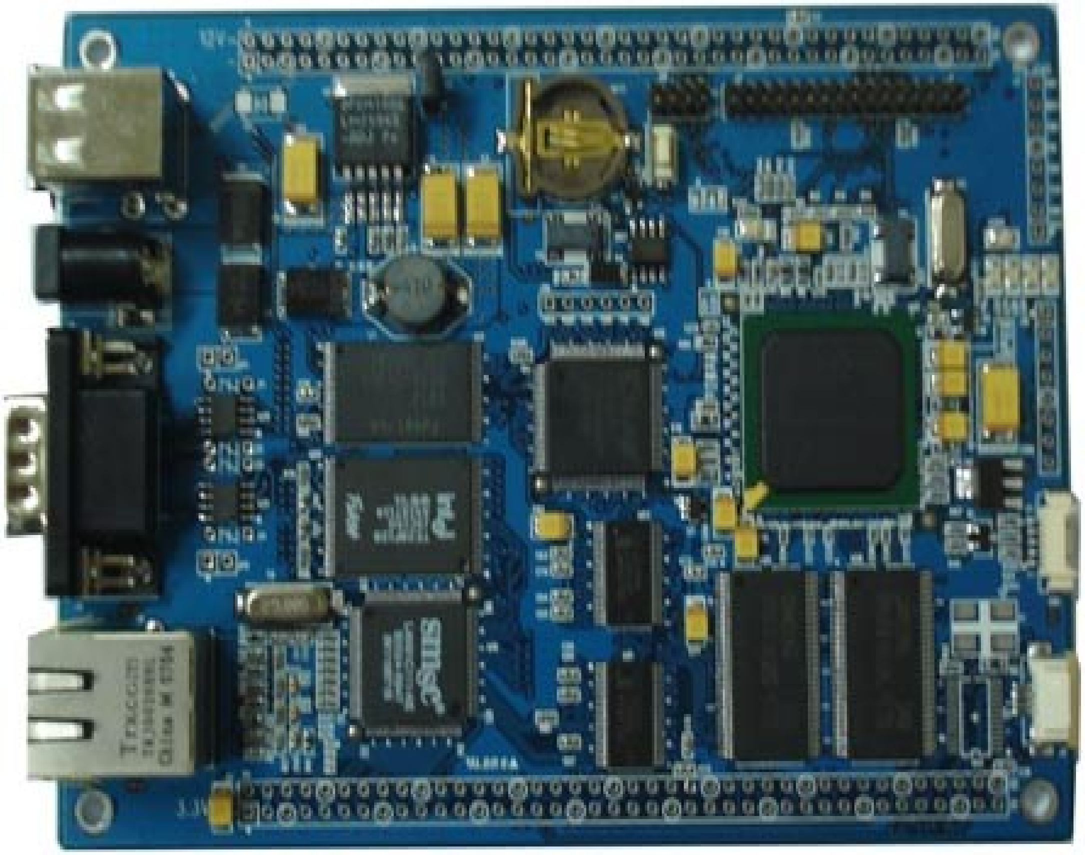


Carrier Board OMBRA-nSHIELD
Example (40x80mm)



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

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



The END

nSHIELD

Thanks for your attention!