Annual review ROME 2012

nSHIELD

WP3 – SPD Node

ARTEMIS

Summary

- WP3 Introduction
- Structure, role and relationships
- Advancement and management status
- Technologies and scenarios
- Tasks and activities
- Conclusions

Workpackage 3: SPD Node

- WP3 aims at providing SPD intrinsic capabilities at node layer.
- The WP is driven by scenarios and is responsible for the:
  - SPD technology assessment,
  - research, development and
  - prototyping

required by nShield scenarios at node level.

- In this context, the WP provides vertical and horizontal tecnologies.

WP3: structure and deliverables

- WP3 structure:
  - T3.1: SDR/Cognitive Enabled node

  (**THYIA**, SG, SICS, TUC, UNIUD, SE, AT, T2D)
  - T3.2 Micro node

  (**ETH**, SG, AT, SICS, T2D, TELC, THYIA, TUC, SE)
  - Task 3.3 Power node

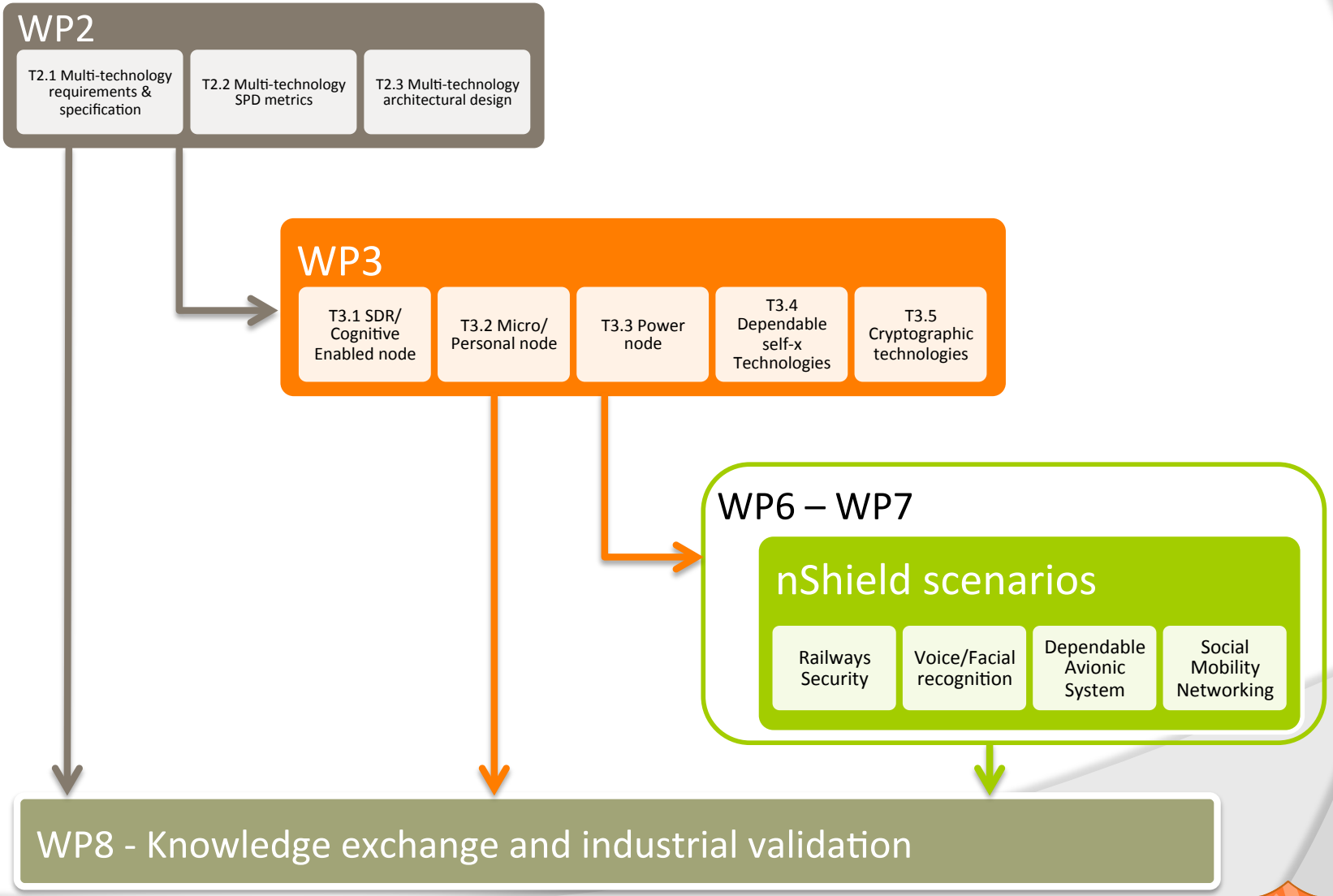
  (**ISD**, SG, AT, SESM, SICS, T2D, TUC, SE)
  - Task 3.4 Dependable self-x Technologies

  (**UNIGE**, ATHENA, TECNALIA, HAI, S-LAB, THYIA, TUC, SE)
  - Task 3.5 Cryptographic technologies

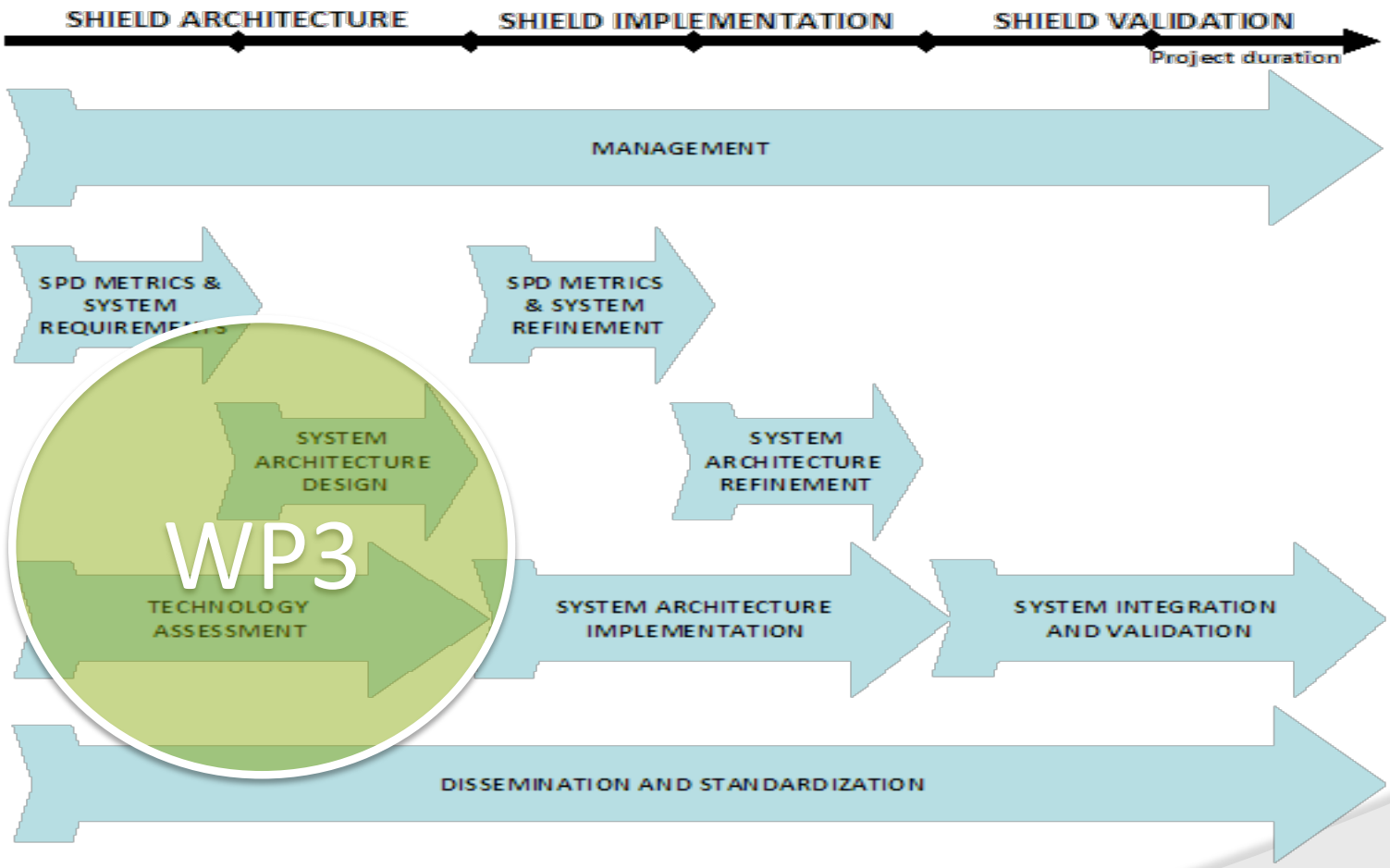
  (**UNIGE**, AT, ATHENA, TECNALIA, S-LAB, SICS, TELC,THYIA, TUC)
- Five deliverables on two main topics, technology assessment and technology prototypes, and two milestones (at M18 and M30).
- Deliverable D3.1, "SPD node technologies assessment", submitted at M6, according to the new plan.

nSHIELD

WP3: role and relationships



Wp3: advancement status



nSHIELD

WP3: management details

- WP3 Management by ETH for year 1, by ISD for the rest of the project.
- Duration: M3-M30.
- Effort: 328 MM.
- Status: ongoing
  - 1 of 5 deliverables submitted
  - ___ of 328 MM, ___% of total planned activities.

T3.1: SDR/Cognitive Enabled Node

- Main topics and activities:
  - Intrinsically secure ES firmware,
  - Power management & supply protection.
- Main achievements:
  - SDR/Cognitive node platform selected: Beaglebord and Beaglebone hardware.
  - Preliminary hypervisor software design.
  - Initial assessment of some suitable software interface and functionalities to the power management features exposed by the platform.

nSHIELD

T3.2: Micro Node

- Main topics and activities:
  - Trusted ESs based on Trusted Platform Module or SmartCard,
  - Easy and dependable interfaces with sensors using protocols that manages node active mode, optimizing power consumption
  - Advanced biometric algorithms that are capable to identify the most significant features of the face and of the voice of a person suitable for ES.
- Main achievements:
  - First outline of the architecture of the face recognition and voice verification system. Design of the architecture of the face recognition and voice verification software.
  - Scheduling support for the first version of the SICS hypervisor and integration with T2Data secure boot.
  - Investigated a framework for delegation of access rights (authorization) on node level.

T3.3: Power Node

- Main topics:
  - Audio based surveillance system,
  - Avionic systems,
  - Integration of heterogeneous embedded systems,
  - Solutions for support of PN and TPM.
- Main achievements:
  - Performed the initial specification of a novel audio based threat detection system for surveillance and anti-tampering, supporting full hardware synchronization at sample level and up to 768 sensors.
  - New IP architecture designed to ease the integration of heterogeneous and independent power nodes and nodes.
  - Feasibility study on how to integrate TPM into firmware.

T3.4: Dependable Self-x Technologies

- Main topics:
  - Mechanisms in charge of preventing non authorized/malicious people to access the physical resources of the node: automatic access control, denial-of-services, self-configuration and self-recovery.
  - Self-reconfigurability and self-adaptation to guarantee robustness and dependability
- Main achievements:
  - Started the design of a novel lightweight traceback mechanism to counter measure DDoS attacks.
  - Selection of a reconfigurable and scalable HW/SW platform potentially useful for the three node typology described in the nShield project.
  - Analysis of inserting digital certificates for M2M in order to preserve privacy putting PKI infrastructure serving M2M (node to node).

T3.5: Cryptographic Technologies

- Main topics:
  - Hardware and software crypto technologies,
  - Asymmetric and ECC Cryptography,
  - Data compression techniques combines with self-reconfiguration and self-recovery.
- Main achievements:
  - Started the implementation of an ECC software library on an microprocessor.
  - Novel cryptographic key exchange algorithm (Controlled Randomness).

The END

That’s all folks!

ARTEMIS