Annual review FLORENCE 2013

nSHIELD

WP3 – SPD Node

Summary

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

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

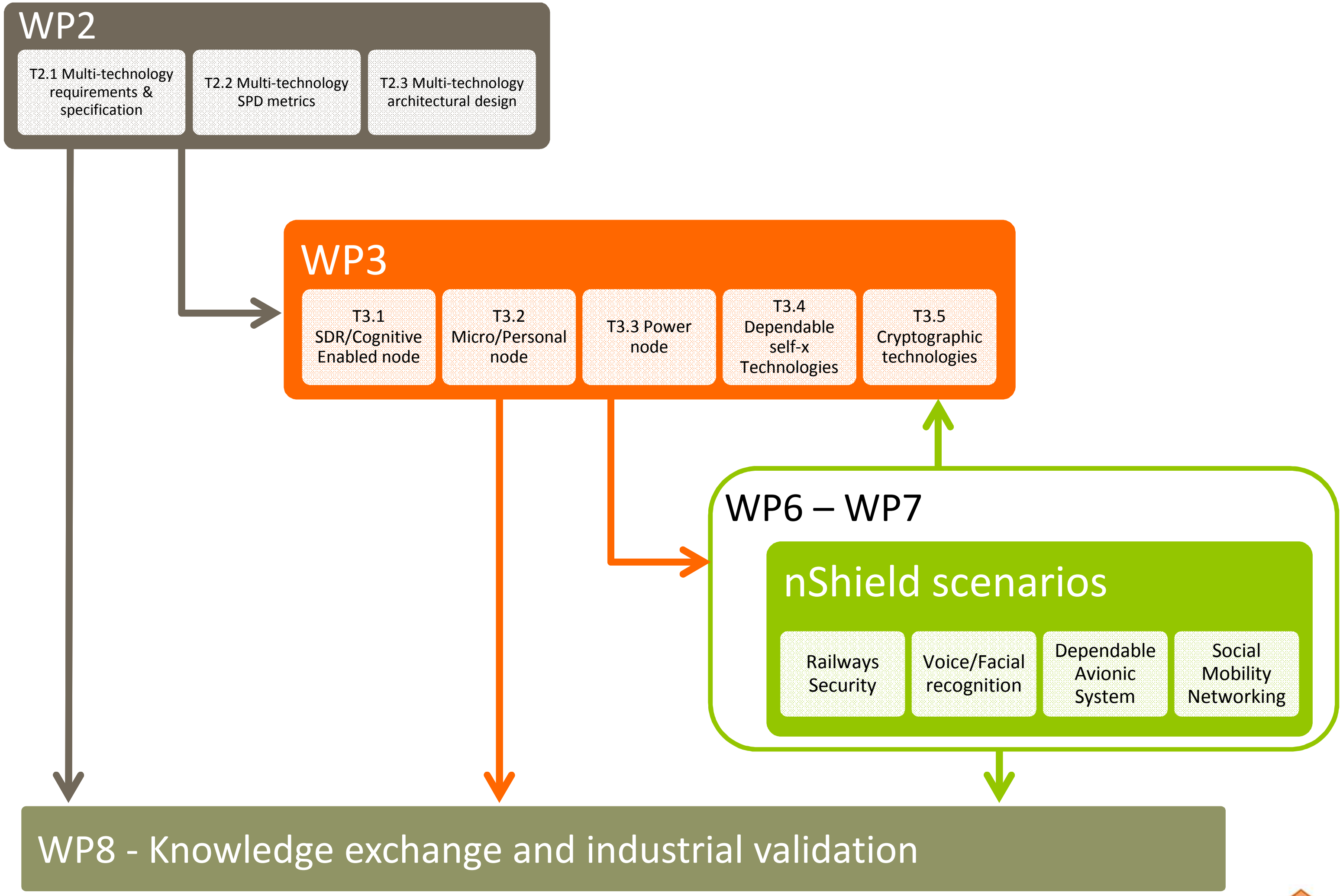
required by nShield scenarios at node level.

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

WP3: Structure and deliverables

- WP3 structure:
  - T3.1: SDR/Cognitive Enabled node
  (**THYIA**, SES, SICS, TUC, UNIUD, AT, T2D)
  - T3.2 Micro node
  (**ETH**, SES, AT, SICS, T2D, TELC, THYIA, TUC)
  - Task 3.3 Power node
  (**ISD**, SESM, SICS, T2D, SES)
  - Task 3.4 Dependable self-x Technologies
  (**UNIGE**, ATHENA, TECNALIA, HAI, S-LAB, THYIA, TUC, SES)
  - 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).

WP3: Role and relationships



WP2

T2.1 Multi-technology requirements & specification

T2.2 Multi-technology SPD metrics

T2.3 Multi-technology architectural design

WP3

T3.1 SDR/Cognitive Enabled node

T3.2 Micro/Personal node

T3.3 Power node

T3.4 Dependable self-x Technologies

T3.5 Cryptographic technologies

WP6 – WP7

nShield scenarios

Railways Security

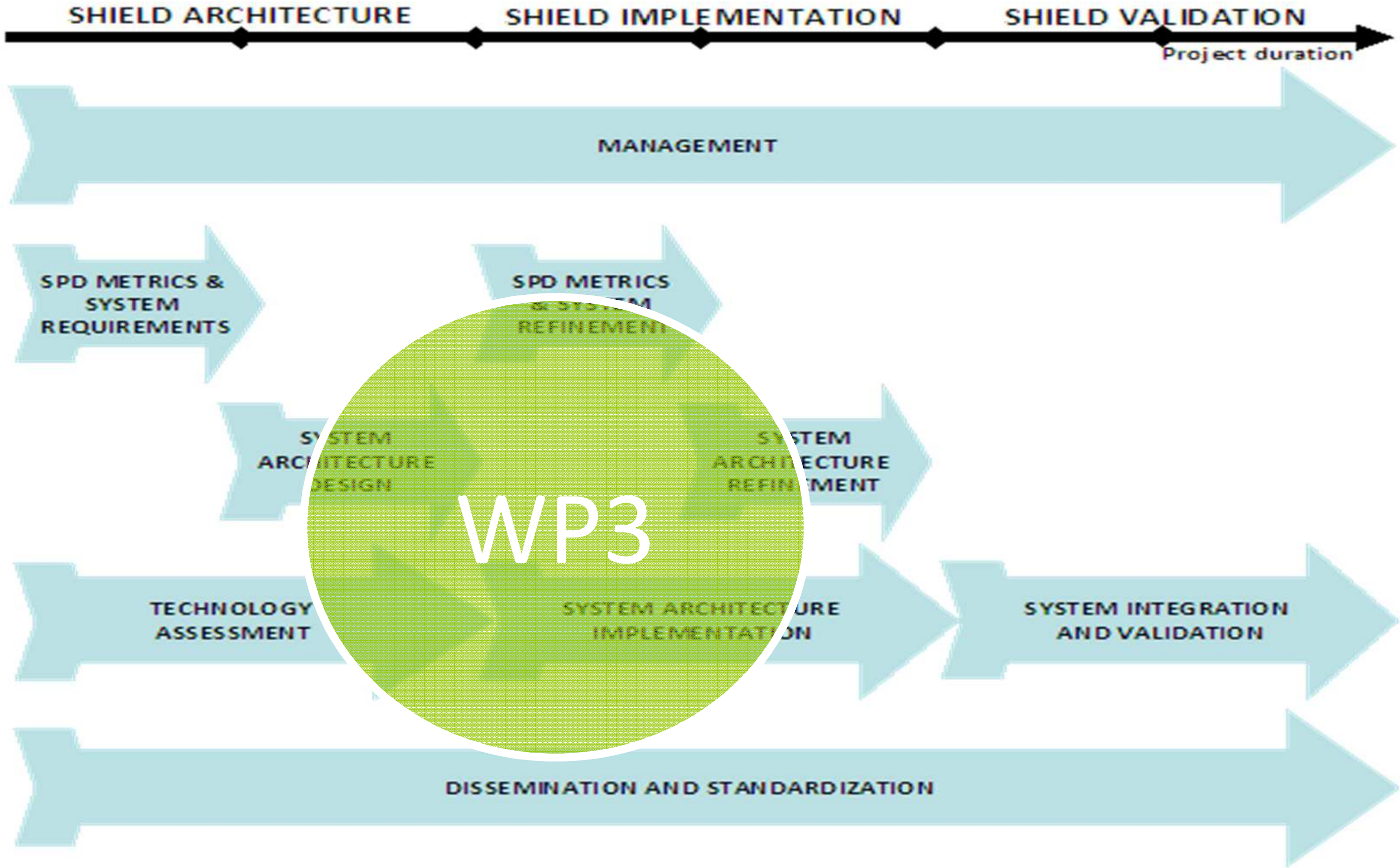
Voice/Facial recognition

Dependable Avionic System

Social Mobility Networking

WP8 - Knowledge exchange and industrial validation

WP3: Advancement status


SHIELD ARCHITECTURE
SHIELD IMPLEMENTATION
SHIELD VALIDATION
Project duration
MANAGEMENT
SPD METRICS & SYSTEM REQUIREMENTS
SPD METRICS & SYSTEM REFINEMENT
SYSTEM ARCHITECTURE DESIGN
SYSTEM ARCHITECTURE REFINEMENT
WP3
TECHNOLOGY ASSESSMENT
SYSTEM ARCHITECTURE IMPLEMENTATION
SYSTEM INTEGRATION AND VALIDATION
DISSEMINATION AND STANDARDIZATION

nSHIELD

WP3: Management details

- Duration: M3-M30.
- Effort: 335 MM.
- Status: ongoing.
  - 1 of 5 deliverables (technology assessment) submitted during Y1 and approved.
  - 2 of 5 deliverables (preliminary prototypes and report) submitted during Y2 on time.
  - 2 of 5 deliverables (final prototypes and report) scheduled for Y3.

T3.1: SDR/Cognitive Enabled Node

- Task topics:
  - Intrinsically secure ES firmware.
  - Power management & supply protection.
- Main activities during the reporting period:
  - AT: Defined power supply protection unit architecture.
  - SICS: Almost finalized a complete Linux port of the hypervisor for security on Beaglebone.
  - T2D: A secure boot design developed together with SICS successfully utilized to securely boot the SICS hypervisor and FreeRTOS on Beaglbone.
  - TUC: Designed, implemented and tested a smartcard authentication protocol based on symmetric keys.
  - UNIUD:
    - Developed a kernel driver for password management of protected SD memory cards.
    - Initiated the development of user and kernel level power management and of activity profiler.

T3.2: Micro Node

- Task topics:
  - Trusted ESs based on Trusted Platform Module or SmartCard.
  - Easy and dependable interfaces with sensors using protocols that manage 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 activities during the reporting period:
  - ETH:
    - Face recognition system prototype developed.
    - Designed an embedded camera prototype used to provide recognition functionalities in a real world scenario.
  - TELC: Designed a framework for delegation of access rights (authorization) on node level.

T3.3: Power Node

- Task topics:
  - Dependable avionic system.
  - Audio based surveillance infrastructure.
  - Integration of heterogeneous embedded systems.
  - TPM support.
- Main activities during the reporting period:
  - SES: Innovative dependable avionic system under development.
  - ISD: Audio based surveillance infrastructure under development .
  - SESM: nSHIELD Gateway development in progress .

T3.4: Dependable Self-x Technologies

- Task 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 activities during the reporting period:
  - UNIGE: Platform selected. Elliptic Curve Cryptography implemented as a demo running in the node prototype. Performance compared to that of a standard PC.
  - ATHENA: Designed a packet marking scheme in conjunction with an intelligent filtering and traceback mechanism that can effectively stop ongoing DDoS attacks.
  - TUC:
    - Developed anonymity service based on the k-anonymity concept.
    - Implemented the Gossamer protocol for automatic access control.

T3.5: Cryptographic Technologies

- Task topics:
  - Hardware and software crypto technologies.
  - Asymmetric and Elliptic Curve Cryptography.
  - Data compression techniques combined with self-reconfiguration and self-recovery.
- Main activities during the reporting period:
  - UNIGE: Developed Elliptic Curve Point Multiplication over prime fields.
  - AT: Defined custom anti-tamper module.
  - ATHENA: Implemented a novel cryptographic key exchange algorithm (Controlled Randomness).
  - TUC:
    - Implemented a compact crypto library in C, containing a set of lightweight ciphers and compact implementations of standard ciphers.
    - Developed a lightweight, efficient, GPU accelerated hashing and hash lookup mechanism utilizing the CUDA GPGPU toolkit. Significant speed-ups have been achieved.
    - Partially implemented a mechanism for establishing cryptographic keys using Identity Based Cryptography.

Conclusions and Future Work

- Y1 and first half of Y2: Main focus on technology development with SPD features driven by preliminary architecture design.
- Second half of Y2 and Y3: Main focus on composability and refinement of SPD metrics based on feedback received from architecture finalization and scenario needs.

The END

nSHIELD

Thank you

ARTEMIS