Annual review ROME 2012

WP5 – SPD Middleware & Overlay

Leader: Andrea Morgagni – Selex Elsag
Presenter: Andrea Fiaschetti – Univ. "La Sapienza"

ARTEMIS

Summary

- WP5 Introduction
- Structure, role and relationships
- Progress and management status
- Technologies and scenarios
- Tasks and activities
- Conclusions

Introduction: WP5 - SPD Middleware & Overlay

- WP5 aims at
  - ✓ Providing innovative SPD functionalities to the SHIELD Middleware
  - ✓ Defining the SHIELD semantic models
  - ✓ Designing and developing the nSHIELD overlay
  - ✓ Defining the SHIELD Policy Management

- The WP is driven by scenarios and is responsible for the:
  - ✓ SPD technology assessment,
  - ✓ research, development and
  - ✓ prototyping

  required by nSHIELD scenarios at middleware level.

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

WP5: structure

- WP5 structure:
  - Task 5.1 SPD driven Semantics [49 MM]

  (**SE**, SG, TECNALIA, HAI, MGEP, THYIA, UNIROMA1)
  - Task 5.2 Core SPD Services & Adaptation of legacy systems [66 MM]

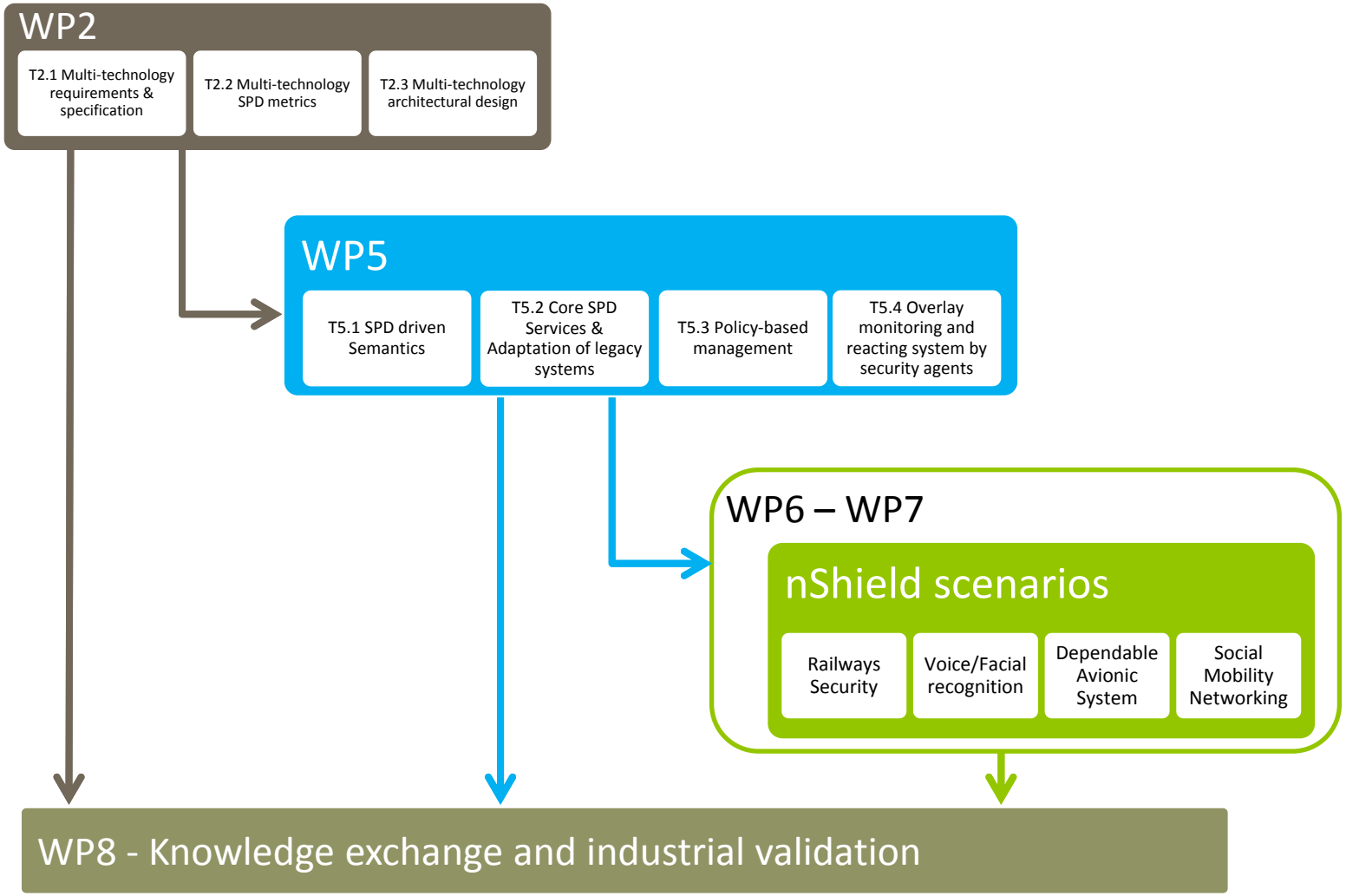
  (**S-LAB**, SG, ATHENA, SE, TECNALIA, THYIA, TUC, UNIROMA1)
  - Task 5.3 Policy-based management [69 MM]

  (**HAI**, SE, TECNALIA, ISL, THYIA, TUC)
  - Task 5.4 Overlay monitoring and reacting system by security agents [48 MM]

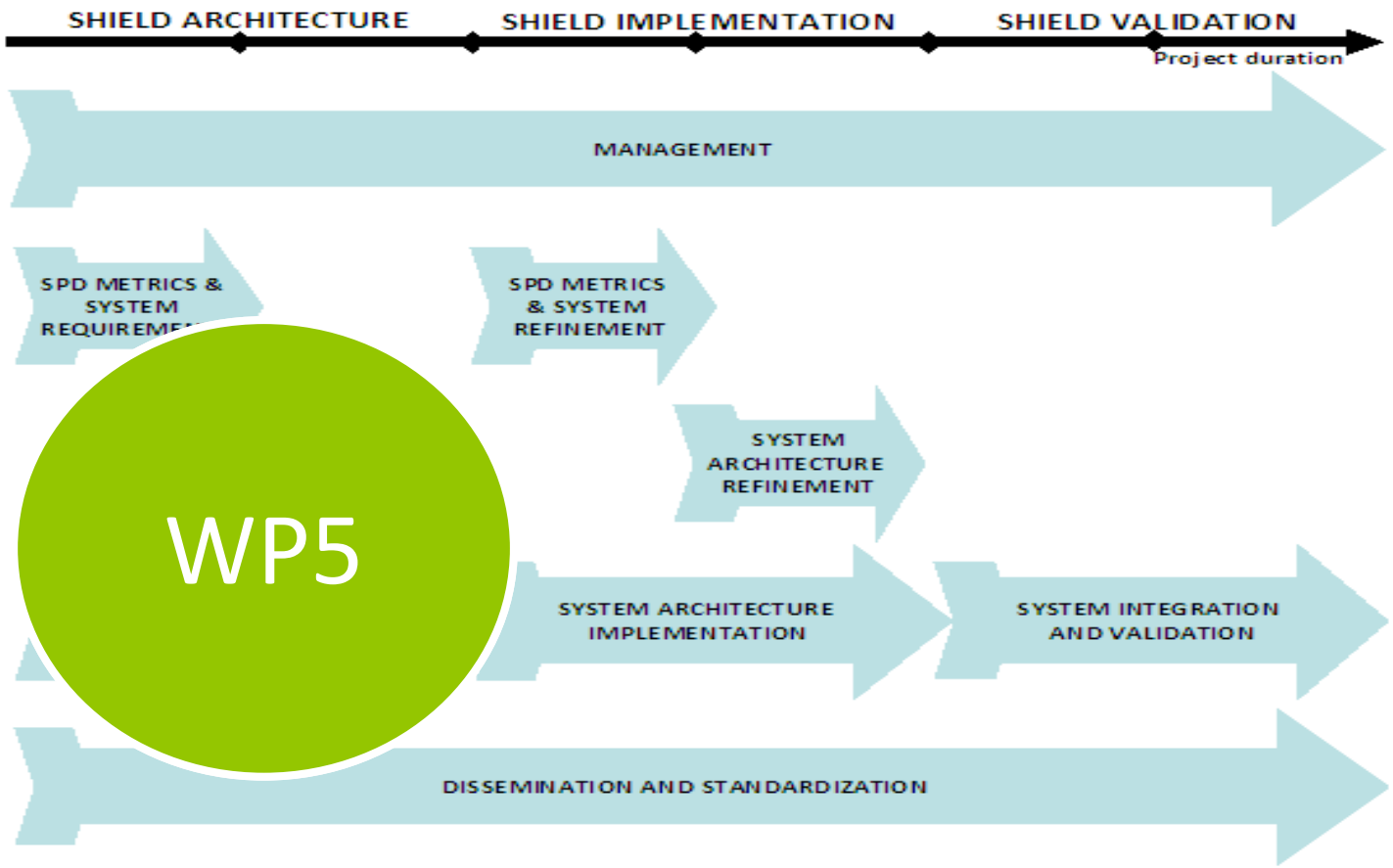
  (**UNIROMA1**, ATHENA, SE, HAI, THYIA)

- **Five deliverables** on three main topics: technology assessment, technology design, prototypes development, and **two milestones** (at M18 and M30).
- Deliverable D5.1, "SPD middleware and overlay technologies assessment", submitted at M10.

WP5: role and relationships



WP5: Progress



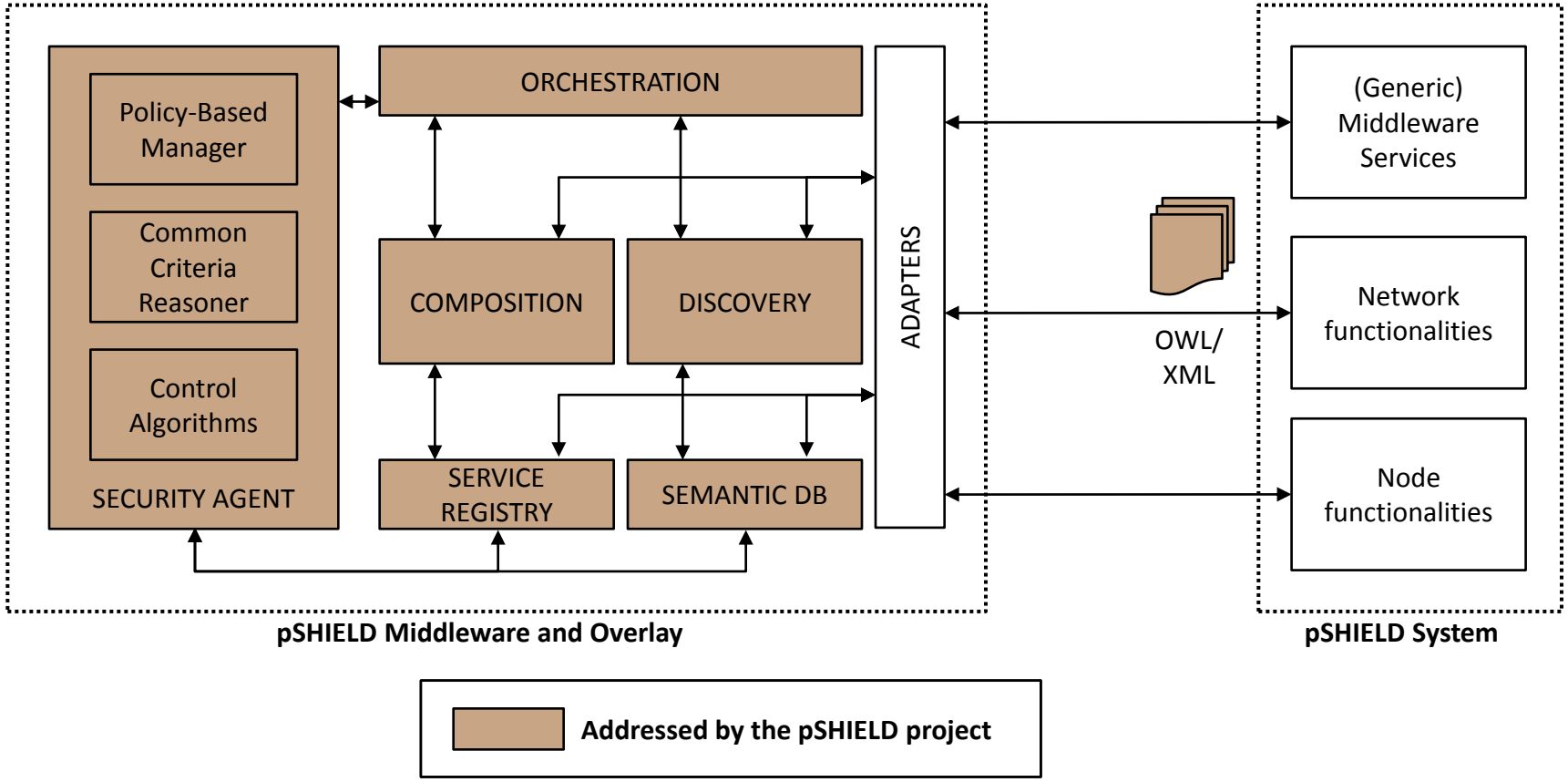
- 7 Months of work performed so far
- Nearest milestone in 6 months (first prototypes and reports)

WP5: Management status

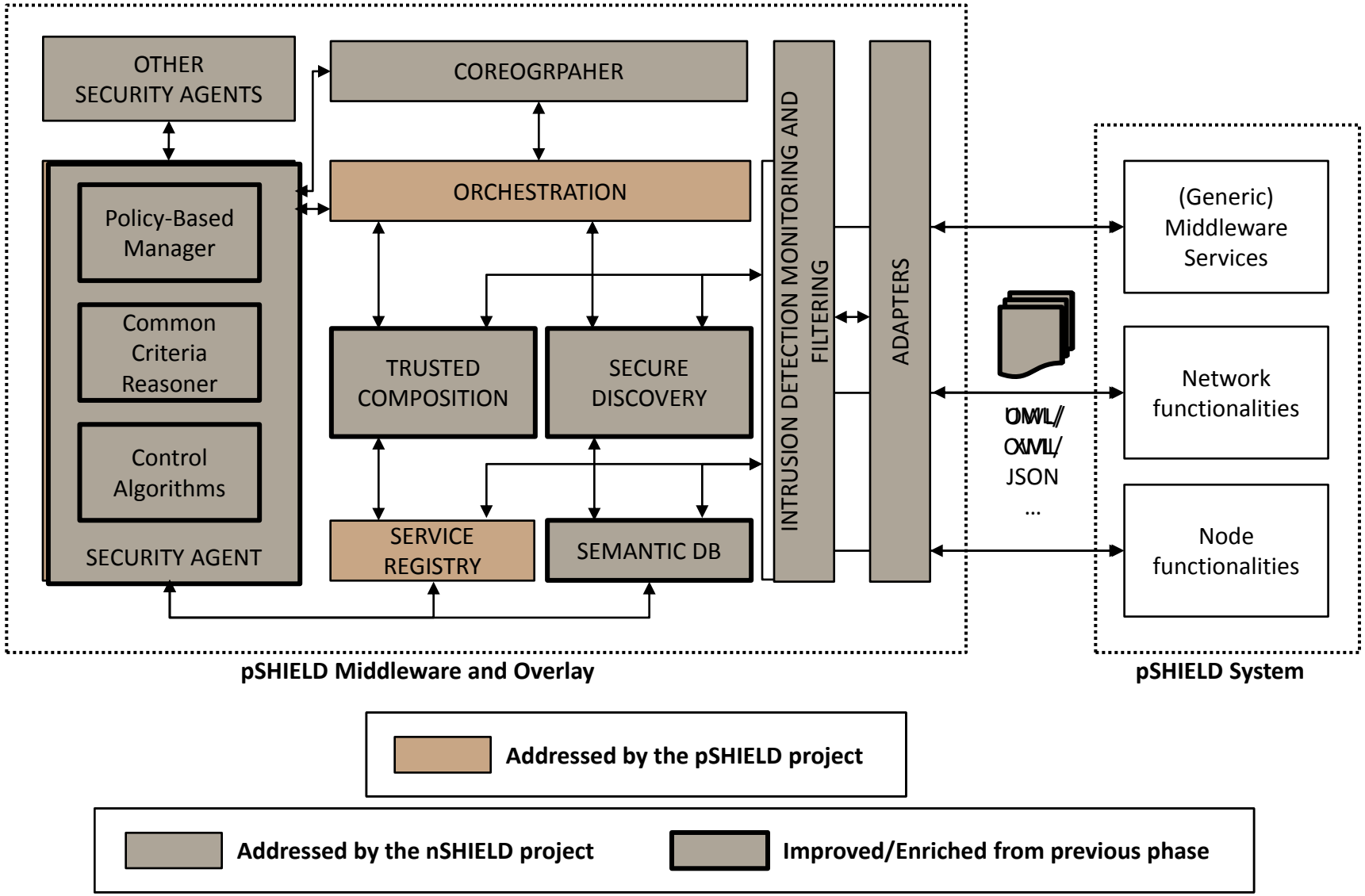
- WP5 Managed by SelexElsag.
- Duration: M5-M30.
- Effort: 232 MM.
- Status: ongoing
  - 1 of 5 deliverables submitted
  - 58 of 232 MM, 25% of total planned activities
- Tasks Status:
  - T5.1 – 25%
  - T5.2 – 30%
  - T5.3 – 10%
  - T5.4 – 30%

- Internal effort reallocation and identification of roles and responsibilities
- We achieved a successful integration of new partners and knowledge
- Set-up of collaborative tools (SVN repository for code sharing) and mailing list
- Input to WP2 activities

WP5: Technologies and scenarios 1/2



WP5: Technologies and scenarios 1/2

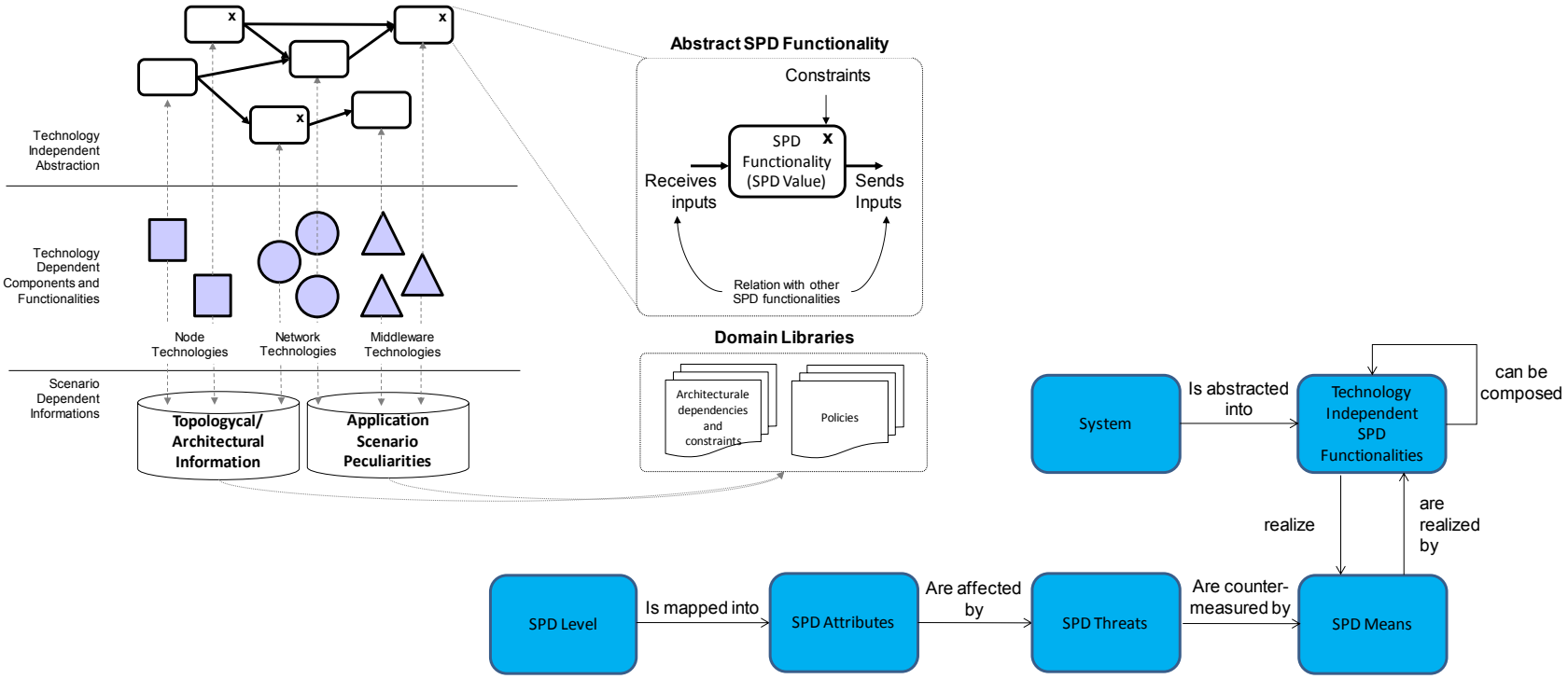


WP5: Technologies and scenarios 2/2

- **Enrichment of the semantic approach** by means of **new languages** and **new procedures** to represent and manage the information necessary to enable the composability
- Improvement of the SHIELD middleware core services, with the enabling of a **"secure" discovery** and a **"trusted" composition**.
- Identification of new middleware core services, like the **"choreographer"** and the **"intrusion detection monitor and filter"**.
- Definition of the **adapters**, by which the SHIELD system is able to interface the external world (and in particular legacy devices)
- The **enrichment of the Security Agent** architecture, with the harmonization of all the approaches (standardized, policy-based or context aware) that drive the composability
- The definition of the **interactions** between several **Security Agents** working together to manage SPD in distributed environments
- The development of **innovative control algorithms**, based on DES and Petri Nets, to model and control the system behaviour
- The **instantiation** of the **Policy Based management** architecture, as well as the **definition** of several **libraries of policies** to manage SPD in different application scenarios.
- The **certification of the protection profile** for the SHIELD middleware (Common Criteria compliant).

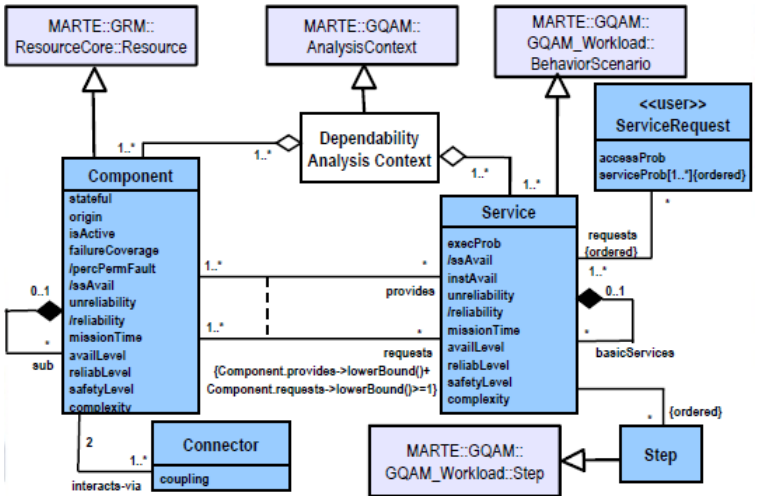
Task 5.1 Main activities and achievements (1/2)

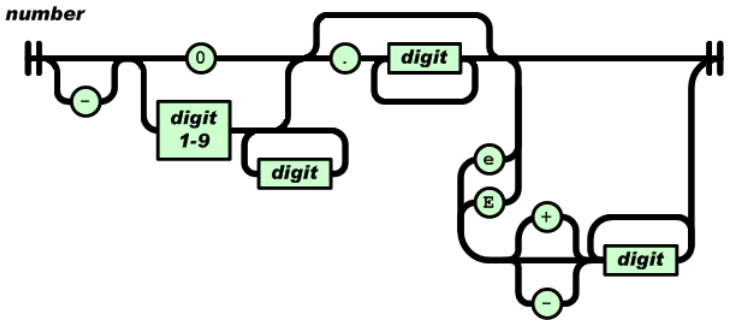
- **Enrichment of the semantic approach** by means of **new procedures** (expressiveness and scalability problems)
  - ✓ Preliminary definition of a methodology based on SPD abstraction
  - ✓ Definition of a methodology based on Common Criteria
  - ✓ Identification of Ontology as mean to perform Intrusion Detection



Task 5.1 Main activities and achievements (2/2)

- **Enrichment of the semantic approach** by means of **new languages** (computational constraints)
  - ✓ Identification of MARTE DAM UML Profile to describe functionalities
  - ✓ Identification of JSON (lightweight data-interchange format.)

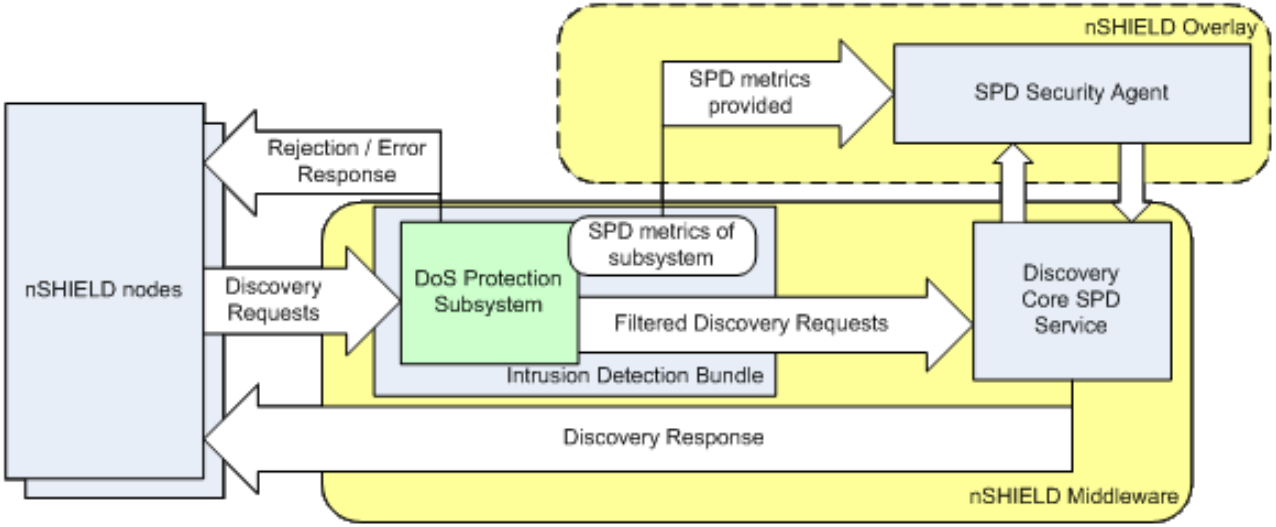




Task 5.2 Main activities and achievements 1/3

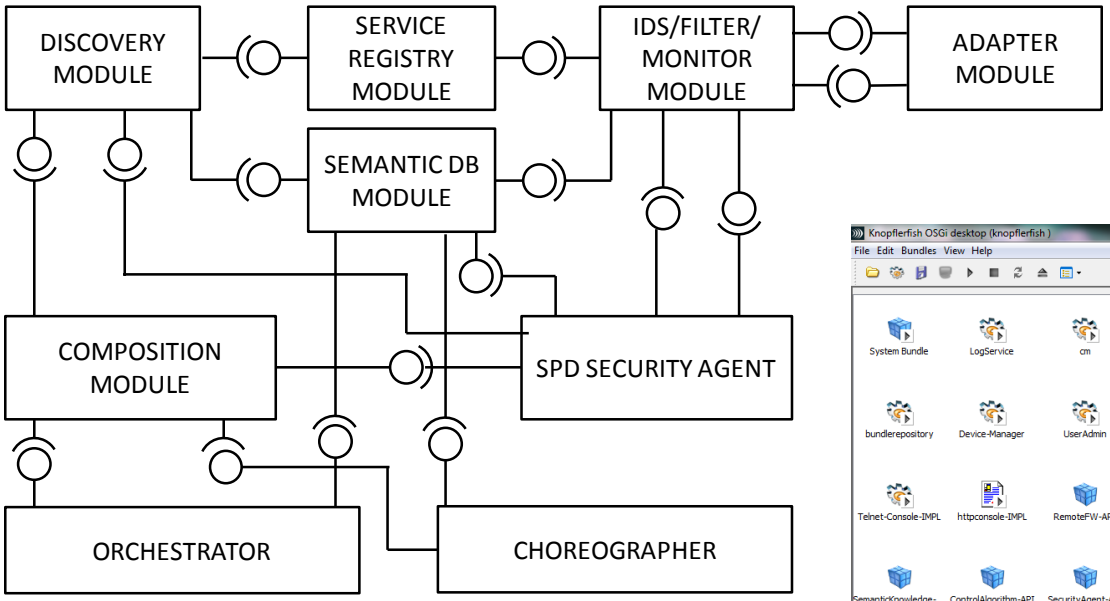
- Improvement of the SHIELD middleware core services, with the enabling of a **“secure” discovery** and a **“trusted” composition**.
- Identification of new middleware core services, like the **“choreographer”** and the **“intrusion detection monitor and filter”**.
- Definition of the **adapters**, by which the SHIELD system is able to interface the external world (and in particular legacy devices)

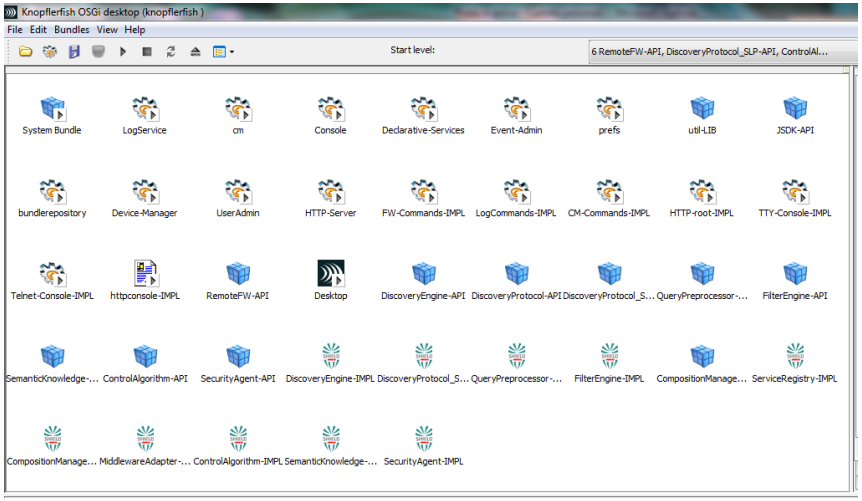
  - ✓ Analysis of the state of the art in Secure Discovery
  - ✓ Analysis of the state of the art in Trusted composition
  - ✓ Preliminary definition of the intrusion detection and monitoring module



Task 5.2 Main activities and achievements 2/3

- ✓ Preliminary definition of the choreographer module
- ✓ Preliminary design of the Core Services Architecture
- ✓ Preliminary definition of the SHIELD adapter
- ✓ Adoption of the OSGI execution environment as starting point for Middleware implementation





Task 5.2 Main activities and achievements 3/3

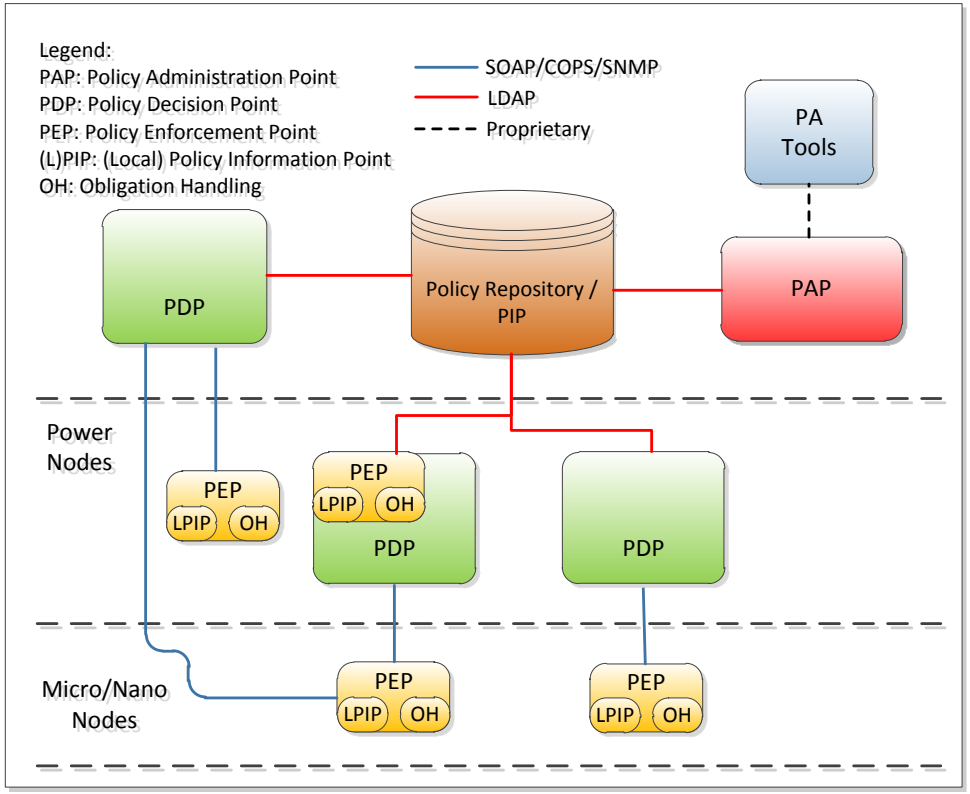
- The **certification of the protection profile** for the SHIELD middleware (Common Criteria compliant).

✓ A Protection Profile (PP) is a document used as part of the certification process according to the Common Criteria (CC). As the generic form of a Security Target (ST), it is typically created by a user or user community and provides an **implementation independent specification** of information assurance security requirements. A PP is a combination of **threats**, **security objectives**, **assumptions**, **security functional requirements** (SFRs), security assurance requirements (SARs) and **rationales**.
A PP specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products.

✓ For the nSHIELD project, the possibility of editing a protection profile for the SHIELD middleware is currently under investigation

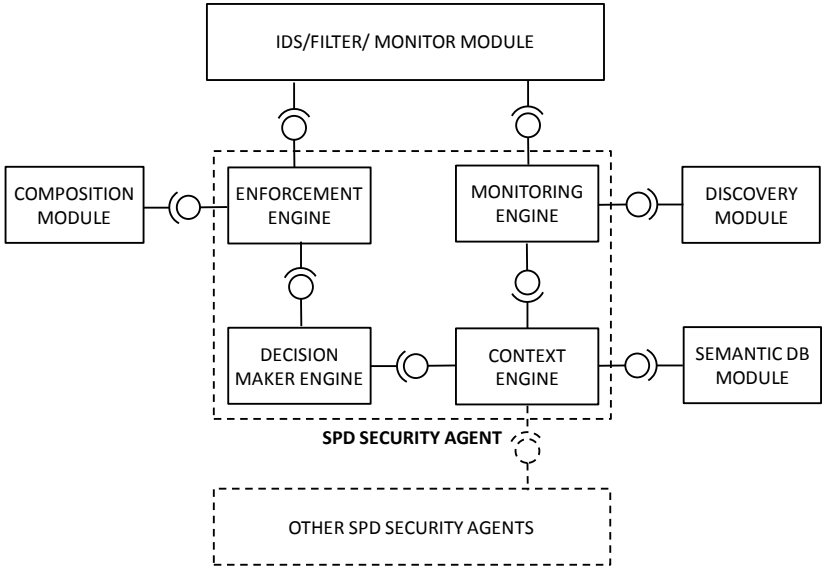
Task 5.3 Main activities and achievements

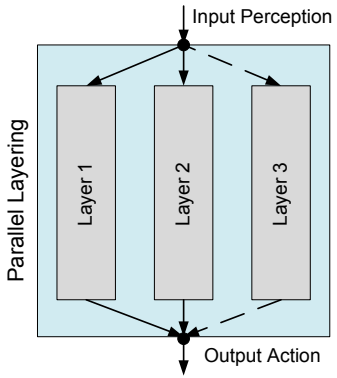
- The **instantiation** of the **Policy Based management** architecture, as well as the **definition** of several **libraries of policies** to manage SPD in different application scenarios.
  - ✓ Definition of the SHIELD PBM architecture
  - ✓ Policies still to be defined (waiting for the consolidation of metrics)

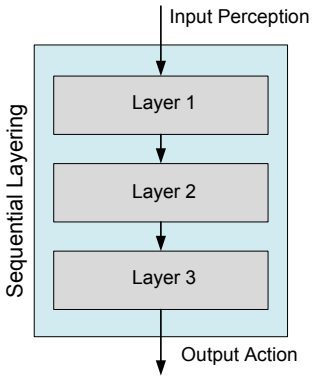


Task 5.4 Main activities and achievements 1/3

- The **enrichment of the Security Agent** architecture, with the harmonization of all the approaches (standardized, policy-based or context aware) that drive the composability
- The definition of the **interactions** between several **Security Agents** working together to manage SPD in distributed environments
  - ✓ Architectural design of the Security Agent (in an OSGI-integration perspective)
  - ✓ Identification of interfaces for communication between security agents
  - ✓ Analysis and preliminary identification of Hybrid Agent as paradigm for Security Agent clustering



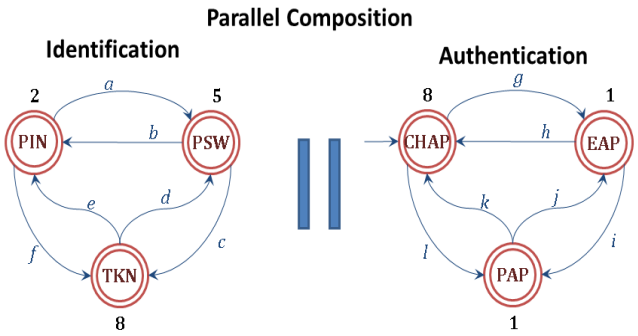


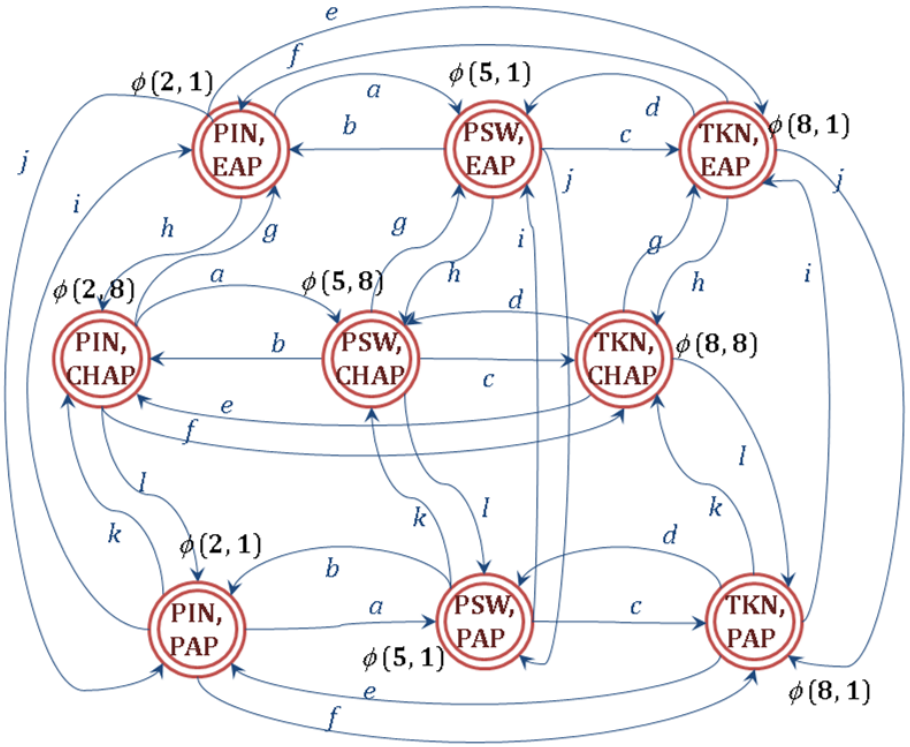


Task 5.4 Main activities and achievements 2/3

- The development of **innovative control algorithms**, based on DES and Petri Nets, to model and control the system behaviour

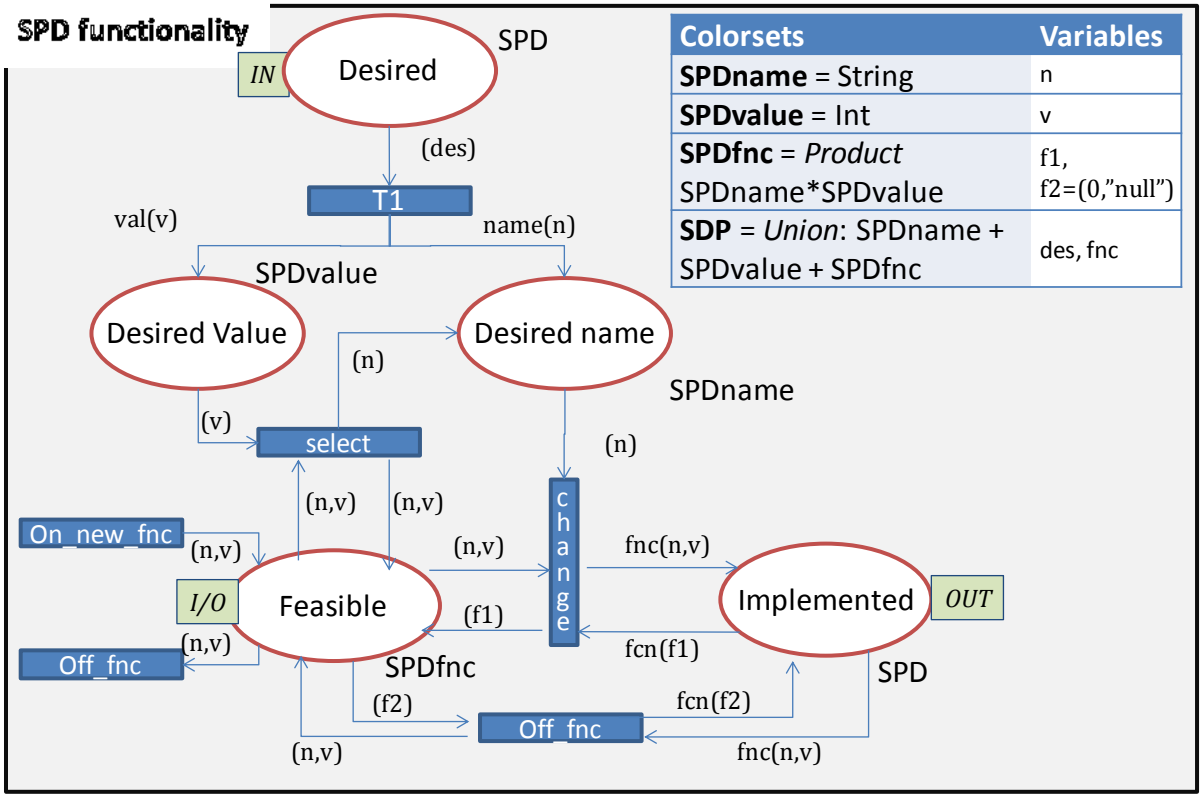
  ✓ Definition of a composability control algorithm based on DES (scalability problems)





Task 5.4 Main activities and achievements 3/3

- ✓ Adoption of a composability control algorithm based on Colored Petri Nets
- ✓ Integration between security agent modelling and SHIELD semantic



Conclusions

- The pSHIELD outcomes provided a solid base on which build the SHIELD final guidelins
- The major enabling technologies under investigation for SHIELD Middleware are:
  - ✓ Semantic modelling
  - ✓ Policies
  - ✓ Control Algorithms
- These technologies enable the **SPD driven composability**, but
- Additional technologies contribute to **enrich the security** of the middleware and overlay itself, like:
  - ✓ Secure Discovery
  - ✓ Trusted Composition
  - ✓ Intrusion detection
- The **certification** of the protection profile for SHIELD middleware would be the very first step toward an official standardization of the SHIELD framework
- The guideline for WP5 activities is the «**feasibility**» of the proposed solutions, since we have moved from a proof of concept towards a prototype delivery.

- First results, in terms of design, implementation and simulations analysis, will be available after the next 6 months.

Remark from WP5 leader

Challenging results (already achieved and hopefully to be achieved) were possible thanks to the help of the enriched WP5 team that provided the consortium with many innovative ideas, experience and solutions

Many thanks to ALL WP5 participants for the work carried out so far

Thanks for your attention

Any questions?

Andrea Fiaschetti