

Annual review ROME 2012




Overview

Selex Galileo - Luigi Trono





 **nSHIELD** is a project co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems



The main objective is to conceive and design an innovative, modular, composable, expandable and high-dependable architectural framework which allows to achieve the desired level of **Security, Privacy and Dependability** in the context of integrated and interoperating heterogeneous services, applications, systems and devices.

nSHIELD consortium



Selex Galileo
Ansaldo STS
Acorde Technologies
ISI / ATHENA
Selex Elsag
Fundación Tecnalia Research & Innovation
I.P.S Sistemi Programmabili - Eurotech Security
Hellenic Aerospace Industry
Indra Software Labs
Integrated Systems Development
Movation AS
Mondragon University
Alfatroll
SEARCH-LAB
SESM scarl
Swedish Institute of Computer Science
T2 Data AB
Telcred
THYIA
Technical University of Crete
Università di Genova
Università di Udine
Università di Roma — La Sapienza

The nSHIELD consortium comprises 6 manufacturers and system integrators, 7 universities, 8 SMEs and 2 Industrial R&D organizations. The project is lead by an industrial partnership (70% of the effort) even if an important role is left to the universities and the research centers (30%) in order to bring the needed high innovation



Web: <http://www.newshield.eu/>

Wiki: <http://nshield.unik.no/wiki/NSHIELD>

Project Leader: Luigi Trono – Selex Galileo

Email: luigi.trono@selexgalileo.com



What is nSHIELD?

The nSHIELD project is a complement and significant technology breakthrough of “pSHIELD”

Ended February 2011



ARTEMIS
Call 2009

SPD Framework
Investigation and
Definition phase

One scenario

Started September 2011



ARTEMIS
Call 2010

SPD Framework
Development and
Implementation phases

Four scenarios

nSHIELD addresses **SPD** in the context of Embedded Systems (ESs) as “**built in**” rather than as “add-on” functionalities, proposing and perceiving the first step toward SPD **certification** for future ES.

How?

1

SHIELD leading concept **Composability** of SPD technologies.

Dynamic composition of State of the art SPD technologies and new SPD technologies depending on different scenarios.

nSHIELD will be the reference milestone for a new generation of “**SPD-ready**” ESs

nSHIELD Innovations

Great impact on the system design costs and time to market of new SPD solutions in ESs.

2

SHIELD Integrated use of **SPD metrics**

Great impact on the development cycles of SPD in ES:

Process as qualification, (re-)certification and (re-) validation of the framework will be faster, easier and widely accepted.

Multi-layer approach & Composability

Four Layers

SPD Modules

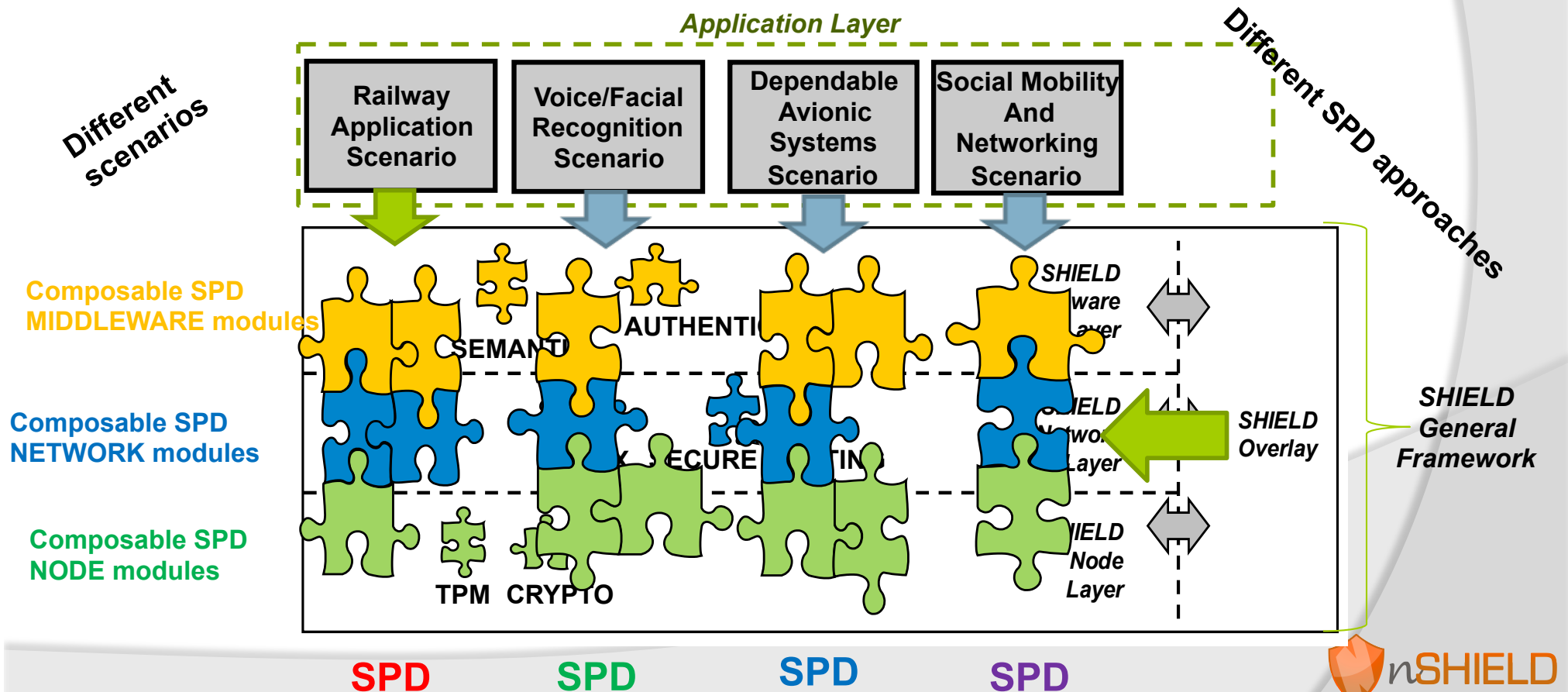
Set of SPD Modules for each layers - Each module implements a SPD technology or a specific SPD functionality.

Four Scenarios

Composability

Modules belonging to different SPD layers (node, network or middleware) can be composed statically or dynamically by the overlay.

Application Layer

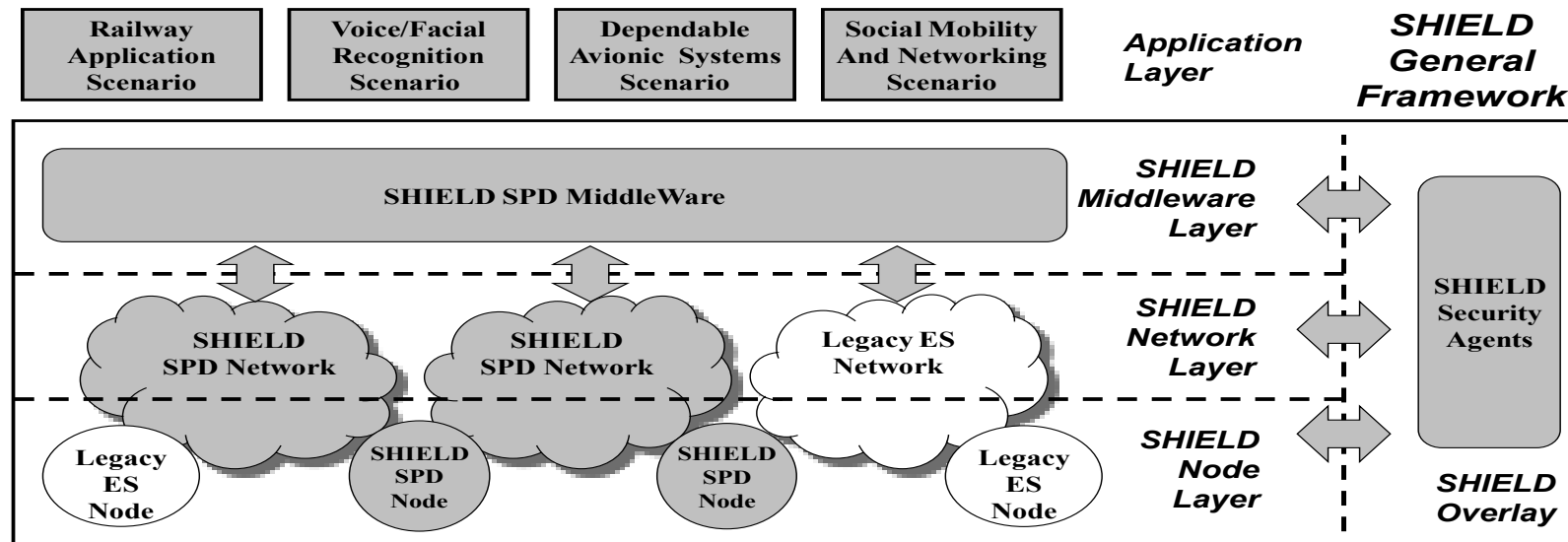


nSHIELD technologies and solutions

For each of the 4 layers, the state of the art in SPD of individual technologies and solutions will be improved and integrated (hardware and communication technologies, cryptography, middleware, smart SPD applications, etc.).

The 4 layers are motivated by the peculiarities of the SPD solutions to be implemented namely at node (hardware and firmware), network (protocol) and middleware (software) level and by the actual industrial contest of embedded system suppliers, which are mainly organized in these three major sectors.

The functionalities will be embedded in nSHIELD SPD modules which will be transparently inserted in each of the layers; transparency means that the insertion of these modules does not entail any modification of the pre-existing algorithms and procedures.

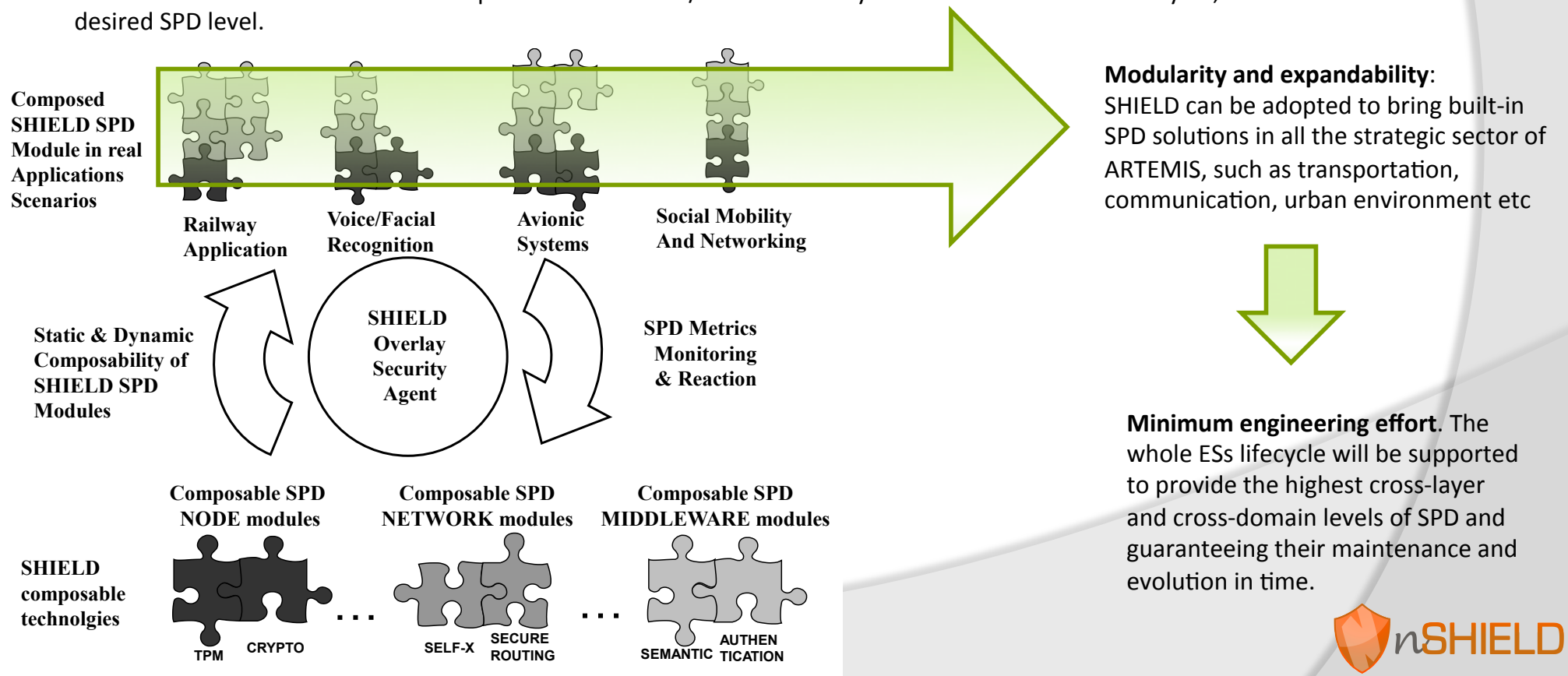


Overlay & Control algorithms

SHIELD will use a defined set of metrics to ensure that the SPD level is appropriate for each application scenario.

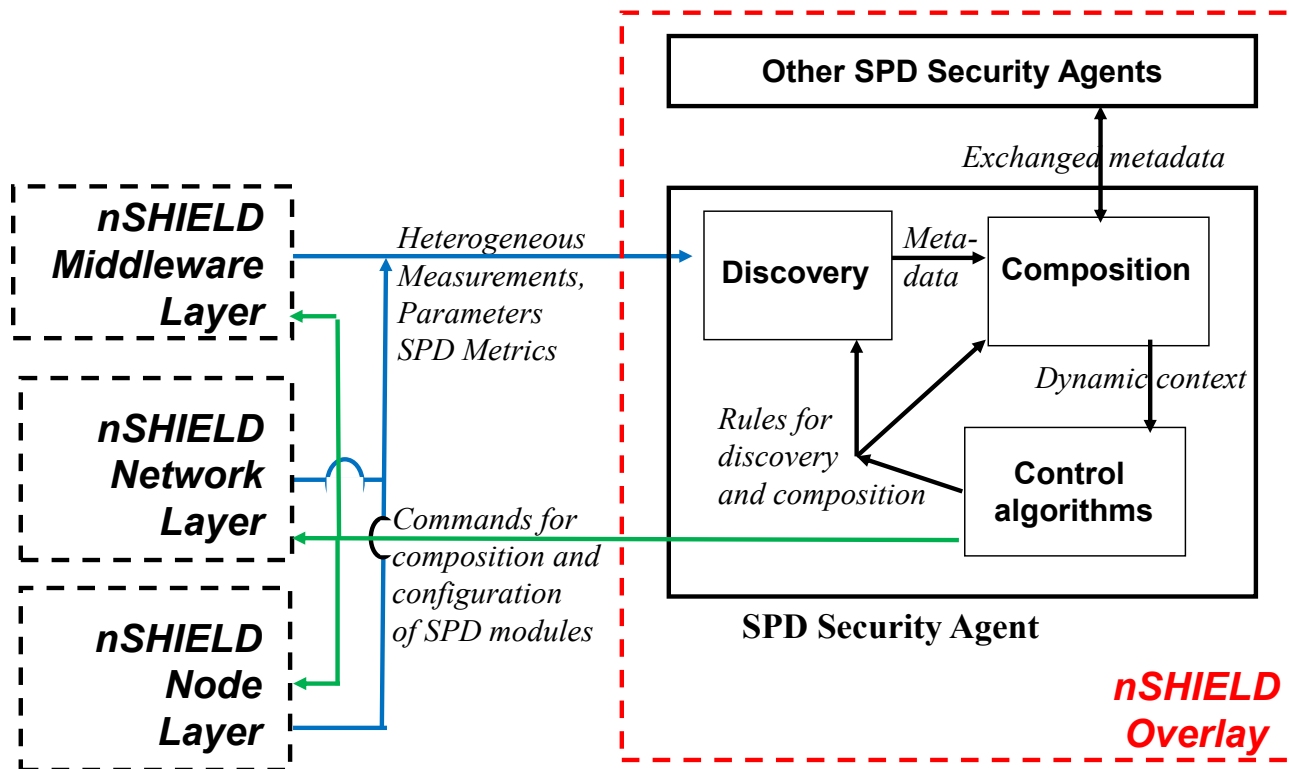
Single nSHIELD SPD modules can be enabled or replaced once the measured SPD **metrics** do not satisfy the required SPD levels. The SPD metrics are continuously monitored by the **security agents** and in case of failure, the security agent reacts discovering, composing and configuring the available SPD modules.

The security agent monitors a set of properly selected measurements and parameters taken at any of the three layers and converted to **homogeneous metadata**. The metadata is the input for a set of control algorithms responsible of dynamically deciding which SPD modules have to be composed and enabled/disabled at any of the three mentioned layers, in order to achieve the desired SPD level.



Overlay & Control algorithms

The nSHIELD project will design and implement overlay security agents which will implement the key *composability* concept:



Using **semantics**, the available technologies can be automatically composed to match the needed, application specific SPD levels, resulting also in an effort reduction during all the design, operational and maintaining phases

SHIELD objectives

- **New technologies:** A wide set of technologies will be used to realize SPD composability and design guidelines will be provided to make any nSHIELD compliant technology composable with the others
- **Metrics:** A complete set of metrics for SPD description will be refined and consolidated. Metrics will be used to validate the whole functionalities of the framework
- **Modular, composable, expandable and high-dependable architectural framework:** Composability of SPD functionality at different layers among different technologies will be refined and developed, taking into account performances and dynamic composability of any kind of technologies. This ensures secure, reliable and timely system services despite accidental failure of system components and/or the activity of malicious intruders.
- **Validation:** the framework will be validated will be validated through proper test beds and demonstrators relevant to the four considered scenarios: **railway, recognition, avionics and social mobility.**



Shield Market Targets



Design Cost Reduction

Cost reduction in system design

a SPD-intrinsic framework can be improved and modified with a lower cost if compared with the cost of designing the whole system and its SPD functionalities from scratch.

Manage the complexity with effort reduction

The static (at design time) and dynamic (at runtime) composability offered by the SHIELD framework addresses the increasing complexity of providing SPD in ESs with less effort during the whole SPD lifecycle

Achieve cross-sectorial reusability of Embedded Systems devices

Composability and modularity allow reusability of the SPD functionalities and technologies over heterogeneous sectors: the architecture will be validated in four different pilot scenarios.

Certification

Cost reduction in development cycles requiring qualification or certification

SPD **metrics** are considered the basement for building standardized methods and industry-wide accepted parameters for certificability.

Effort and time reduction for re-validation and recertification after change

Re-validation and re-certification processes will be reduced by two innovations: the definition of common SPD metrics and the development of tools to support the SPD lifecycle over the whole ES.



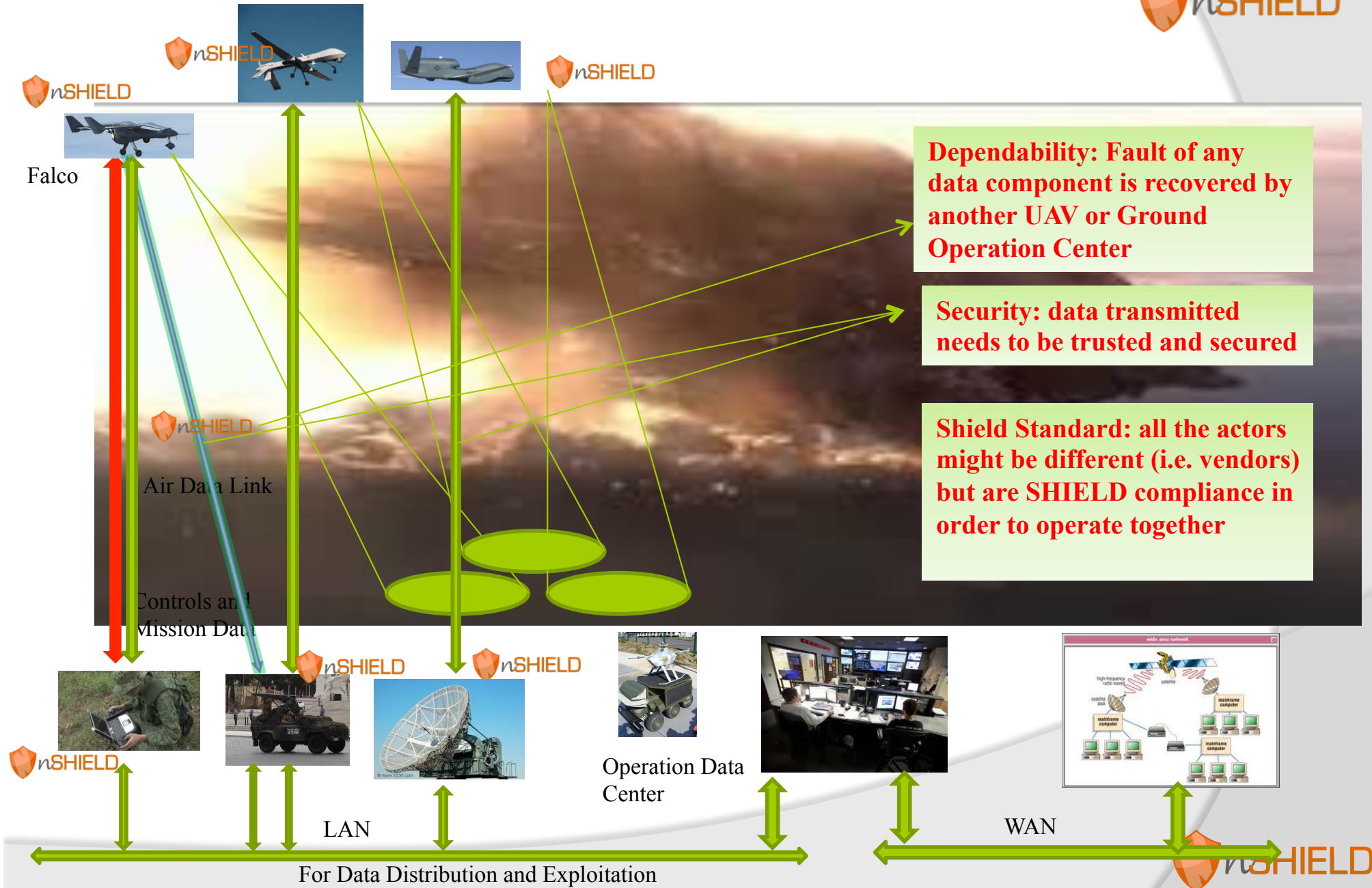
nSHIELD will be the first step towards SPD certification for future ES.

Market Impact

By addressing the reusability of previous designed solutions, the interoperability of advanced SPD technologies and the standardized SDP certificability, it is possible to estimate an overall **30% cost reduction for a full nSHIELD oriented design methodology.**



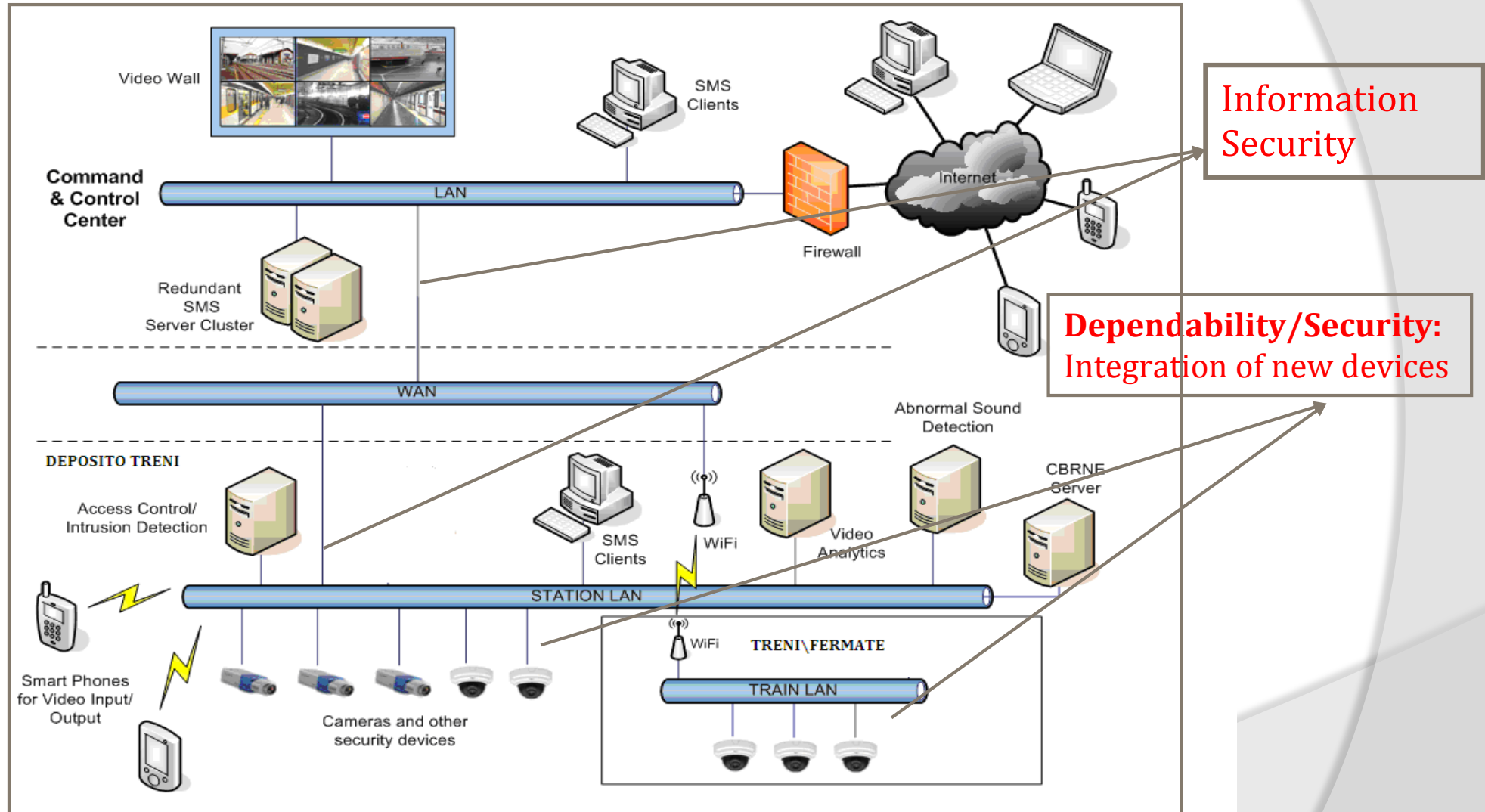
Dependable Avionics Scenario



SHIELD Solutions

Today Gaps	SHIELD Advantages
Partial integration, only with same family systems	SHIELD permits the integration of new systems and subsystems shield compliant
Only HW redundancy and Scalability allowed with added engineering effort	Redundancy guaranteed through the SHIELD compliance and scalability allowed with fast module reconfiguration and low engineering cost.
Sensitive to cyber attacks	Resilience to cyber attacks (UAVs architecture changes continuously) (polymorphism). New Algorithms improve data security.

Railway Security Application Scenario



Dependability: Faults of components and/or whole system

SHIELD Solutions

Today Gaps	SHIELD Advantages
Information Security	Transparent and adaptive user authentication and data encryption for 'open' communication channels (e.g. WLAN, Internet, etc.).
Faults Resilience	Automatic threat detection and system reconfiguration using redundancy, fault-tolerance and fall-back mechanisms.
Assessable integration of new devices	Open middleware, with clear interface specifications, for the easy integration of different protocols in a way which ensures transparency at the user level while keeping system SPD easy-to- assess. In fact, reference semantic models ease modular holistic certification with the re-use of already certified components.

Voice recognition and person identification

Example of a real scenario: access control at a military facility entrance.



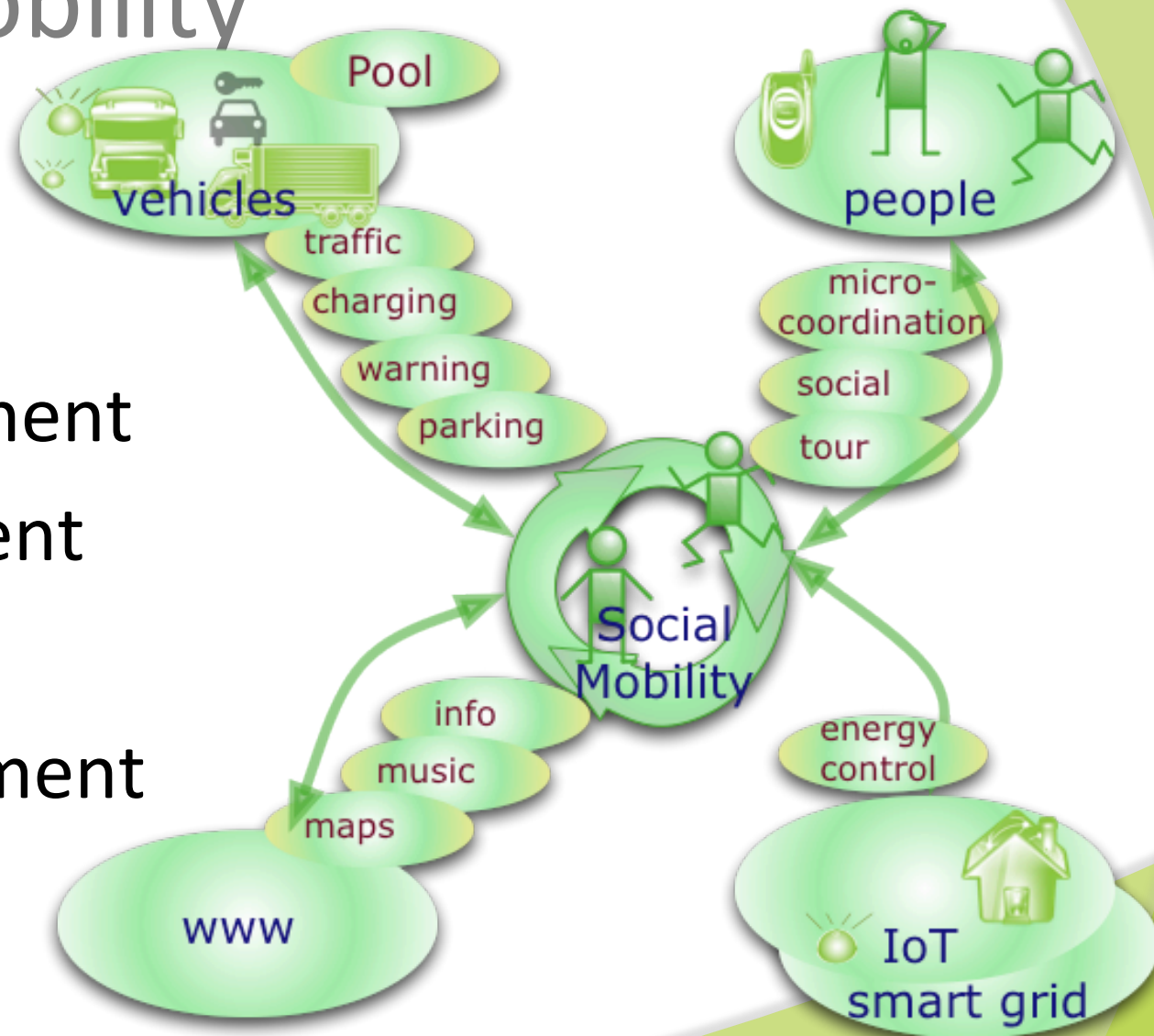
- Leaving the camp:
 - Car plate recognition
 - Driver's voice recognition
 - ZigBee Tag association to car and driver
- Entering the camp:
 - Car plate, driver voice and tag recognition
 - Comparison with stored profile
 - Access management and alarm generation

SHIELD Solutions

Today Gaps	SHIELD Advantages
Complex HW/SW recognition systems	nSHIELD provides an embedded/mobile solution
Difficult to provide recognition in dynamic scenarios	People recognition in static and also in dynamic scenarios.
Trusted data communication and privacy	New Algorithms improve data security and guarantee users privacy

Social Mobility

- From
- Entertainment
- Infotainment
- To
- Socialtainment



SHIELD Solutions

Today Gaps	SHIELD Advantages
Lacks of trusted and secure sensors and systems	Enhanced Security, Privacy and Dependability features for embedded devices
Lack of joined SPD services & applications	A new class of SPD services for merging physical and social networks
Lacks of Interoperability issues related to the new nSHIELD SPD sensors and networks	Integrity and interoperability measures

Vision

Railways security
Voice/Facial Recognition
Dependable Avionic Systems
Social Mobility



The END



Thank You!

