Demonstrating Security, Privacy and Dependability for Sensors to Systems

> “Interoperability in security and safety is a breakthrough in Innovation”
>
> Antonio Vecchio (June 2010. Naples)

Summary

The pSHIELD project aims at addressing Security, Privacy and Dependability (SPD) issues in the context of Embedded Systems (ESs) as “built in” rather than as “add-on” functionalities. Enhanced embedded Services built on the layered pSHIELD platform will profit from a dependable security architecture, where data and access are provided according to the trust level between the requester and the provider of the data. The overall goal for the pSHIELD project is to create services based on input from embedded systems (ESs) at the edge of the network in order to contribute to the development of the Internet of Things.

Project Leader:
Space Drakul (Thyia Technologies)
email: sdrakul@thyia.si

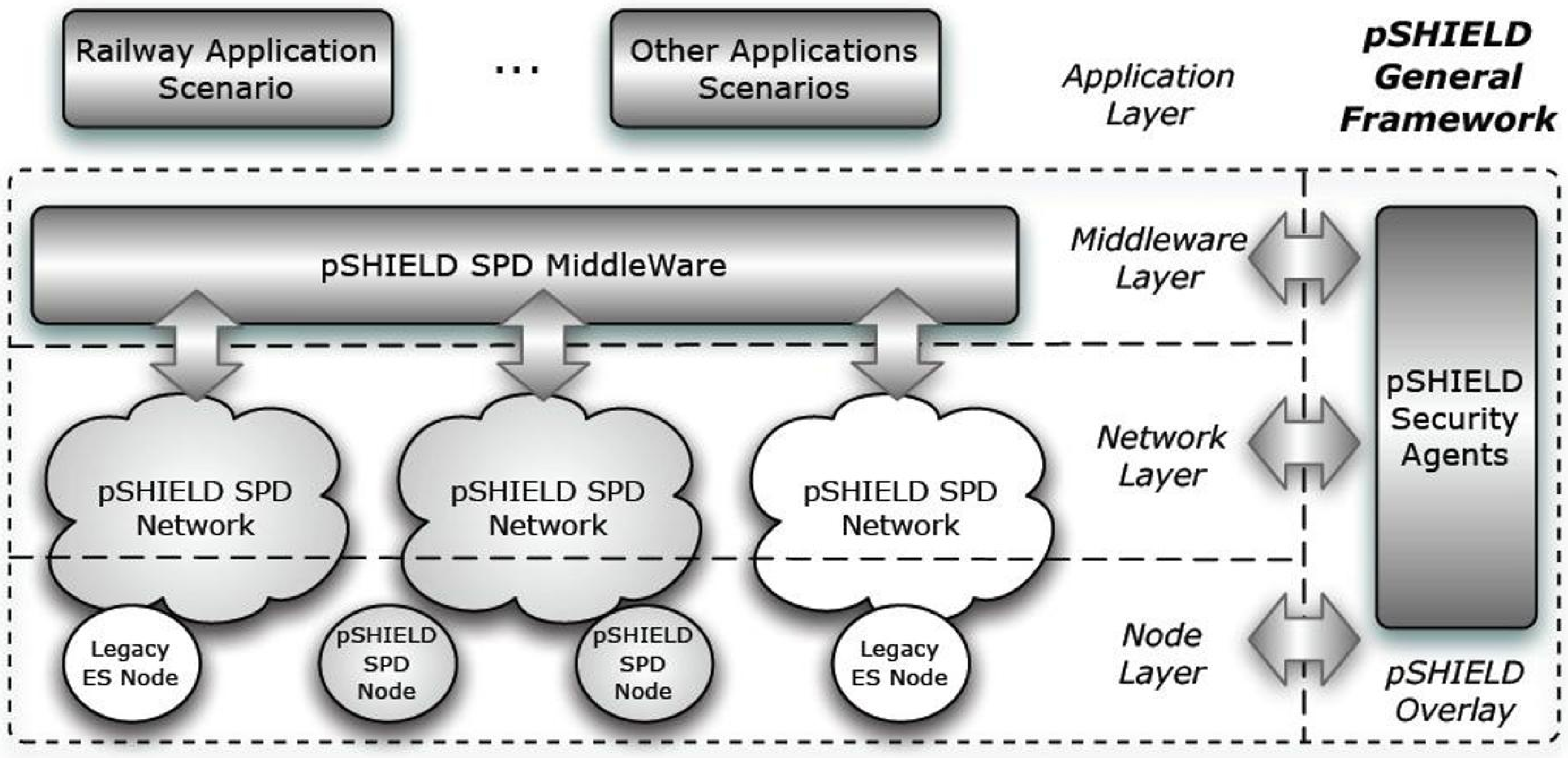
Technology Leader:
Antonio Di Marzo (SESM)
email: adimarzo@sesm.it

Norwegian Contact:
Josef Noll
email:josef@movation.no

Contributors: CWI, MOVATION, Jernbaneverket, telenor | objects

pSHIELD Architecture

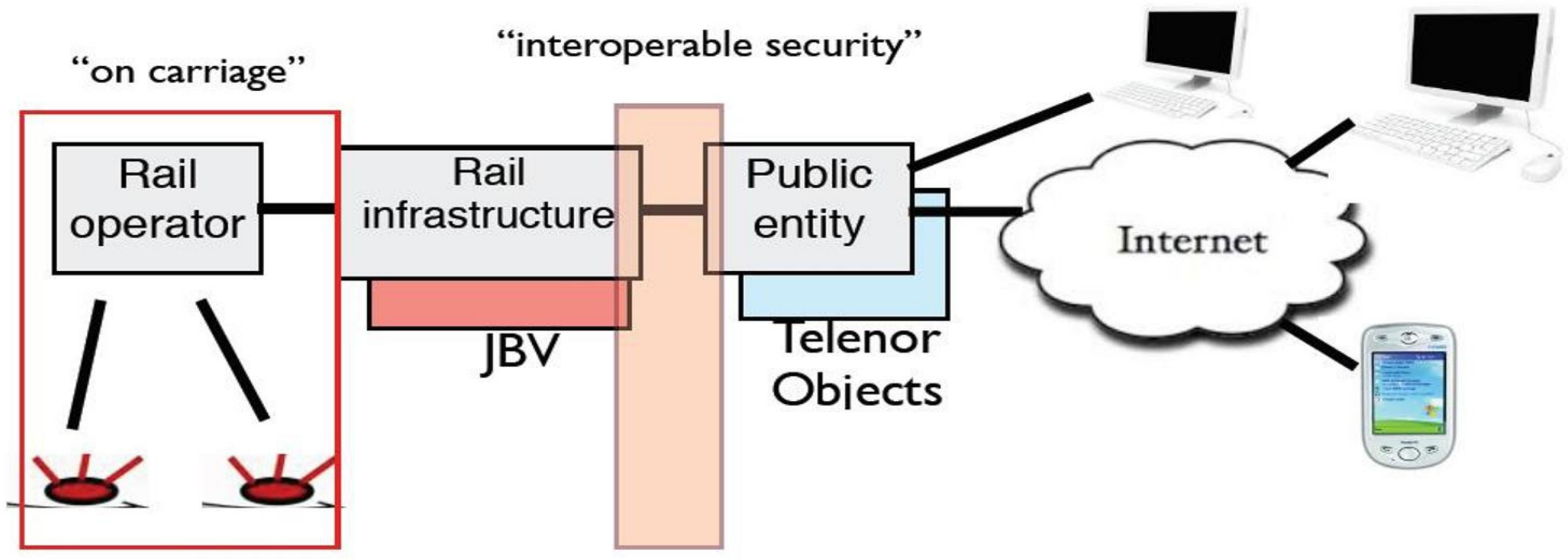
The concept of pSHIELD is to provide system’s functionalities, from the Security, Provacy and Dependability (SPD) perspectives, in a tightly integrated way incorporating nodes (sensors and devices), networks and middleware. The goals of pSHIELD will be achieved by approaching SPD at four levels: node (hardware and firmware), network (protocol), middleware (software) and overlay. The output of each layer will be available at the upper level , which will take advantage of SPD features developed at a lower level. SPD functionalities will be inserted seamlessly and transparently in each layer. The SPD functionalities can be dynamically enabled/disabled following the decisions of the Overlay. Such an approach will affectESs design cost-effectiveness because of the intrinsic SPD features of each layer in pSHIELD architecture. It ensures that future architecture will have the capability of being designed according to pSHIELD SPD requirements in a scalable and interoperable way.



Use Case: Interoperable Rail Information System (IRIS)

The use case of reference for this outlook is the continuously monitoring of trains and railway infrastructure. The purpose is twofold (i) detecting any unusual condition such as high temperature, extremely high temperature, strange sounds and unexpected movement, and (ii) transferring such information to different actor (i.e., train operator, rail infrastructure owner, consumer) involved in the rail system both automatically and in a request/response demand-based passive mode. The train is equipped with several heterogeneous computing devices such as sensors, actuators, GPS receiver, and gateway-embedded computer for detection of such conditions. These devices interact using heterogeneous protocols for sensing the information in their vicinity and sending it to the gateway. As an intelligent device, the gateway figures out any irregularity, and it sends the details to the smart train operator. If the irregularity information is related with rail infrastructure, then the infrastructure owner and provider is also interested to know about such information. The gateway send this information to all actors, but they also need monitoring and periodically checking about the condition of the train and the rail infrastructure.

Realization of pSHIELD



DEMO

- Handling sensors for critical infrastructures
- Sensors integration into middleware platform
- Addressing interoperability between JBV sensor and Telenor Object management platform
- Linking Sensor data while preserving privacy

Test Bed

- **Embedded System:** EPIA Nano-ITX embedded board
- **Operating System:** Ubuntu embedded Linux
- **Sensor Platform:** Sun SPOT, IQRF

Pilot SHIELD

pilot embedded Systems
arcHItecturE for multi-Layer Dependable solutions

SEVEN FRAMEWORK PROGRAMME
ARTEMIS