2nd Annual review
Florence 15th November 2013

nSHIELD

Railway security demonstrator

Physical Security Information Management (PSIM) systems for rail-based mass transit

• Rail-based mass transit systems are vulnerable to many criminal acts, including vandalism, thefts, pickpocketing, sabotage, terrorism.

• **Assets:** Tunnels, Vehicles, Line, Public areas (concourse, platform, etc.), Technical Rooms, Control Rooms, Depots, etc.

• In PSIM, heterogeneous intrusion detection, access control, intelligent audio-video surveillance, environmental sensors and CBRNe devices are integrated using different network links (wired copper/optical Ethernet, proprietary serial buses, WSN, Wi-Fi, Internet links, etc.)

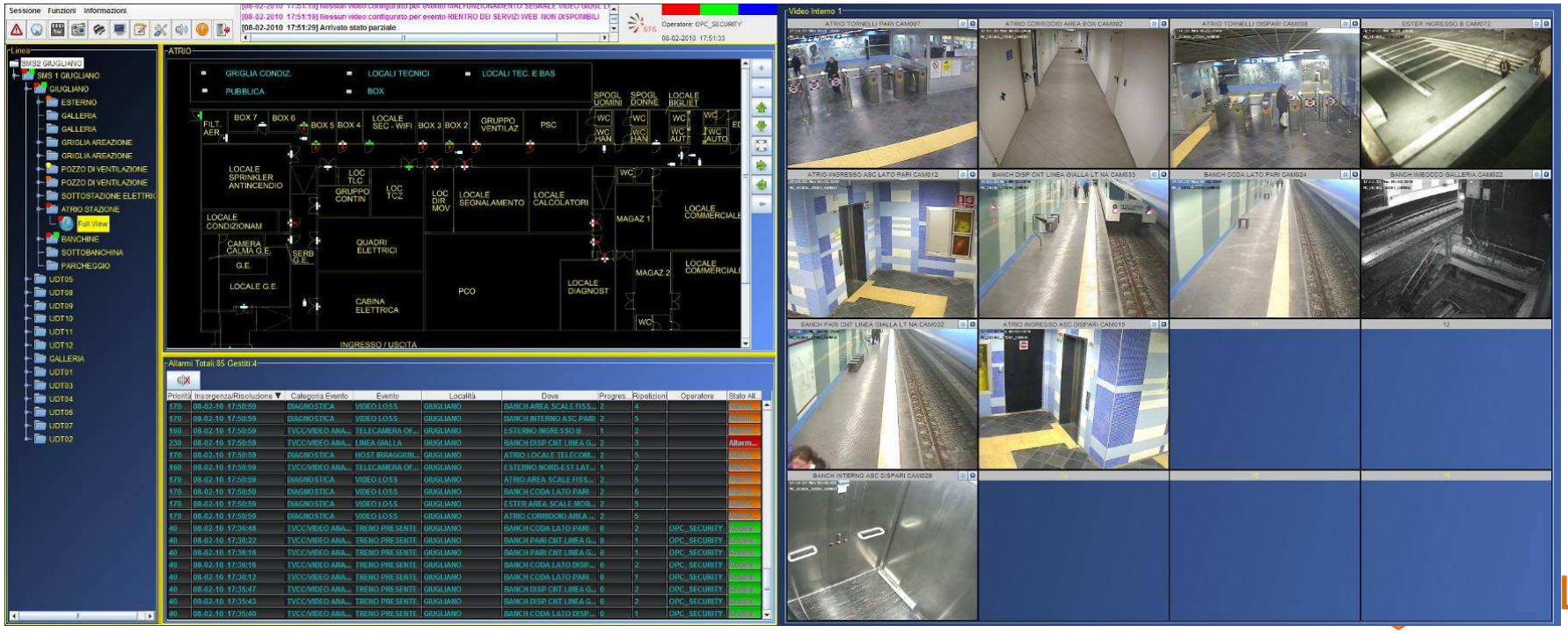
• Network links and devices are often installed in open areas, accessible to the public, and therefore exposed to several SPD threats (both random and malicious)

nSHIELD

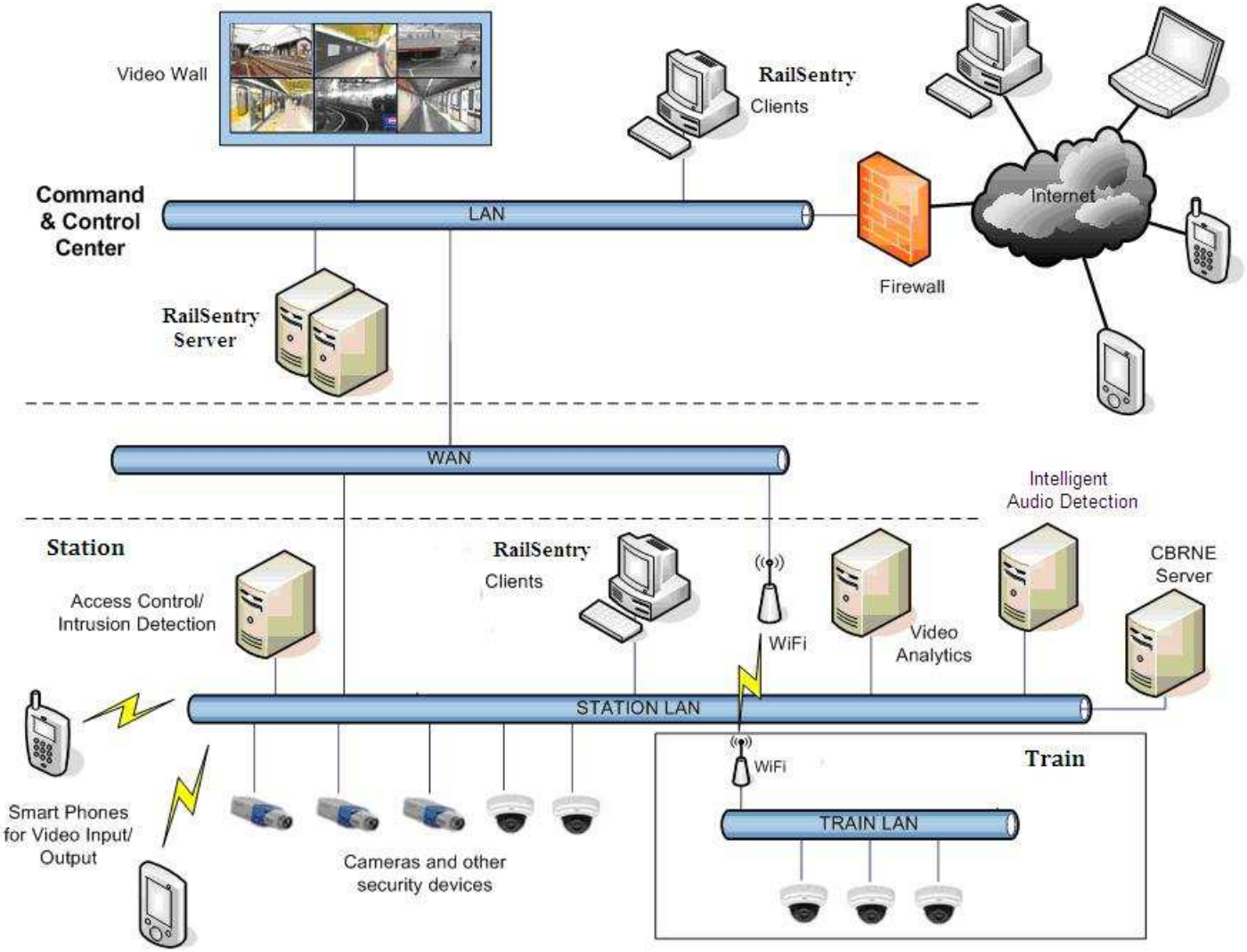
Ansaldo STS PSIM: RailSentry

• RailSentry core is a web-based software application featuring a graphical user interface.
• Architecture is distributed and hierarchical, with both local and central control rooms collecting sensor data. In case of emergencies, system orchestrates response procedures.

• System *Security, Privacy and Dependability* are essential since:
    • Information and alarms need to be trustworthy
    • Critical personal data (including passenger “faces”) is sent through the network
    • Surveillance needs to be highly available, fault-tolerant and resilient



RailSentry - Typical Architecture



nSHIELD

Issues and nSHIELD solutions

Heterogeneity in hardware and software technologies
Criticality in terms of SPD requirements

ISSUES:

How to effectively and efficiently protect the overall system (including proprietary protocols and legacy devices) against both random and malicious faults?

How to measure system SPD during system operation ?

nSHIELD solutions:

- Homogeneous embedded hardware and software architecture to collect, exchange and tune SPD information, allowing for fault/attack-detection and dynamic system reconfiguration, according to system-level SPD requirements

- Justifiably measurable and real-time dynamically upgradeable SPD by means of appropriate metrics, ontologies, semantic models and composability mechanisms

nSHIELD

Example risk analysis to classify threats

Assets to protect	Threats	Vulnerability (V)	Likelihood (P)	Consequences (D)	Risk R= P xV x D
Ethernet Camera Analog Microphone	Physical tamper/manumission	HIGH If they are located in a public c area.	LOW	LOW Operation of the single sensor is compromised, as the related monitoring functionality. The easy detection of the attack reduces its impact	**LOW**
Ethernet Camera Wi-Fi Camera Mote WSN	HW fault: •Loss of component functionality •Loss of sensor functionality SW fault: Bug, Aging, Transient fault	MEDIUM In general HW and SW are vulnerable, especially after some operation time, to this fault.	MEDIUM It depends on HW and SW robustness and environmental condition.	MEDIUM Effects range from loss of specific functions to loss of related monitoring functionality. It is difficult to diagnose	**MEDIUM**
Application server	Unauthorized network access Sniffing	MEDIUM The network is connected to the Internet. Using firewalls reduces vulnerability	MEDIUM Nowadays attempts to attack public utility servers are not rare	HIGH Once accessed by the attackers, the servers are completely under their control, and furthermore the attack con be difficult to detect.	**HIGH**

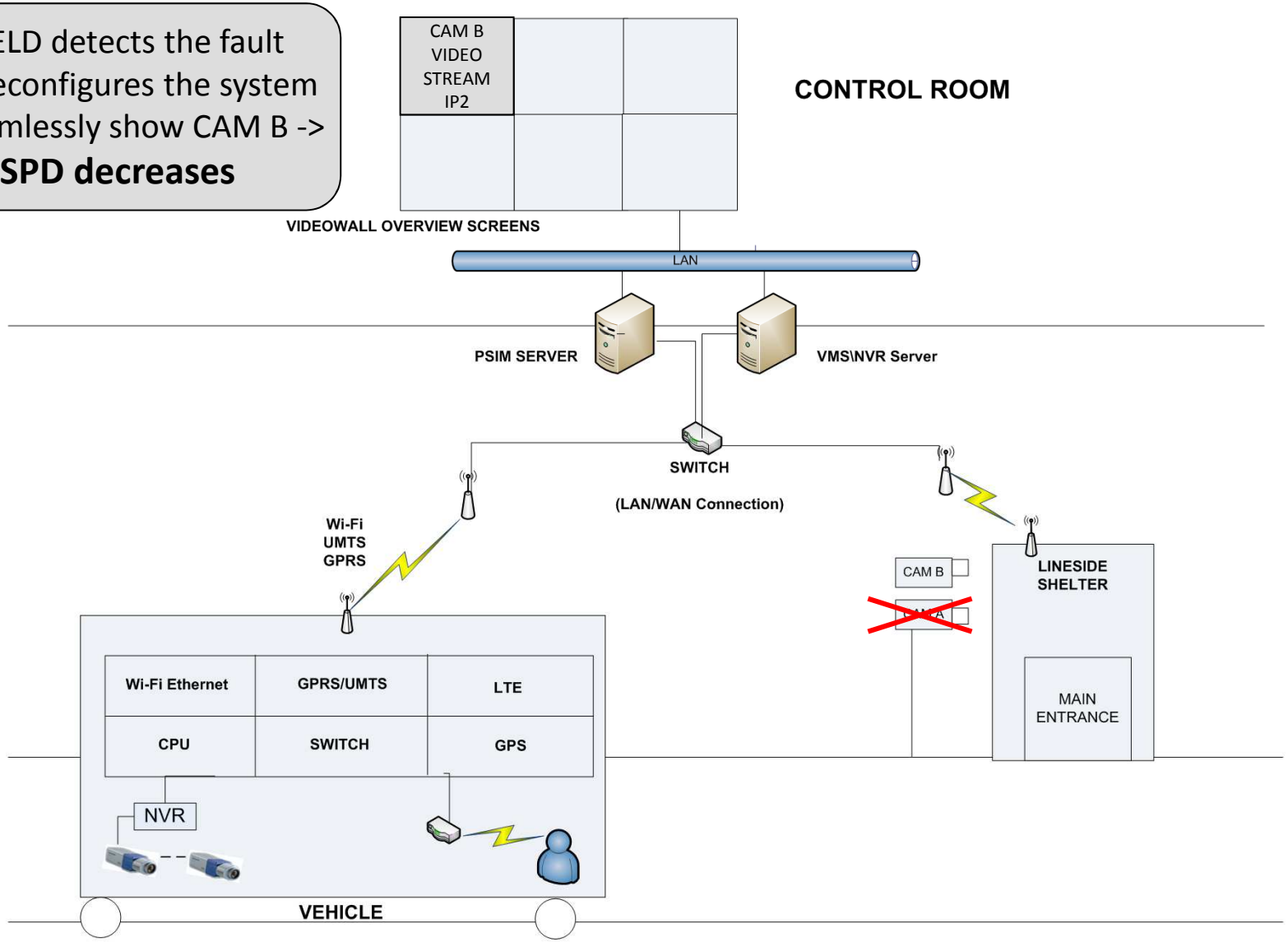
P V	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

PV D	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

nSHIELD

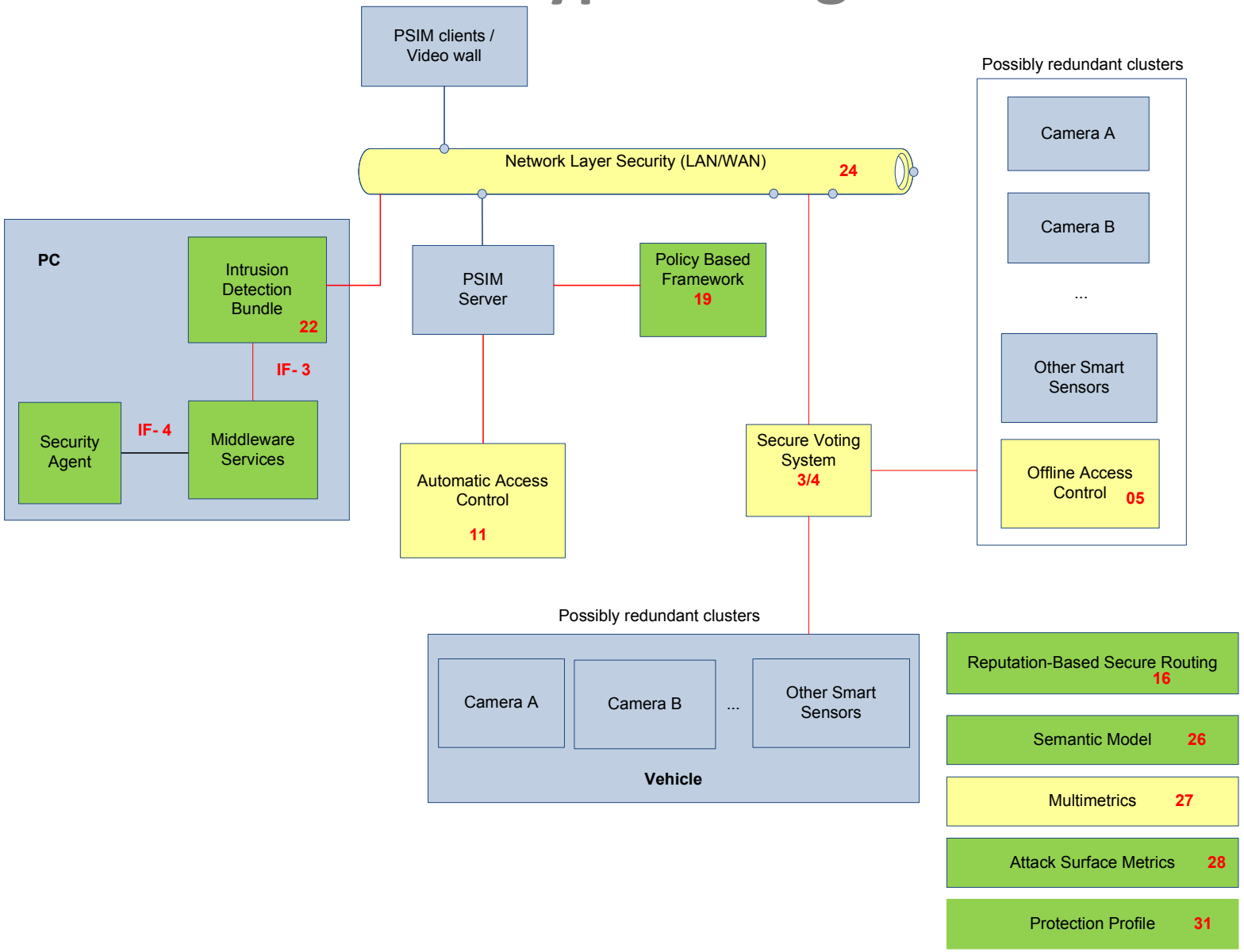
Railway security demonstrator example

SHIELD detects the fault and reconfigures the system to seamlessly show CAM B -> **SPD decreases**



nSHIELD

Prototypes Integration



nSHIELD

Prototypes involved

Code	Prototype name	Description	Partner
3	Hypervisor	Guaranteeing isolation and secure interaction between co-existing open software components	SICS
4	Secure Boot	The firmware for CPU core to prevent tampering	T2D
5	Secure Power (&) Communication cape	Secure Access control system	AT/TELC/TUC
11	Automatic Access Control	Access control mechanisms for physical resources of a network node	TUC
16	Reputation-Based Secure Routing	For WSN sensors	TUC/HAI
19	Policy based access control	Control of access to devices and their resources via security policies	TUC/HAI
20	Control Algorithms	Reconfiguration	UNIROMA
22	Middleware Intrusion Detection System	Filter for middleware services	S-LAB
24	Network Layer Security	Security communication between nodes	TUC
25	OSGI Middleware	Platform for middleware services	UNIROMA
26	Semantic Model	Domain description	UNIROMA
27	Multimetrics	Metrics computation	TECNALIA
28	Attack Surface Metrics	metrics computation	SES
31	Middleware Protection Profile	Defines the rules or rather the SPD requirement for prototypes Integration	SES
32	Secure Discovery	Middleware service	UNIROMA
33	Security Agent	Middleware service	UNIROMA

The END

That’s all folks!