Barcelona, March 6th 2013

nSHIELD Project

Rail-Based Mass Transit Security Case-Study

ARTEMIS

nSHIELD

AnsaldoSTS
A Finmeccanica Company

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

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

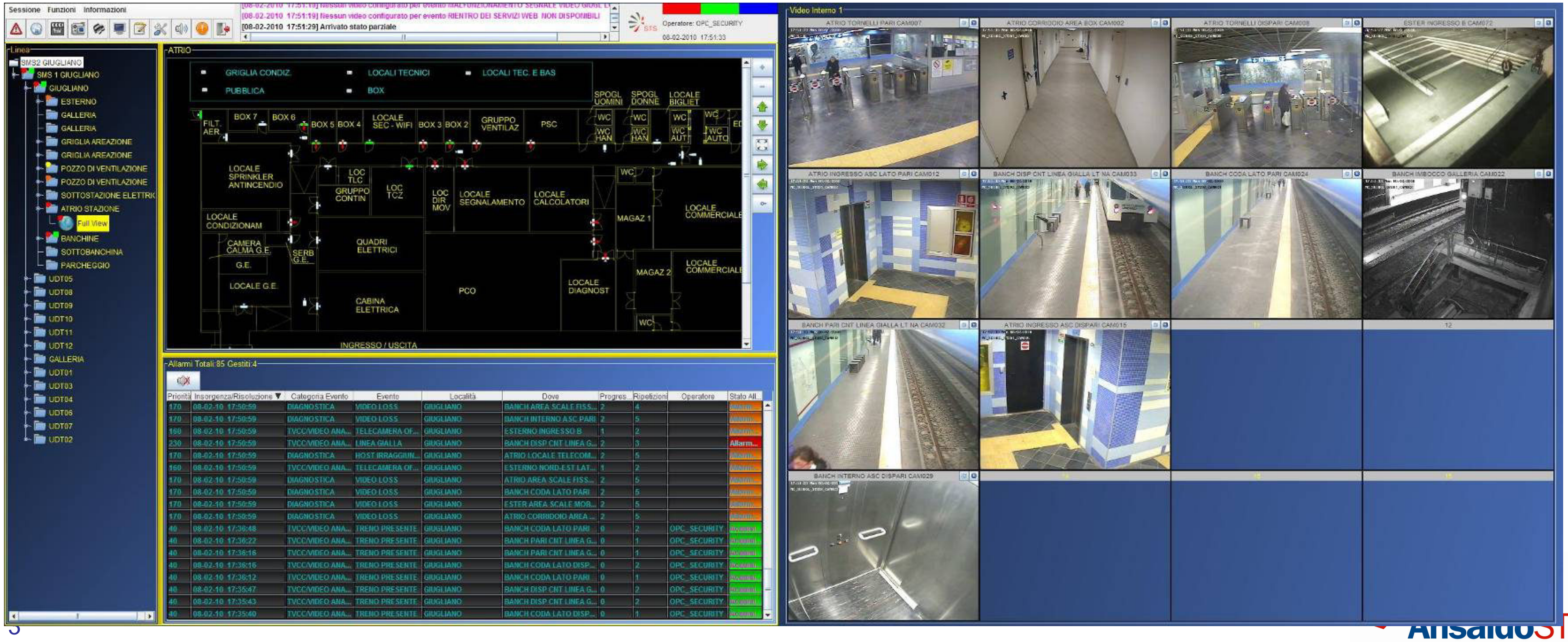
- **Assets:** Tunnels, Vehicles, Line, Public areas (concourse, platform, etc.), Technical Rooms, Control Rooms, Depots, etc.

- 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 SPD threats (both random and malicious).

Ansaldo STS PSIM: RailSentry

- RailSentry core is a web-based software application featuring a graphical user interface.
- The architecture is distributed and hierarchical, with both local and central control rooms collecting remote sensor data.
- In case of emergencies, the procedural actions are orchestrated by RailSentry.
- System Security, Privacy and Dependability is essential since it processes critical personal data (including passenger "faces"), it must be highly available and alarms need to be trustworthy.



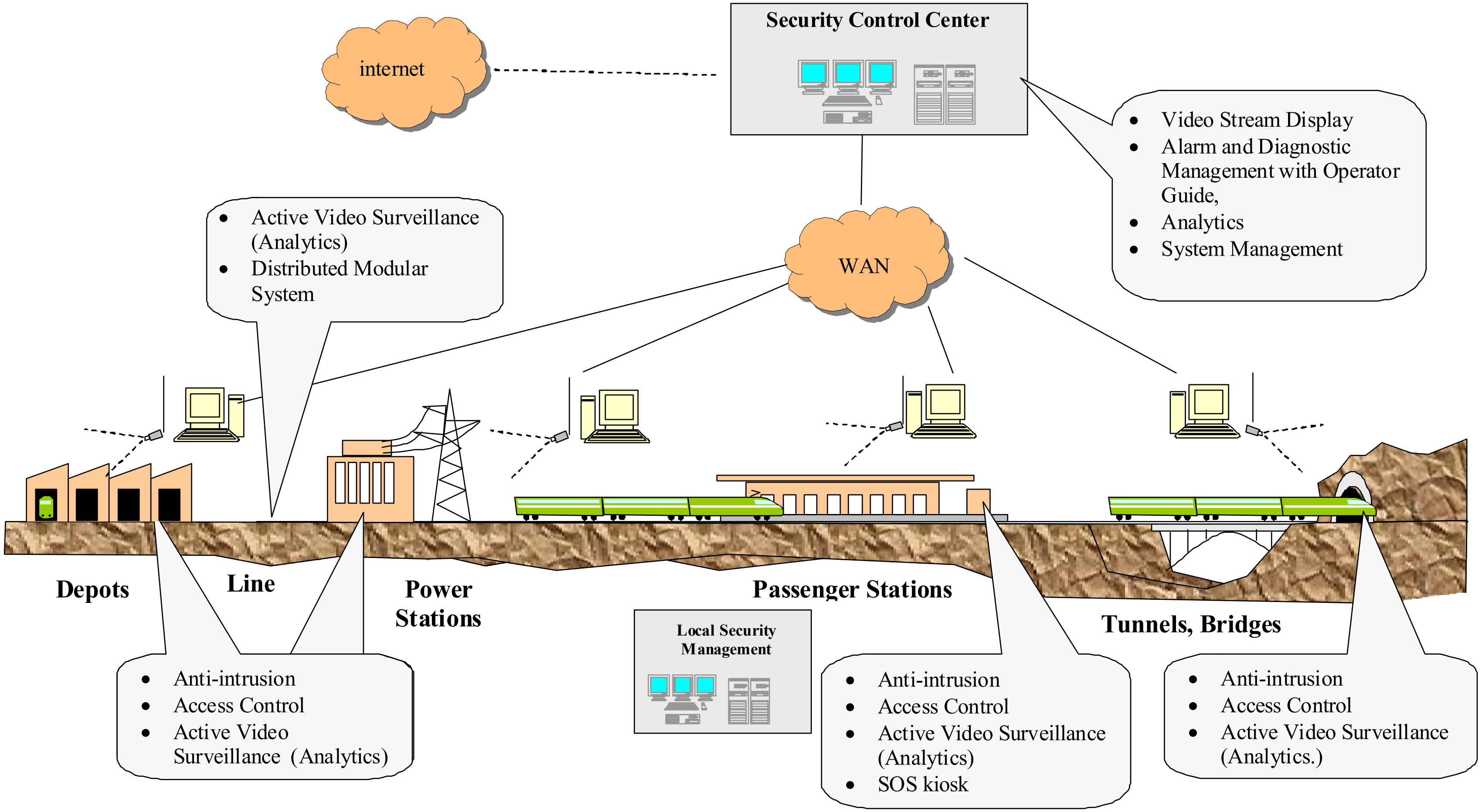
```
[08-02-2010  17:51:19] Nessun video configurato per evento MALFUNZIONAMENTO SEGNALE VIDEO GIUGL L
[08-02-2010  17:51:19] Nessun video configurato per evento RIENTRO DEI SERVIZI WEB  NON DISPONIBILI
[08-02-2010  17:51:29] Arrivato stato parziale
```

Operatore: OPC_SECURITY
08-02-2010 17:51:33

Allarmi Totali:85 Gestiti:4

Priorità	Insorgenza/Risoluzione ▼	Categoria Evento	Evento	Località	Dove	Progres...	Ripetizioni	Operatore	Stato All...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	BANCH AREA SCALE FISS...	2	4		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	BANCH INTERNO ASC PARI	2	5		Allarm...
160	08-02-10 17:50:59	TVCC/VIDEO ANA...	TELECAMERA OF...	GIUGLIANO	ESTERNO INGRESSO B	1	2		Allarm...
230	08-02-10 17:50:59	TVCC/VIDEO ANA...	LINEA GIALLA	GIUGLIANO	BANCH DISP CNT LINEA G...	2	3		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	HOST IRRAGGIUN...	GIUGLIANO	ATRIO LOCALE TELECOM...	2	5		Allarm...
160	08-02-10 17:50:59	TVCC/VIDEO ANA...	TELECAMERA OF...	GIUGLIANO	ESTERNO NORD-EST LAT...	1	2		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	ATRIO AREA SCALE FISS...	2	5		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	BANCH CODA LATO PARI	2	5		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	ESTER AREA SCALE MOB...	2	5		Allarm...
170	08-02-10 17:50:59	DIAGNOSTICA	VIDEO LOSS	GIUGLIANO	ATRIO CORRIDOIO AREA ...	2	5		Allarm...
40	08-02-10 17:36:48	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO PARI	0	2	OPC_SECURITY	[illegible]
40	08-02-10 17:36:22	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH PARI CNT LINEA G...	0	1	OPC_SECURITY	[illegible]
40	08-02-10 17:36:16	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH PARI CNT LINEA G...	0	1	OPC_SECURITY	[illegible]
40	08-02-10 17:36:16	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO DISP...	0	2	OPC_SECURITY	[illegible]
40	08-02-10 17:36:12	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO PARI	0	1	OPC_SECURITY	[illegible]
40	08-02-10 17:35:47	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH DISP CNT LINEA G...	0	2	OPC_SECURITY	[illegible]
40	08-02-10 17:35:43	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH DISP CNT LINEA G...	0	2	OPC_SECURITY	[illegible]
40	08-02-10 17:35:40	TVCC/VIDEO ANA...	TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO DISP...	0	1	OPC_SECURITY	[illegible]

Physical Security Systems for Railways: an overview



Security Control Center

- Video Stream Display
- Alarm and Diagnostic Management with Operator Guide,
- Analytics
- System Management

internet

WAN

- Active Video Surveillance (Analytics)
- Distributed Modular System

Depots

Line

Power Stations

Passenger Stations

Tunnels, Bridges

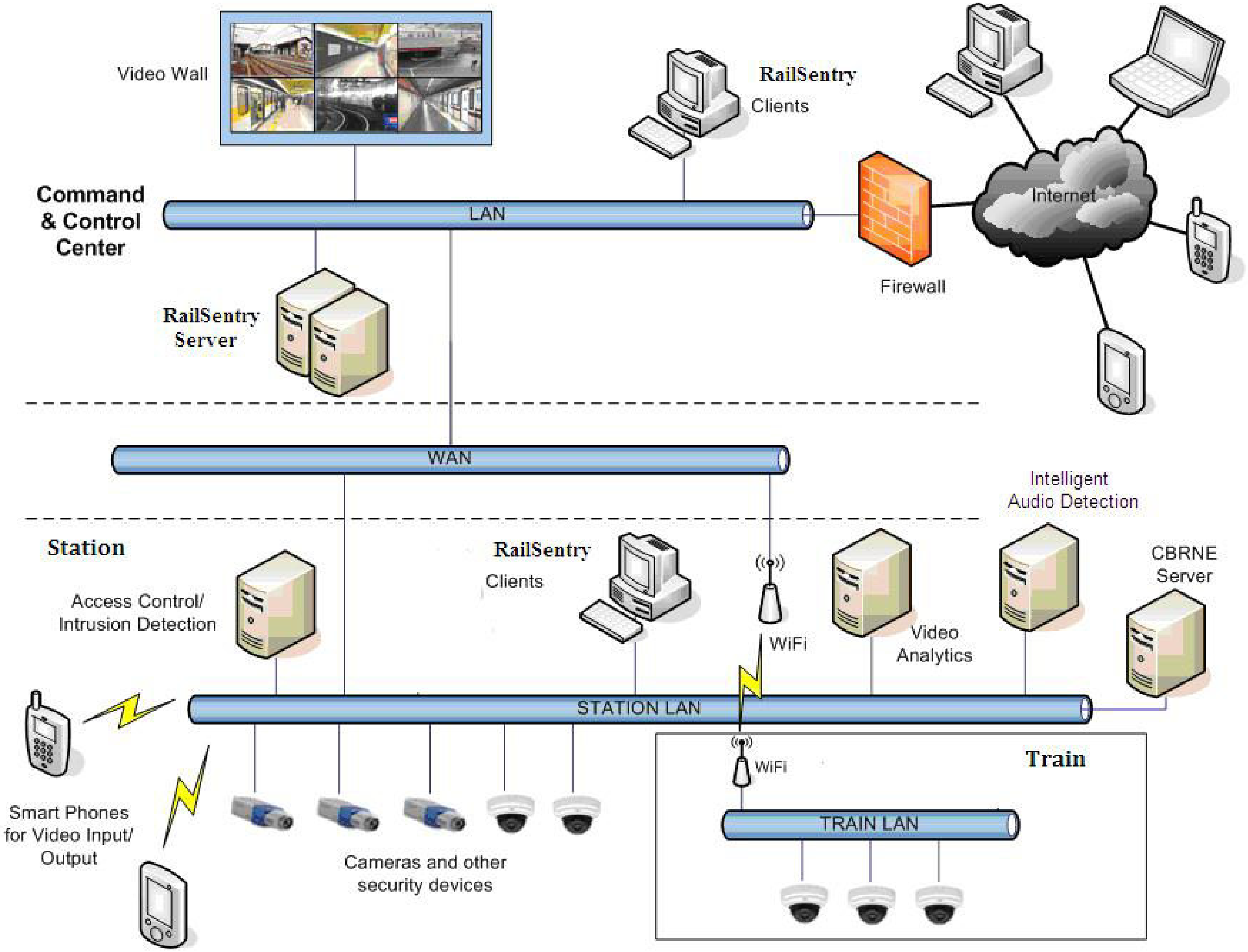
Local Security Management

- Anti-intrusion
- Access Control
- Active Video Surveillance (Analytics)

- Anti-intrusion
- Access Control
- Active Video Surveillance (Analytics)
- SOS kiosk

- Anti-intrusion
- Access Control
- Active Video Surveillance (Analytics.)

RailSentry - Typical Architecture



AnsaldoSTS
A Finmeccanica Company

RailSentry: Problems and Needs

- Currently, the system is highly heterogeneous in terms of detection technologies (which will remain such), embedded computing power and communication protocols/interfaces.

- Very difficult (if not impossible) to ensure holistic measurable and justifiable SPD.

Problems -> Needs:

  - **Lack of homogeneous information security levels** → need for common and easily configurable (possibly from a control post) cryptographic protocols for data integrity and confidentiality.

  - **Not easy integration of new devices (proprietary protocols and different SPD)** → need for seamless integration of new devices with the possibility of directly evaluating the impact of such integration on the overall system SPD.

  - **The holistic assurance and evaluation of dependability parameters (e.g. for assessment/certification purposes or even in real-time after component failures) would be a very difficult task** → appropriate "adaptive" (possibly computable "on-line" during system operation) metrics are required.

  - **Lack of resilience: faults can impact on system availability and indirectly on safety** → automatic fault-detection and system reconfiguration.

Threats to open communication channels (wireless, Internet, etc.) as defined by the CENELEC railway standards

The mechanisms provided by nSHIELD would mitigate the effects on the system of the following logical threats:

- **Repetition** (a message is received more than once)
- **Deletion** (a message is removed from a message stream)
- **Insertion** (a new message is implanted in the message stream)
- **Re-sequencing** (messages are received in an unexpected sequence)
- **Corruption** (the information contained in a message is changed, casually or not)
- **Delay** (messages are received at a time later than intended)
- **Masquerade** (a non-authentic message is designed thus to appear to be authentic)

For example, those terms are used as “keywords” in hazard analysis for railway control systems in order to find appropriate countermeasures (timestamps, sequence numbers, CRC, etc.).

Risk analysis

Assets to protect	Threats	Vulnerability (V)	Likelihood (P)	Consequences (D)	Risk R= P xV x D
Ethernet Camera **Analog Microphone**	Physical tamper/manumission such as: •Cable disconnection; •Theft •Significant movement or replacement •Other relevant damage meant to put the unit out of order	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 diagnosability 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

SHIELD solutions

Today Gaps	SHIELD Adavantages	RAILWAY SECURITY Scenario
Information Security	Cryptographic protocols improve data security.	Requirments, Architecture, Node layer, Network layer, Middleware layer
Integration of new devices	SHIELD permits the integration of new systems and the evaluation of impact on the overall system dependability.	Requirement, Architecture, Metrics, Node layer, Network layer, Overlay layer
Complex Certification	Easy certification of the overall architecture	Requirement, Architecture, Standardisation
Faults Resilience	Automatic reconfiguration	Requirement, Architecture, Metrics, Node layer, Network layer, Overlay layer
Expensive Integration of different standards	SHIELD standard will embrace different standards	Standardisation, Dissemination