nSHIELD- Use case description: Railway security

The context and architecture

Rail-based mass transit systems are vulnerable to many criminal acts, ranging from vandalism to terrorism. Therefore, physical security systems for infrastructure protection comprises all railway assets as for tunnel, train on board, platform and public areas, external Areas, technical control room, depots, electrical substations and etc…
The objectives are to forecast critical threats as: aggressions and abnormal behaviours, sabotage and terrorism, vandalism and graffiti, thefts and pickpocketing.
A modern smart-surveillance system suitable for the protection of urban or regional railways is made up by the following subsystems:

1. Intrusion detection and access control:
    - volumetric sensors for motion detection;
    - magnetic contacts to detect illicit doors opening;
    - glass break detectors;
    - microphonic cables for fence/grill vibration detection;
    - active infrared barriers for detecting intrusions inside the tunnels;
2. Intelligent video-surveillance and Intelligent sound detection:
    - advanced cameras with special features;
    - digital video processing and recording, using efficient data compression protocols;
    - video-analytics of the scenes, using computer vision algorithms;
    - Microphones.
3. Dedicated communication network
4. Integrated management system

Distributed smart-sensors are installed along the railway line both in fixed (e.g. bridges, tunnels, stations, etc.) and mobile (passenger trains, freight cars, etc.) locations (Figure 1).

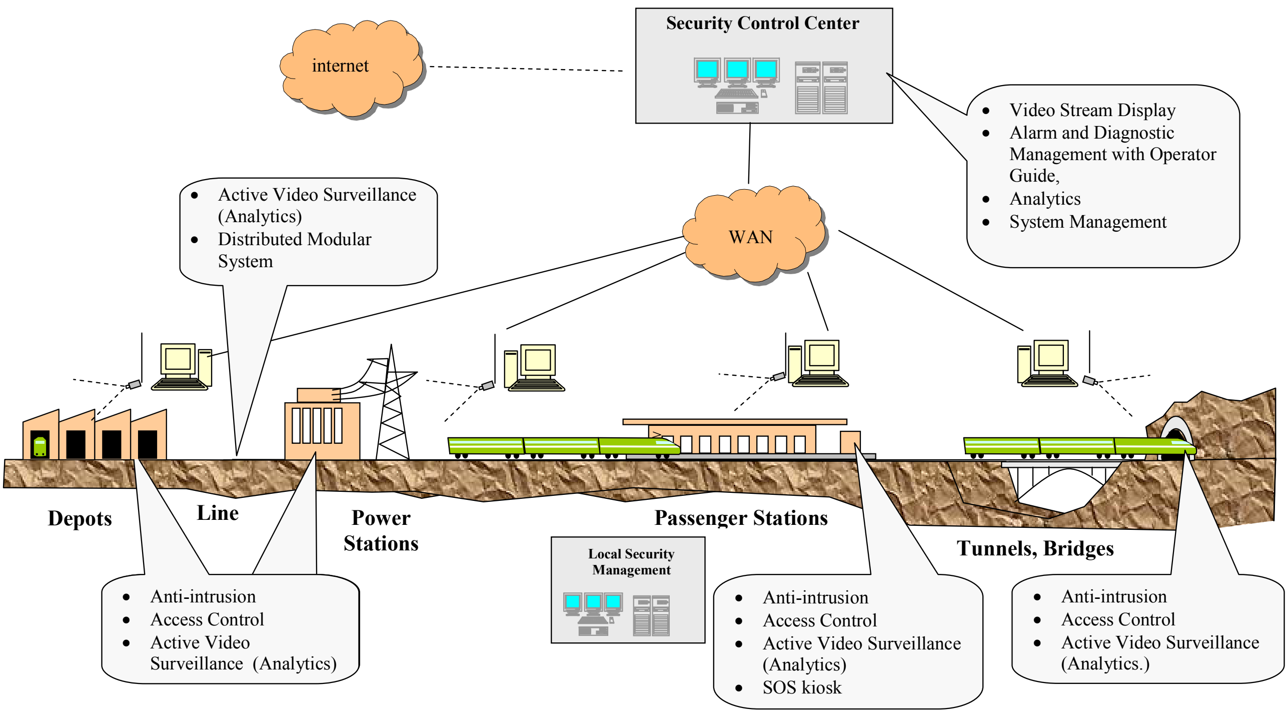

Figure 1 The monitoring architecture

They are integrated locally using local wireless infrastructures (e.g. Wi-Fi, ZigBee, etc.) and then data is collected by WSN gateway nodes and transmitted remotely by means of WAN (Wide Area Network). Low/average bandwidth networks are strictly required to transmit alarms to the control center, which are often already available (like GSM-R for railways) or easy to deploy (like satellite) and provide an extensive coverage of the infrastructure. However, if high-quality video streams from cameras need to be shown to the operators in order to verify the alarm and/or supervise the situation, higher bandwidth is required which can be possible achieved by multiple low bandwidth connections.

This system are already been designed by Ansaldo STS for metro railways, where heterogeneous intrusion detection, access control, intelligent video-surveillance and abnormal sound detection devices are integrated in a cohesive Security Management System (SMS), figure 2.

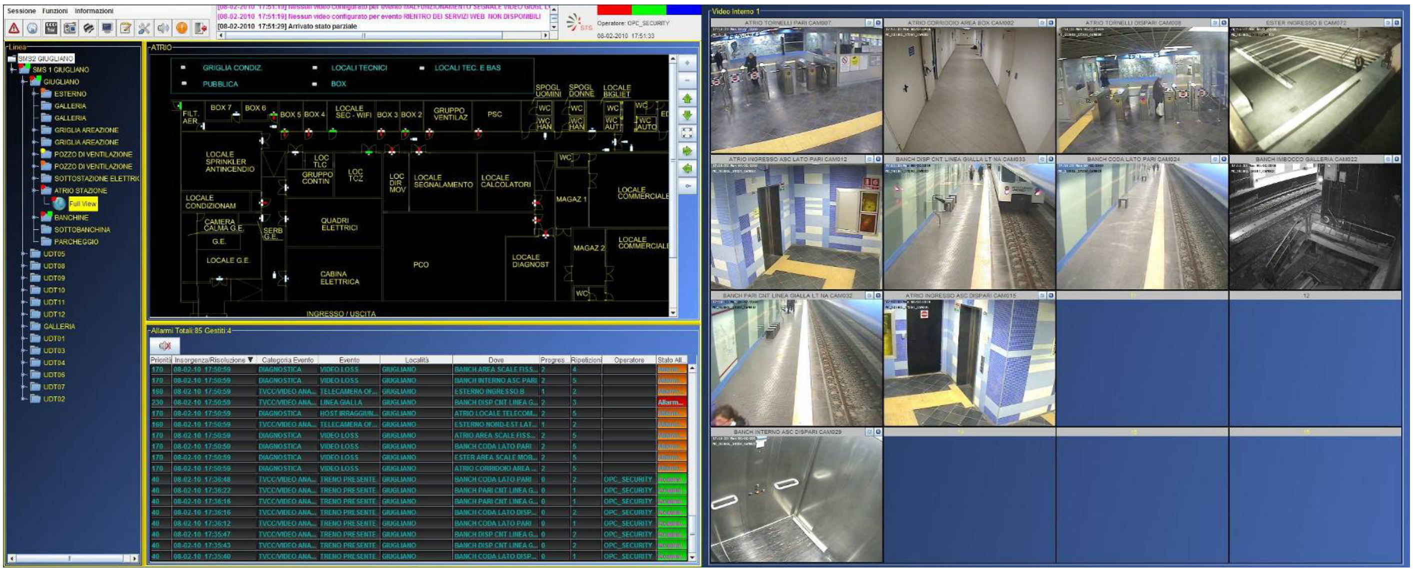

Figure 2 SMS-Security Management System GUI

The core of the SMS consists of a web-based software application featuring a graphical user interface. System architecture is distributed and hierarchical, with both local and central control rooms collecting alarms according to different scopes and responsibilities. In case of emergencies, the procedural actions required to the operators involved are orchestrated by the SMS. Redundancy both in sensor dislocation and hardware apparels (e.g. by local or geographical clustering) improve detection reliability, through alarm correlation, and overall system resiliency against both random and malicious threats. Video-analytics is essential, since a small number of operators would be unable to visually control the large number of cameras which are needed to extensively cover all the areas needing to be protected. Therefore, the visualization of video streams is activated automatically when an alarm is generated by smart-cameras or other sensors, following an event-driven approach. Very high resolution cameras installed close to the turnstiles are used to automatically detect and store the faces of passengers, whose database can be accessed for post-event investigations. Real-time communication between the on-board and the ground is allowed by a wide-band wireless network.

Needs and problems

Currently, the security system described above is highly heterogeneous in terms not only of detection technologies (which will remain such) but also of embedded computing power and communication facilities. In other words, sensors differ in their inner hardware-software architecture and thus in the capacity of providing information security and dependability. This causes several problems:

- Information security must be provided according to different mechanisms and on some links - which are not “open” but still vulnerable to attacks - information is not protected by cryptographic nor vitality-checking protocols;
- Whenever any new sensor needs to be integrated into the system, a new protocol and/or driver must be developed and there is no possibility of directly evaluating the impact of such integration on the overall system dependability;
- New dedicated and completely segregated network links often need to be employed in order not to make the sensor network exposed to information related threats;
- The holistic assurance and evaluation of dependability parameters (e.g. for assessment/certification purposes) would be a very difficult task.

In particular both natural and malicious faults can impact on system availability and indirectly on safety, since the SMS is adopted in critical infrastructure surveillance applications.

The problems mentioned above can be solved by adopting the nSHIELD architecture. Cohesion will be assured by wrapping sensors of any nature with homogeneous embedded hardware and software providing information security, by e.g.:

- Cryptographic protocols
- Vitality checking (heartbeat/watchdog timers based on sequence numbers and time-stamping)

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)

Some sensing devices will be converted into smart-sensors by integrating the sensor unit with the nSHIELD processing units (both hardware and software) at the node level. The sensor networks will be integrated by the nSHIELD middleware before data is collected by the SMS and used at the presentation level (integration and reasoning).

Typically, the monitoring system is composed by different sensors (IP-cameras, microphones, anti-intrusion device, etc…). They are connected through different communication networks and several topologies to a data center. The data center is connected to commad and control center. In figure is showed a typical architecture.

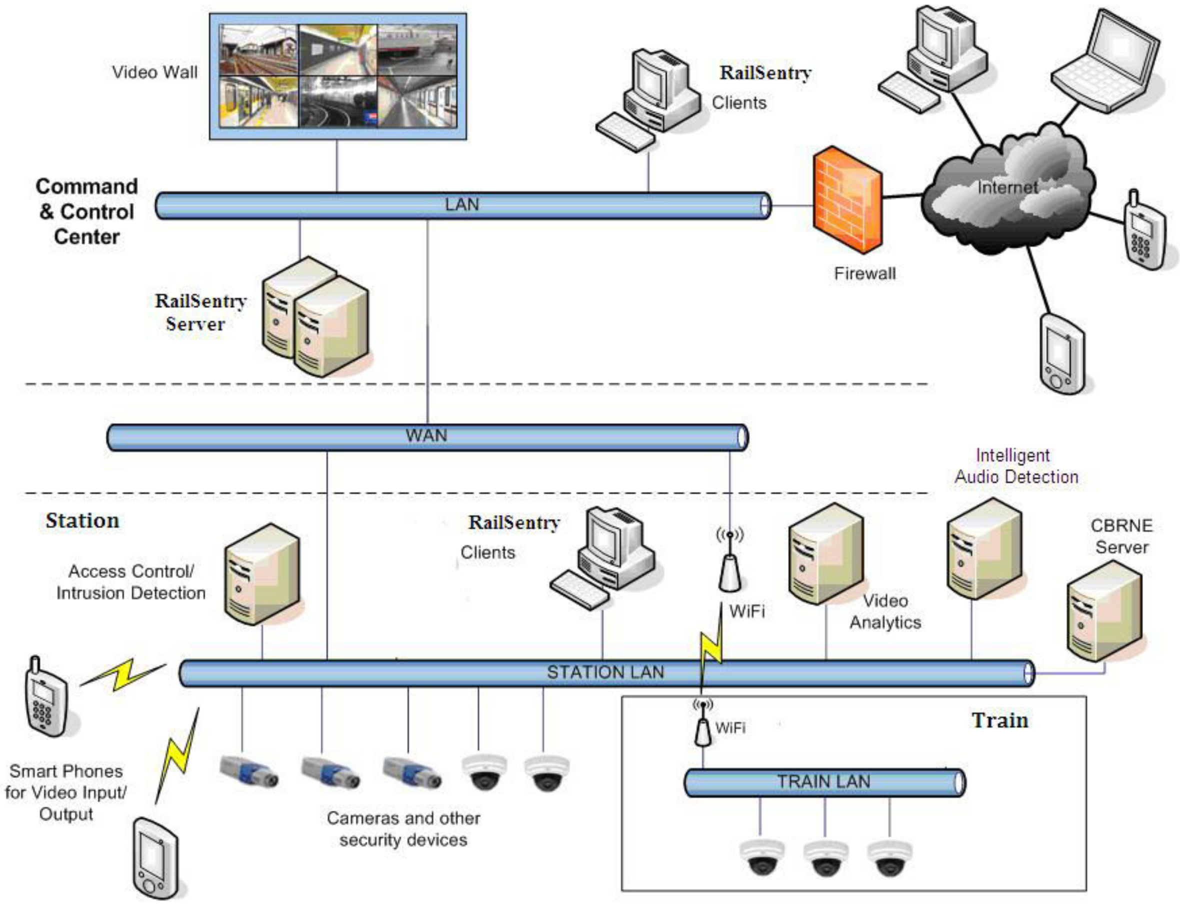

Figure 3 System Security architecture

The sensors collect information about asset and send them to the Security Management Systems (SMS).

The security system is composed by different sub-systems such as: video-surveillance, anti-intrusion detection, smart-audio surveillance. Signals coming from different sub-systems are elaborate in order to detect the corresponding events.

The video-surveillance sub-system is able to guarantee both traditional functionalities (video stream management from different cameras, digital recording) and automatic video-analytics (motion detection, motion tracking) in order to manage critical events in the station.

The anti-intrusion sub system and access control detect non-authorized access to protected sites (depots, Technical control rooms, etc..) . The elaboration servers are able to recognize false alarms with the use of different type of technologies.

The smart-audio-surveillance Sub-systems is able to:

- Detect abnormal sound corresponding to vandalism, aggressions, etc…
- Identify the place in which happens this acts.

All sub-systems are connected through dedicated and completely segregated network links. .Instead, real-time communication between the on-board and the ground is allowed by a wide-band wireless network.

Risk Analysis

Risk analysis will be used for evaluation of SPD risk in the nSHIELD railway security scenario.

Is possible to approach with the following steps:

- Define asset/component;
- For each asset/component will be identified the threat (T);
- For each T identified will be defined:
  - Likelihood (P): expected probability of occurrence of T (i.e. how probable is the threat);
  - Vulnerability (V): expected vulnerability with respect to T (i.e. how probable is it that T will cause the expected consequences);
  - Consequences (D): expected damage caused by T (i.e. an estimation of consequences caused by the threat);
  - calculate risk (R): $R = P \cdot V \cdot D$.

For likelihood, vulnerability and consequences evaluation is adopted a qualitative technique.

Qualitative evaluation use reduced scales of values of intuitive meaning, for instance: Low, Medium, High. The advantage is that estimations can be more straightforward and computations easier. The disadvantage is that results are usually less rigorous and the combination of qualitative indices questionable.

The $P \cdot V$ factor is compacted into a single factor, which – to avoid confusion – we will define here as the frequency F of "successful" threats. Hence:

$$F = P \cdot V$$

The F evaluation is conducted through an associative matrix:

Table 1 Qualitative frequency evaluation using associative matrix

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

Qualitative risk evaluation uses associative matrix reported below using the estimated values of F and D:

Table 2 Qualitative Risk evaluation using associative matrix

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

Based on this information is possible to identify the mean element of architecture to protect and possible threats for Railroad Security scenario. In table 1 are showed some components and relative 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.	HIGH	LOW Operation of the single sensor is compromised, as the related monitoring functionality. The easy diagnosability of the attack reduces its impact	MEDIUM
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.	HIGH 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	HIGH
Ethernet Camera **Wi-Fi Camera** **Mote WSN**	Alteration of connection due to: • Network overload • Involuntary disconnection	MEDIUM It depends on environmental condition, bandwidth, capacity of connection, number of sensors	MEDIUM It depends on network architecture.	LOW Communication of the single sensor is compromised, as the related monitoring functionality. The easy diagnosability of the fault reduces its impact	LOW
Ethernet Camera	Unauthorized network access Data destruction	LOW Connection are wired and encrypted It depends on attacker ability.	LOW	HIGH The attacker take the control of communication and he can alterate the data of sensors and relative alarms. It is difficult to diagnose.	MEDIUM
Wi-Fi Camera **Mote WSN**	Physical tamper/manumission, such as: • Theft • Significant movement or replacement • Any other relevant damage meant to put the unit completely out of order	HIGH If they are located in a public c area.	MEDIUM	MEDIUM Operation of the single sensor is compromised, as the related monitoring functionality. The easy diagnosability of the attack reduces its impact	HIGH
Wi-Fi Camera **Mote WSN**	Alteration of connection due to: • Interferences with electromagnetic device	HIGH The connection are wireless	LOW It depends of network architecture.	LOW Operation of the single sensor is compromised, as the related monitoring functionality. The easy diagnosability of the fault reduces its impact	LOW
Wi-Fi Camera **Mote WSN**	Unauthorized network access Data destruction	MEDIUM Connection are wireless but can be encrypted	MEDIUM	HIGH The attacker take the control of communication and he can alterate the data of sensors and related alarms. It is difficult to diagnose.	HIGH
Ethernet Camera **Wi-Fi Camera** **Mote WSN**	Data alteration	MEDIUM Connections can be encrypted	MEDIUM	HIGH The attacker takes control of communication and he/she can modiify the data of sensors and related alarms. It is difficult to diagnose.	HIGH
Ethernet Camera	Data Sniffing	LOW Connection is wired	MEDIUM It requires physical access to cable connection.	HIGH	MEDIUM
Wi-Fi Camera **Mote WSN**	Data Sniffing	HIGH Connection is wireless	HIGH It requires equipments available commercially	HIGH	HIGH

Analog Microphone	HW fault: • Loss of component functionality • Involuntary disconnection	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
Wi-Fi Camera **Mote WSN**	Transmitted data scrambling (e.g. high- power microwave generators)	HIGH	LOW It requires equipments not available commercially	MEDIUM Since it can affect a large number of sensors located in the same area.	MEDIUM
Anti-intrusion sensor (via serial loop through proprietary protocol)	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.	MEDIUM	HIGH Operation of the single sensor is compromised, as the related monitoring functionality. The easy diagnosability of the attack reduces its impact	HIGH
Anti-intrution sensor (via serial loop through proprietary protocol)	HW fault: • Loss of component functionality • Involuntary disconnection 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
Anti-intrusion sensor (via serial loop through proprietary protocol)	HW fault: • Loss of component functionality • Involuntary disconnection	MEDIUM In general HW and SW are vulnerable, especially after some times, 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	Random corruption of data Loss of data integrity	MEDIUM It depends on redundant/fault-tolerant components.	LOW It depends on how much the HW is reliable/ruggedized and on environmental conditions (e.g. air conditioning).	HIGH Effects range from loss of specific functions to loss of a whole (sub)system.	MEDIUM
Application server	Physical tamper/manumission such as: • Cable disconnection; • Theft • Significant movement or replacement • Other relevant damage meant to put the unit out of order	LOW The servers are in technical control room	LOW The servers are in technical control room	HIGH The monitoring application is compromised	MEDIUM
Application server	Unauthorized network access Sniffing	MEDIUM The network is connect 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 can be difficult to detect.	HIGH
Application server	Transmitted data scrambling (e.g. high-temperature generators, fault of air conditioning)	LOW The servers are in technical control room	MEDIUM It requires equipments available commercially.	HIGH Since it can affect a large number of servers located in the same area. The monitoring application is compromised	MEDIUM
Application server	HW fault: • Loss of component functionality • Loss of server 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	Alteration of connection due to: • Network overload • Involuntary disconnection	MEDIUM It depends on environmental condition, bandwidth, capacity of connection, number of servers	LOW It depends of network architecture.	HIGH Operation of the server is compromised, as the whole monitoring system.	LOW
Emergency button	HW fault	MEDIUM In general HW and SW are vulnerable, especially after some times, to this fault.	MEDIUM It depends on HW and SW robustness and environmental condition.	MEDIUM Loss of alert functionality	MEDIUM
Emergency button	Physical tamper/manumission such as: • Cable disconnection; • Destruction	LOW	MEDIUM	MEDIUM Loss of alert functionality	MEDIUM
Client operator/video wall	HW fault: • Loss of component functionality • Loss of video functionality SW fault: • Bug • Aging • Transient fault	MEDIUM In general HW and SW are vulnerable, especially after some times, to this fault.	MEDIUM It depends on HW and SW robustness and environmental condition.	MEDIUM Loss of specific functions functionality. It is easy to diagnose	MEDIUM
Client operator/video wall	Alteration of connection due to: • Network overload • Involuntary disconnection	MEDIUM It depends on environmental condition, bandwidth, capacity of connection.	LOW It depends on network architecture.	MEDIUM Loss of specific functions functionality. It is easy to diagnose	MEDIUM
Client operator/video wall	Unauthorized network access • Data disruption/alteration • Loop video	LOW Connection are wired	LOW It depends on attacker ability.	HIGH Difficult to diagnose	MEDIUM
Mobile client (PDA, Smartphone, etc,) or remotely connected client (using Internet)	HW fault: • Loss of component functionality • Loss of client functionality SW fault: • Bug • Aging • Transient fault	MEDIUM In general HW and SW are vulnerable, especially after some times, 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 alert function.	MEDIUM
Mobile client	Alteration of connection due to: • Network overload • Involuntary disconnection	MEDIUM It depends on environmental condition, bandwidth, capacity of connection.	LOW It depends on network architecture.	LOW Loss of alert functionality	LOW
Mobile client	Alteration of connection due to: • Interferences with electromagnetic	MEDIUM The network is connect to the Internet. Using firewalls reduces vulnerability	LOW It depends on network architecture.	LOW Loss of alert functionality	LOW
Mobile client	Unauthorized network access • Data destruction/alteration	MEDIUM The network is connect to the Internet. Using firewalls reduces vulnerability	MEDIUM It depends on hacker ability.	HIGH Difficult to diagnose	HIGH
Network Switch	Physical tamper/manumission such as: • Cable disconnection; • Theft • Other relevant damage meant to put the unit out of order	LOW The switch are in technical control room	LOW	HIGH Loss of communication	MEDIUM
Network Switch	HW fault: • Loss of component functionality	MEDIUM	MEDIUM	HIGH	MEDIUM

	• Loss of switch functionality SW fault: • Bug • Aging • Transient fault	In general HW and SW are vulnerable, especially after some times, to this fault.	It depends on HW and SW robustness and environmental condition.	Loss of communication	
Network Switch	MAC flooding Control of switch	HIGH	MEDIUM Some security means can limit this threat (e.g. Port security.)	HIGH Loss of communication	HIGH
Logical control unit for Anti-intrusion/Access Control via Ethernet	Physical tamper/manumission such as: • Cable disconnection; • Theft • Significant movement or replacement • Other relevant damage meant to put the unit out of order	LOW The Control Units are in technical control room	MEDIUM	HIGH Loss of functionality	MEDIUM
Logical control unit for Anti-intrusion/Access Control via Ethernet	HW fault: • Loss of component functionality • Loss of camera functionality SW fault: • Bug • Aging • Transient fault	MEDIUM In general HW and SW are vulnerable, especially after some times, to this fault.	MEDIUM It depends on HW and SW robustness and environmental condition.	HIGH Effects range from loss of specific functions to loss of related monitoring functionality.	HIGH
Logical control unit for Anti-intrusion/Access Control via Ethernet	Alteration of connection due to: • Network overload • Involuntary disconnection	MEDIUM It depends on environmental condition, bandwidth, capacity of connection.	LOW It depends on network architecture.	HIGH Loss of functionality	MEDIUM