# Use Cases for the nSHIELD demonstrator

Starting from the description of the railway security case-study (see file: ASTS_Case_Study.pdf, at link: http://nshield.unik.no/wiki/WP7), in this document we provide some use case proposals to be discussed for possible demonstrations.

### Scenario n. 1

In order to ease comprehension, the attention can be focused on a subset of entire architecture previous described. In particular the connection between cameras and server, showed in the figure 1 the components are described following.

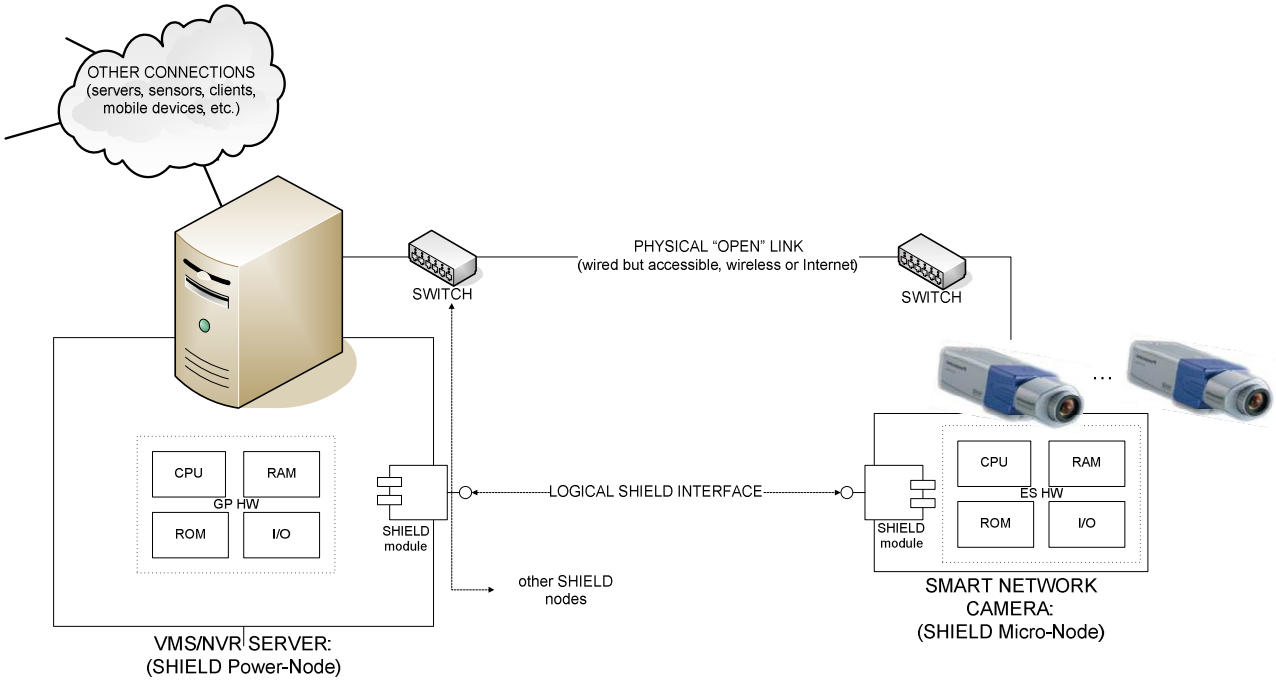


**Figure 1 Scenario 1**

VMS/NVR SERVER - Can be supposed as **SHIELD Power Node.**
The main features are:

- General purpose Commercial-Off -The-Shelf computer
- Win or Linux OS
- Good performance and storage
- Typically installed in access controlled technical rooms
- Typically working in controlled environmental conditions

The main threats are:

- STOP PROCESSING OR DAMAGE DATA
    - random or malicious

    - primary impact on availability
- ACCESS TO PC AND READ DATA
    - Malicious
    - primary impact on privacy
- ACCESS TO PC AND WRITE DATA
    - Malicious
    - primary impact on security

SMART NETWORK CAMERA - Can be supposed as **SHIELD Micro Node.**
The main features are:

- Embedded system
- Proprietary OS, TinyOS or similar
- Low performance and storage
- Possibly installed in public areas
- Possibly exposed to hard environmental conditions

The main threats are:

- STOP PROCESSING OR DAMAGE DATA
    - random or malicious
    - primary impact on availability
- ACCESS TO ES AND READ DATA
    - Malicious
    - primary impact on privacy
- ACCESS TO ES AND WRITE DATA
    - Malicious
    - primary impact on security

THE PHYSICAL OPEN LINK - can be wired or wireless.

The main threats are:

- STOP, SCRAMBLE OR CORRUPT DATA FLOW
    - random or malicious
    - primary impact on availability
- READ DATA FLOW
    - Malicious
    - primary impact on privacy
- WRITE IN DATA FLOW
    - Malicious
    - primary impact on security

THE LOGICAL SHIELD INTEFACE - should be able to exchange data among nodes related to:

- DISCOVER/PUBLISH/SUBSCRIBE SHIELD SERVICES
- DIAGNOSE/NOTIFY NODE FAILURES
- SET/NOTIFY ENCRYPTION MODE AND KEY SIZE
- SET/NOTIFY CHECKSUM MODE AND SIZE
- SET/NOTIFY MTBF & MTTR PARAMETERS
- SET/NOTIFY MAX TIME DELAY
- SET/NOTIFY REDUNDANCY MODE
- SET/NOTIFY RECONFIGURATION STRATEGY

**Use Case**

1. Central operator requests to record video stream from one camera with specified **SPD=(AVAILABILITY=HIGH, PRIVACY=VERY HIGH, DELAY=VERY LOW, …)**

2. **SHIELD** translates those high-level (qualitative) SPD REQS into low-level (QUANTITATIVE) **SPD METRICS** using ontology models

3. **SHIELD** verifies if devices available can fulfil the required SPD
    a. If NOT, a notification is sent and USER can choose to relax SPD REQS
    b. If YES without reconfiguration, the requested service is provided
    c. If YES with reconfiguration, the reconfiguration strategy is propagated to the nodes to increase cryptography (KEY LENGTH), redundancy (MORE NETWORK LINKS), ETC.
4. After a while, a redundant network links fails during operation
5. Adjacent nodes detect the failure and notify it to the higher level nodes
6. USER is notified of the decrease in SPD that does not allow to fulfil initial requirements, and/or the service is automatically interrupted.

**Scenario n. 2**

Let us assume a camera is used to monitor the main entrance of a shelter (building for housing electrical and electronic high-tech telecommunications, and control systems for railways; see Figure 2) linked via WAN to a video-wall in a central control room. In order to improve reliability, two cameras (CAM A and CAM B) are installed for redundancy in a cluster-like architecture, with identical position and SPD characteristics.

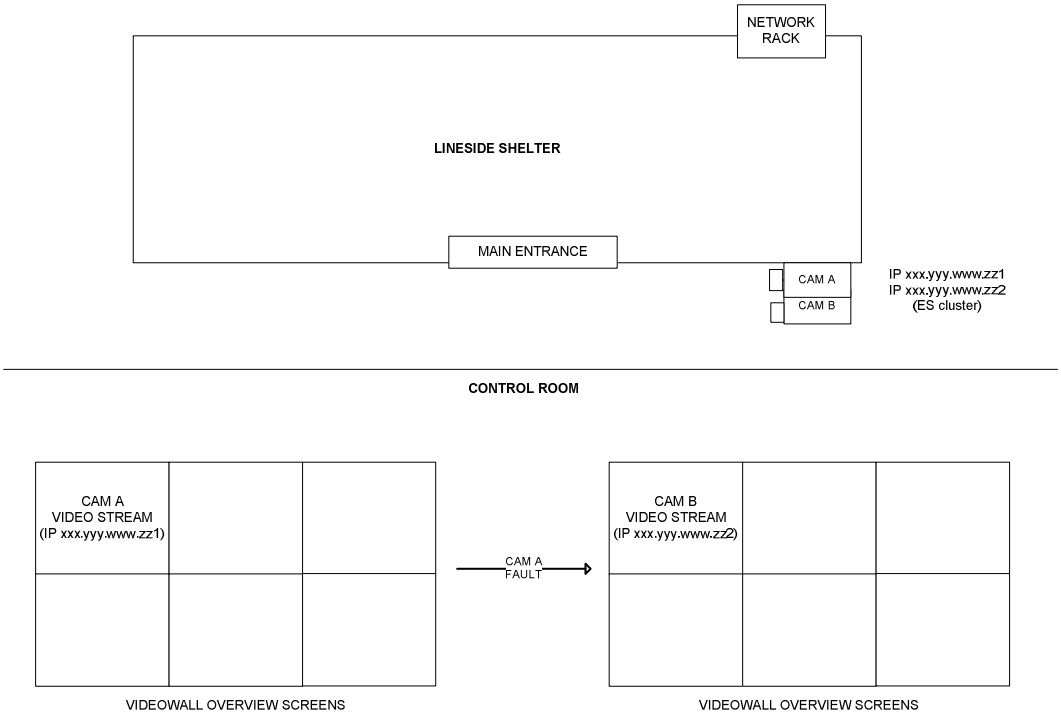


**Figure 2 Shelter video-surveillance from control room.**

Use Case

1. CAM A works properly.
   **SHIELD set SPD_level=X**
2. Cam A fails
3. SHIELD allows to automatically detect the failure and reconfigure the system such that
   **a.** Cam B replaces Cam A in a transparent manner (e.g. the IP to which the box on the videowall points changes so quickly that the user hardly realizes).
   **b.** System dependability level decreases, **Dependability_level=X-delta**

   Note: if CAM B fails while CAM A is still working, no reconfiguration happens but administrator is notified of the decrease in the dependability level.

## Scenario n. 3

This scenario regards video surveillance from a control room of a vehicle (e.g. light metro, tram) moving in a urban area (Figure 3).
The link between vehicle and control room is wireless and the exchanged information are:

- Vehicle to control room:
  - On-board diagnostics and alarms generated by emergency buttons, environmental sensors and video analytics running on the on-board NVR (Network Video Recorder)
  - GPS information for localization (periodic, on request or on event)
  - Event activated real-time video streaming (at adaptable quality, resolution and frame-rate depending on available bandwidth) from on-board cameras
  - User-requested video recordings from on-board NVR

- Control room to vehicle
  - Configuration change commands
  - Requests for information (position, video streams, downloads of recording, device status report, etc.)

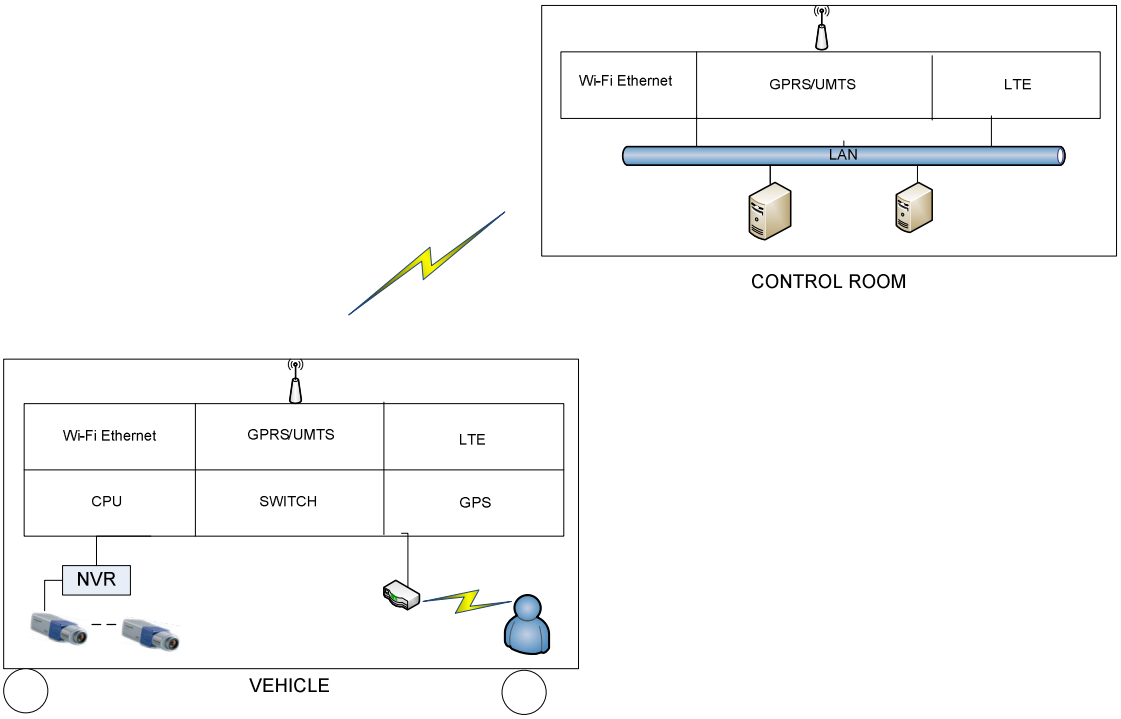


**Figure 3. On-board surveillance (scenario 3)**

This scenario needs adaptivity to different wireless network connections (Wi-Fi, GSM/GPRS, UMTS, etc.) and signal conditions as the vehicle moves through the city, since no fixed infrastructure with assured QoS is assumed. Furthermore, there will be wired connections in the depot for daily downloading of log-files and recordings (for back-up or long term video archiving). Different technologies and configuration/encryption options (WEP, WPA, etc.) will obviously feature different SPD requirements.
In such a scenario SHIELD would reconfigure SPD properties depending on locations (depot, tunnel, etc.) and other measured parameters (network connection, estimated bandwidth and S/N ratio) considering that public networks (mobile or wireless) do not assure QoS or SPD. Of course the intra-vehicle (wired) network connecting on-board devices is dedicated and segregated, therefore featuring potentially higher and controllable QoS and SPD.