Why is it important to work on the (network) lower layers in cybersecurity?

Christophe Gransart / Virginie Deniau

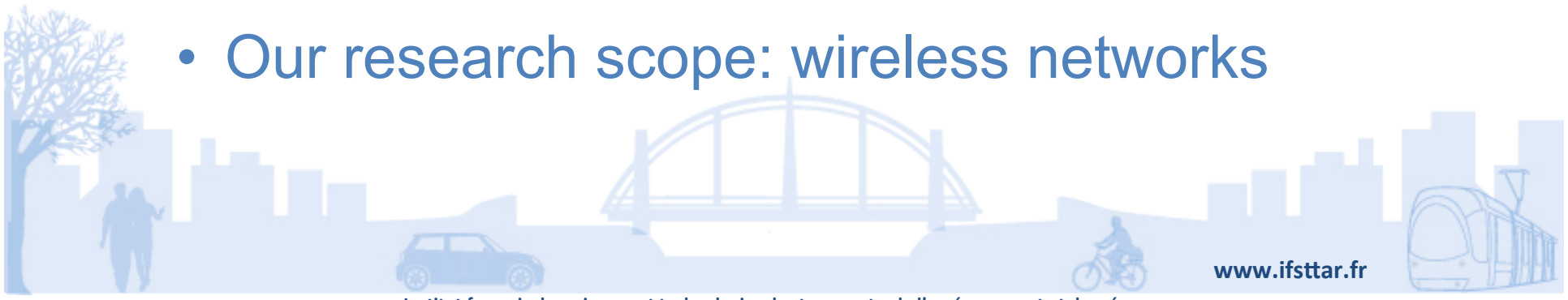
christophe.gransart@ifsttar.fr

virginie.deniau@ifsttar.fr

IFSTTAR

Monitoring Critical Infrastructures

- Why is it important?
  - After the security analysis, mitigations can not be applied everywhere (threat dependent …)
  - To reduce the risk, monitoring is an answer to the threat detection problem
  - Our research scope: wireless networks

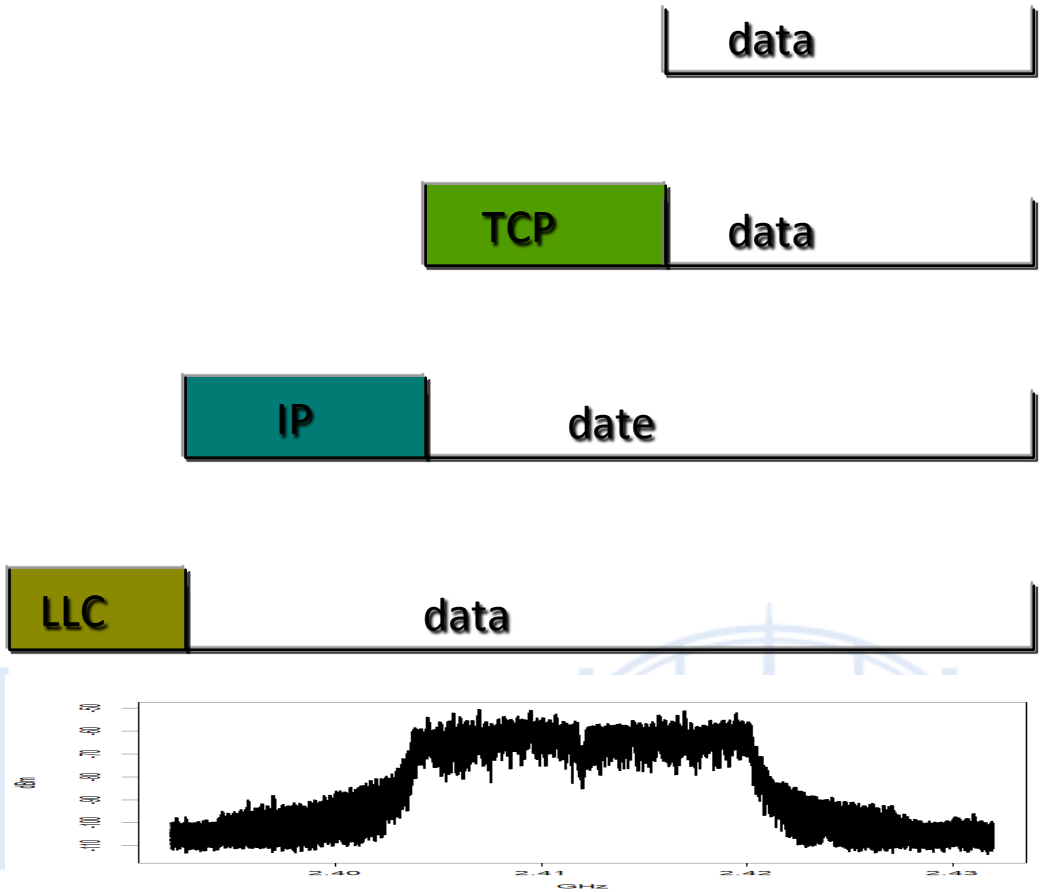


SIEM and IDS

- SIEM
  - Security Information Management System
  - Log management and correlation between events
- IDS
  - (Network based) Intrusion Detection System
  - Analyze the network traffic

Stateful Packet Inspection

- Only headers are analyzed



L7: APP (content)

L4: TRANSPORT (ports)

L3: NETWORK (@IP)

L2: DATA LINK (frames)

L1: PHYSICAL (spectra)

Deep Packet Inspection

- Principle
  - All the content is analysed (even the data (L7))
- Drawback
  - Time consuming
  - traffic slower
- Privacy problem
  - Big brother is watching you!

Working at low level

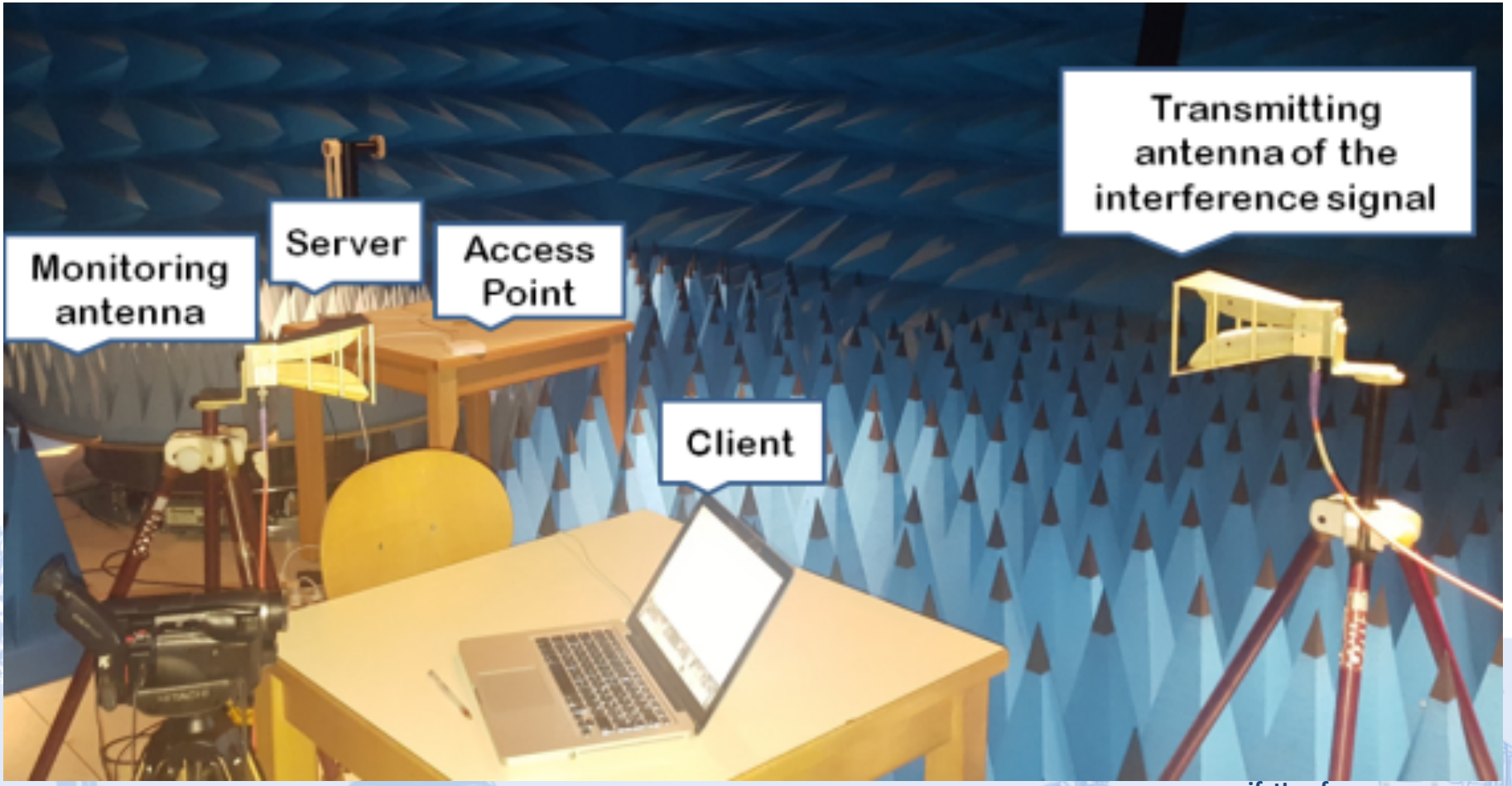
- Research work at
  - Physical level (L1)
  - Data link level (L2)

- Example:
  - Work on OFDM wave form
  - Could be applied on LTE, 802.11n, …

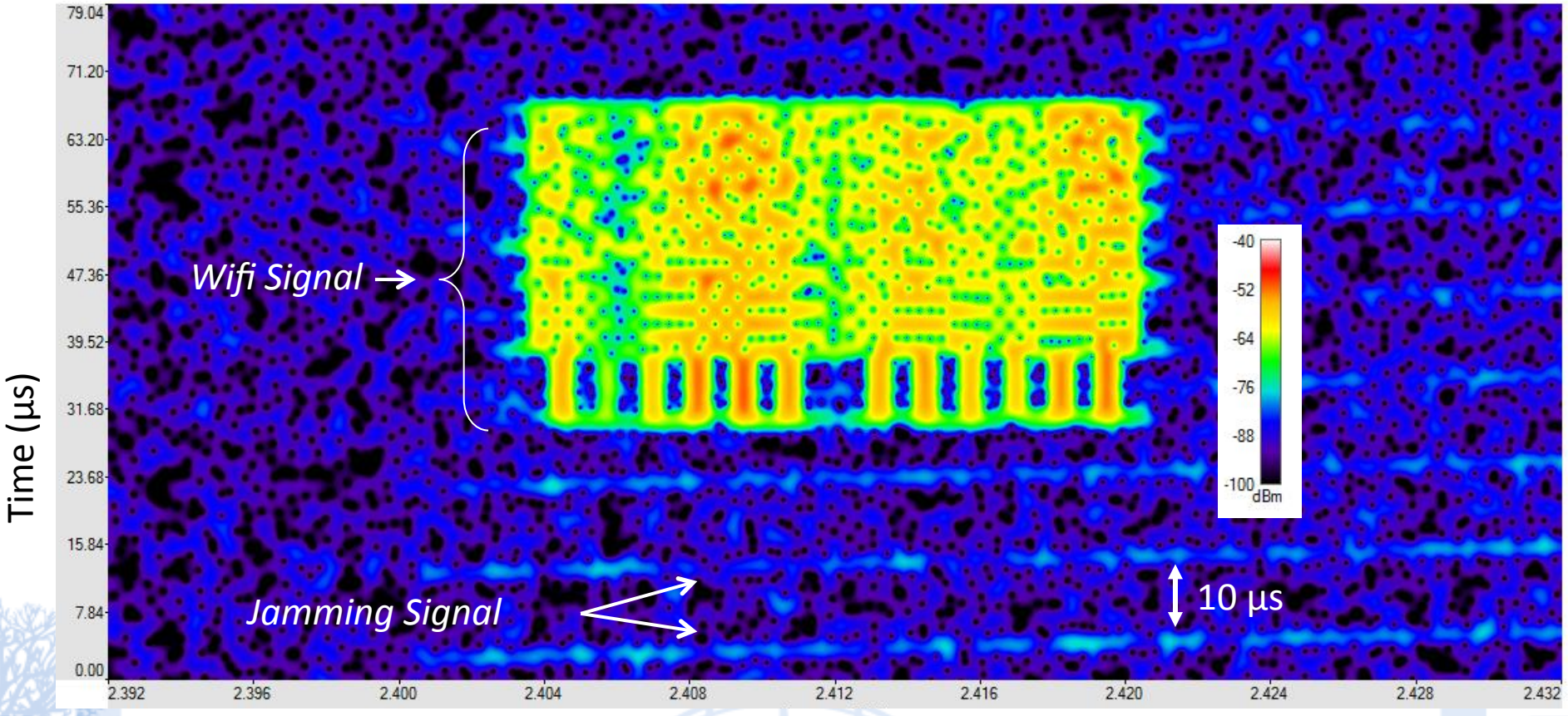
Examples of threats at low level

- Monitoring lowest levels could detect
  - Jammer
  - Fake access point / eNodeB
  - Attacks on IoT with low level of traffic

Monitoring system example (at L1)

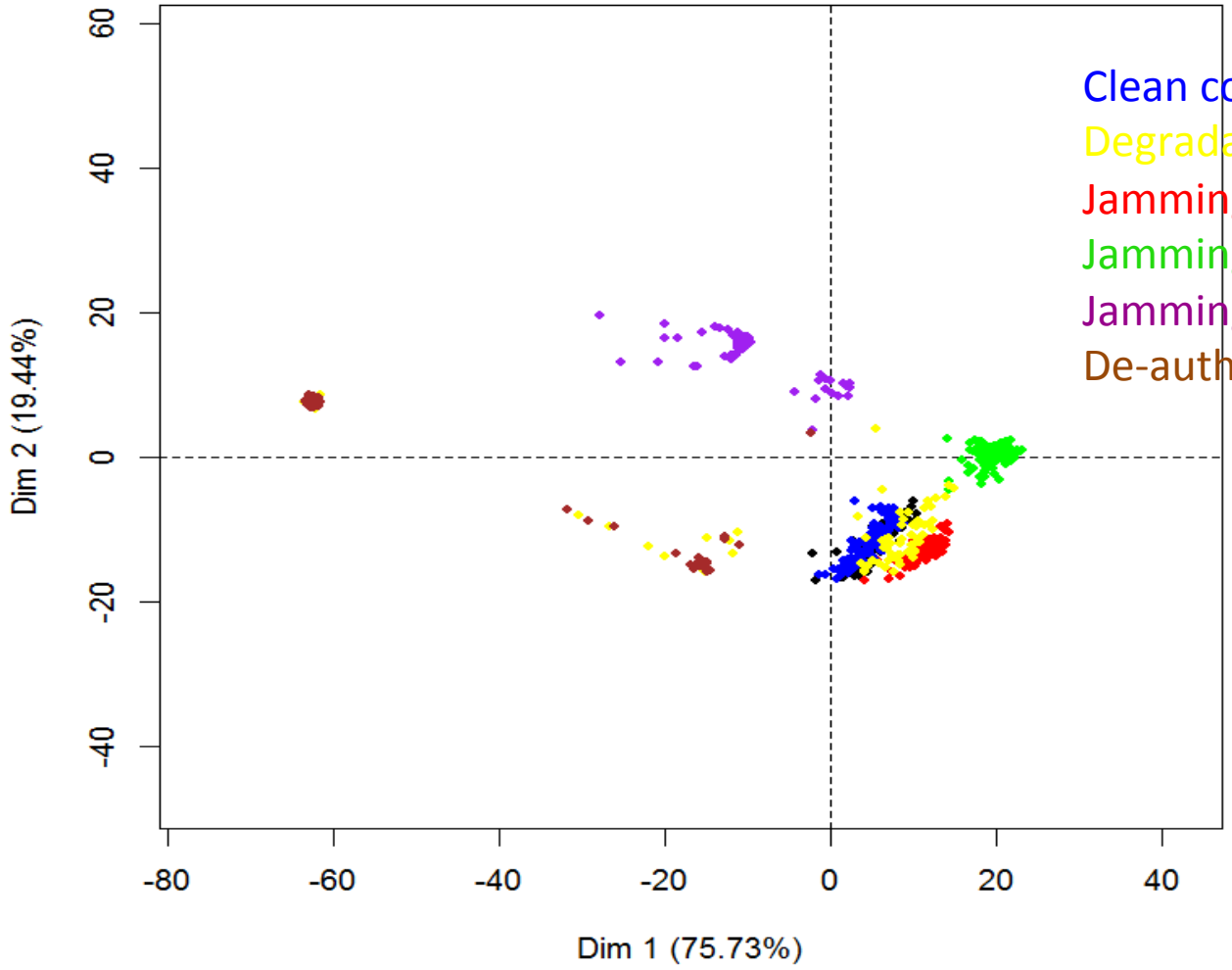


OFDM signal analysis



Deep Signal Inspection?

- Monitoring and classification

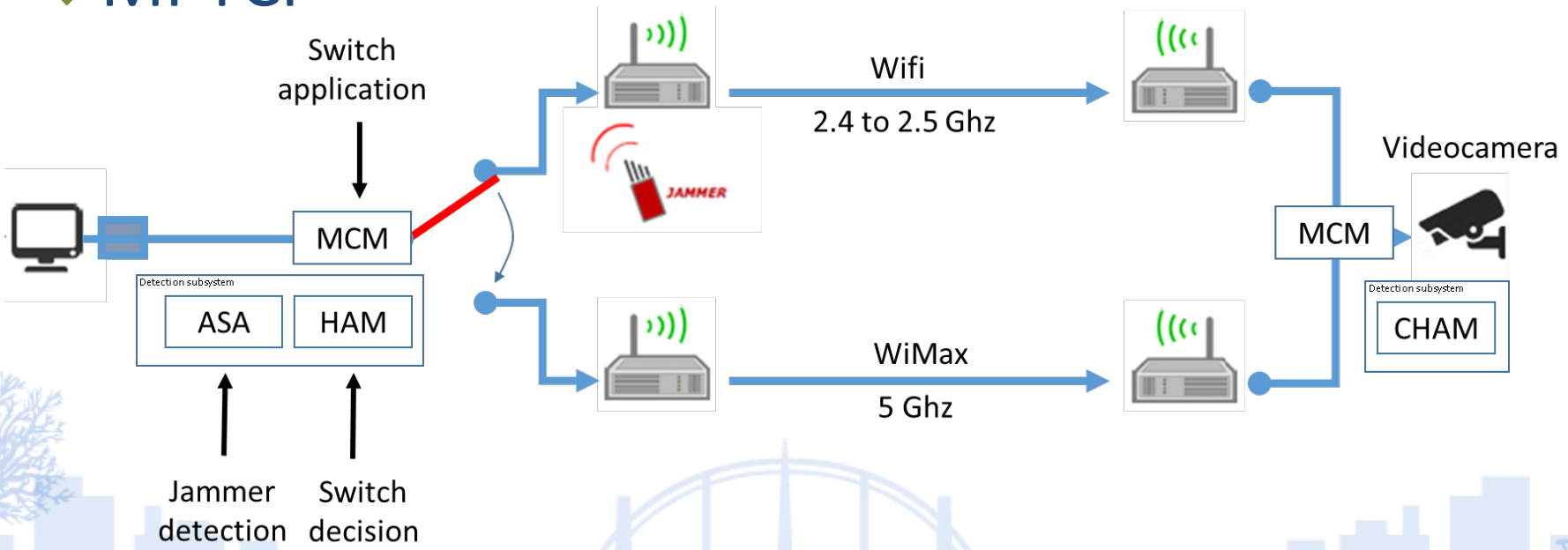


Clean communication
Degradation of propagation conditions
Jamming without impact on the quality
Jamming with low impact
Jamming with communication lost
De-authentification

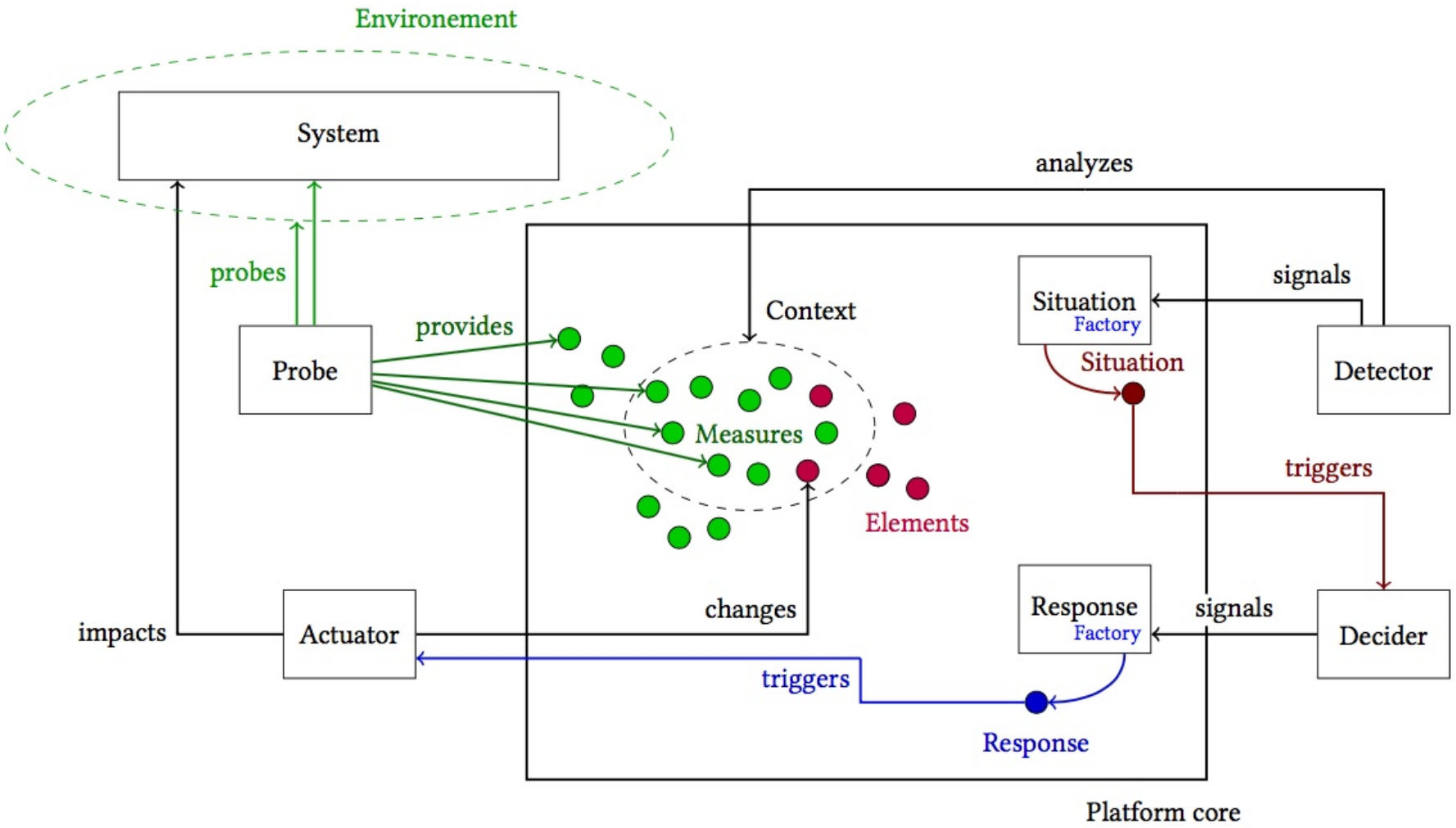
Joint research between IFSTTAR, IEMN, IMT, Railenium

Case n°1: monitoring functions in parallel of the network to protect

- IP-Based MCS
- MPTCP



Case n°2: architecture of the network to protect including the monitoring



Conclusion

- Monitoring network low level layers of critical infrastructures is complementary to high level monitoring

- Based on
  - Physical signals
  - Machine learning and classification