IoT Security challenges in vertical sectors: 
Smart Cities
Cybersecurity for a connected world – Why is important

despite the strong offer of IoT products and solutions
specific standards or regulations still under development and
only accredited bodies have the knowledge

and experience to support the market by proposing
certification framework based on meta-schemes...
Cybersecurity for a connected world – The scenario

Modern buildings promise **comfort** and **safety** by using IoT connected devices and domotic systems...

But are IoT systems secure?

Definitely NO, cybersecurity threats could lead to serious incidents...

And shocking consequences for the safety...
Cybersecurity for a connected world – The answer

what you should do to secure your domotic systems is identify the vulnerabilities by performing security audits and penetration testings

...cybersecurity threats could be addressed to drastically reduce the risks of incidents and improve your safety!
Cybersecurity for a connected world – How to do it

Security auditing

- **Penetration testing** and **vulnerability analysis**, including:
  - White box/Black box evaluations, including **source code reviews**.
  - **Logical** (software) and **physical** (hardware) **attacks**, including all the available **communication networks**, both wired and wireless.
  - Both standalone products and integrated product suites, ranging several products.
  - Internal development tools review and auditing.

- **Prototype reviewing** and feedback
  - A robust design will be more resilient
Cybersecurity for a connected world – The IoT Lab

Our proposal

The Applus+ IoT Lab will allow manufacturers and developers to verify the reliability and security of their IoT solutions and provide end users with a quality guarantee by means of the IoT Certified mark.
Cybersecurity for a connected world – The IoT Lab

IoT Certified Mark (labeling)

- Within the IoT Lab, the technology evaluators will propose a testing program adapted to each project’s requirements to ensure the regulatory compliance and IoT Functional testing of the different products and devices of the IoT solution.
- After completing the testing program, manufacturers will be able to access the IoT Certified voluntary certification mark, which provides end-clients technical guarantees as to the quality of the IoT solution.
- Based on internally defined meta-schemes, Cybersecurity labeling will be product-oriented in order to grant the costs of the certification is suitable for different customer profiles.
IoT Security challenges in vertical sectors

thanks...