Connecting Trustable Things

Maghsoud Morshedi

EyeNetworks

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

Why we Need Trustable Things?

- Gartner, Inc. forecasts 20.4 billion connected things by 2020
- According to BullGaurd, 375 million devices were potentially vulnerable in 2017, which will grow to more than 900 million by 2020.
- According to F5, IoT attacks increased 280% in 2017 over period of July 1 through December 31, 2016, which Mirai attack happened.

What is SCOTT?

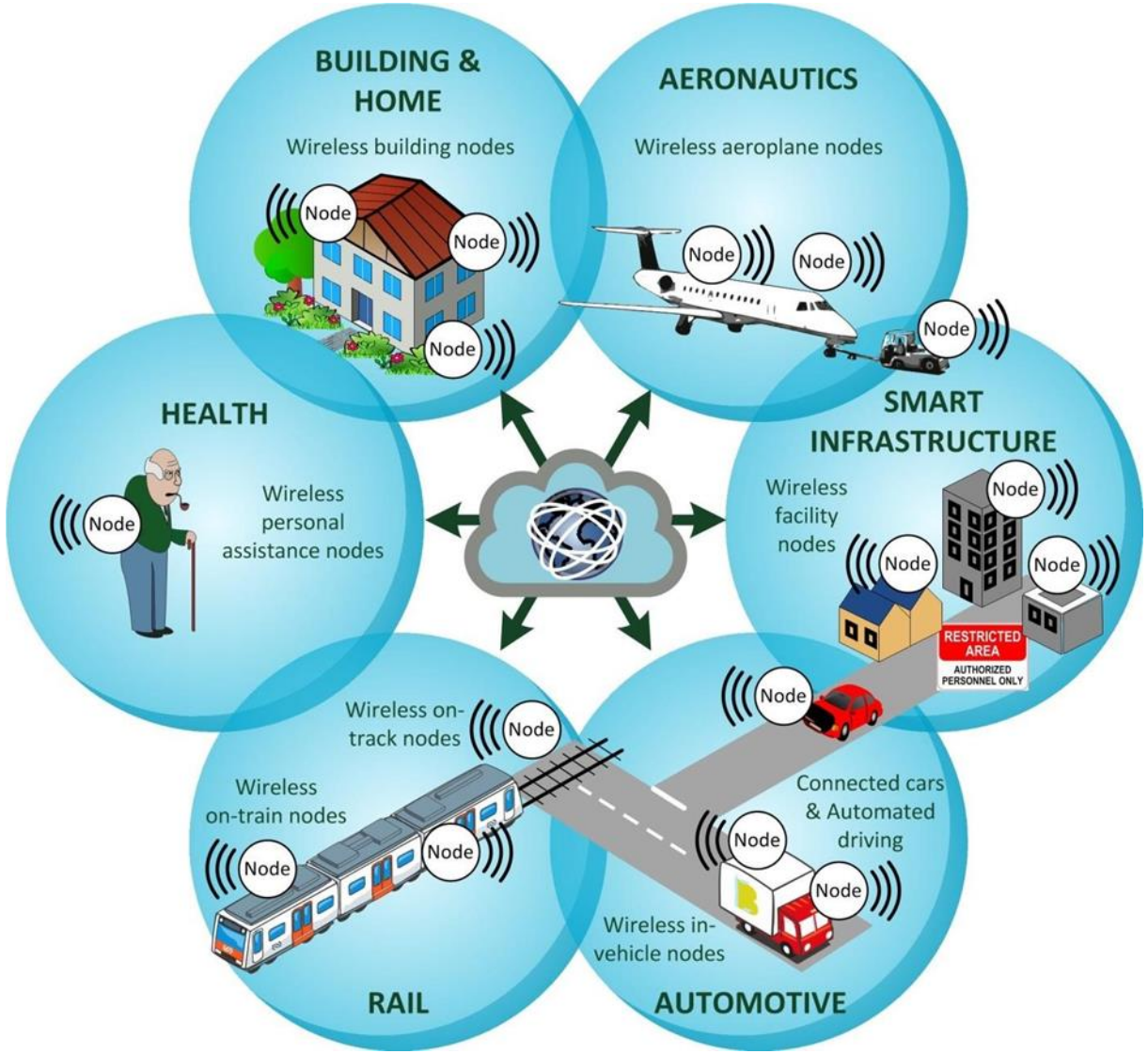
- SCOTT is an European project with 57 partners from 12 countries
- Create trust in wireless solutions
- Increase social acceptance of wireless products
- Enhance efficiency in secure wireless products
- Achieve full potential of Internet of Thing (IoT)
- Consists of 15 industrial use cases

What are the goals of SCOTT?

- Enhance security, privacy, trustability and safety of wireless solutions
  - Trust framework
  - Privacy labeling
  - Security classes
  - Link between security and safety
- Improve interoperability of wireless solutions

Various Domains

- Aeronautics
- Automotive
- Building and home
- Health
- Rail
- Smart infrastructure

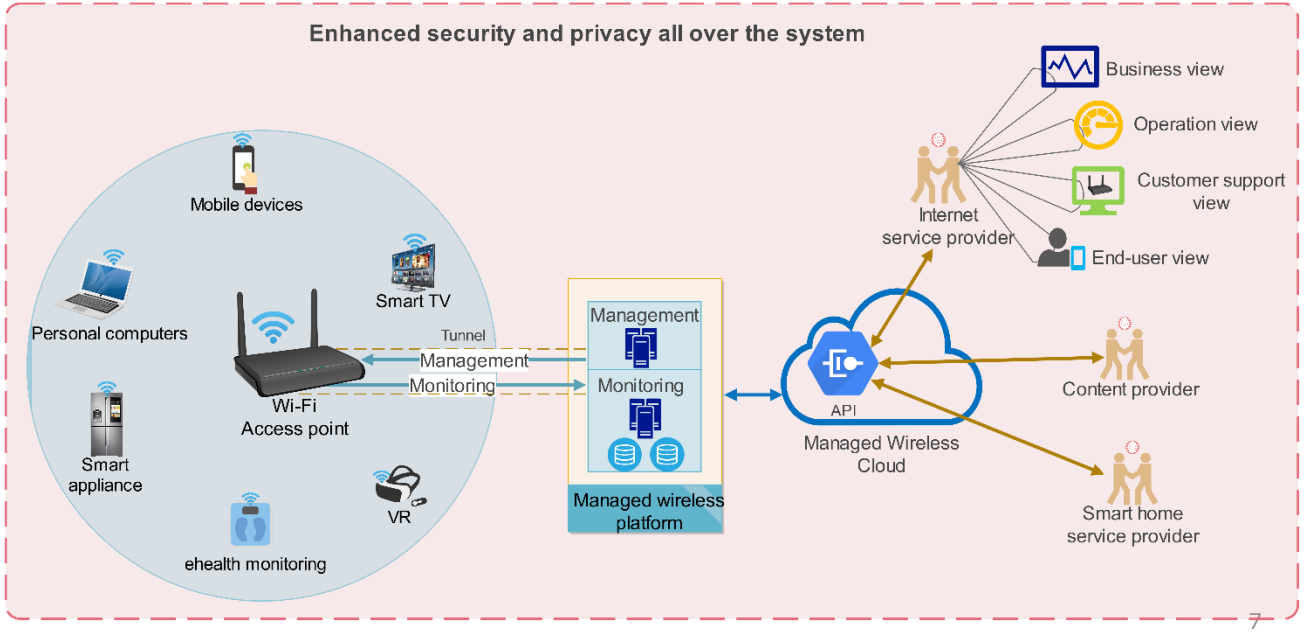


EyeNetworks Contribution in the SCOTT

- Develop concept of managed wireless for smart infrastructure use case
- Collaboration in in-vehicle wireless communication use case
- Collaboration in industrial facility management with secured wireless devices use case
- Collaboration in building trust framework for wireless remote management

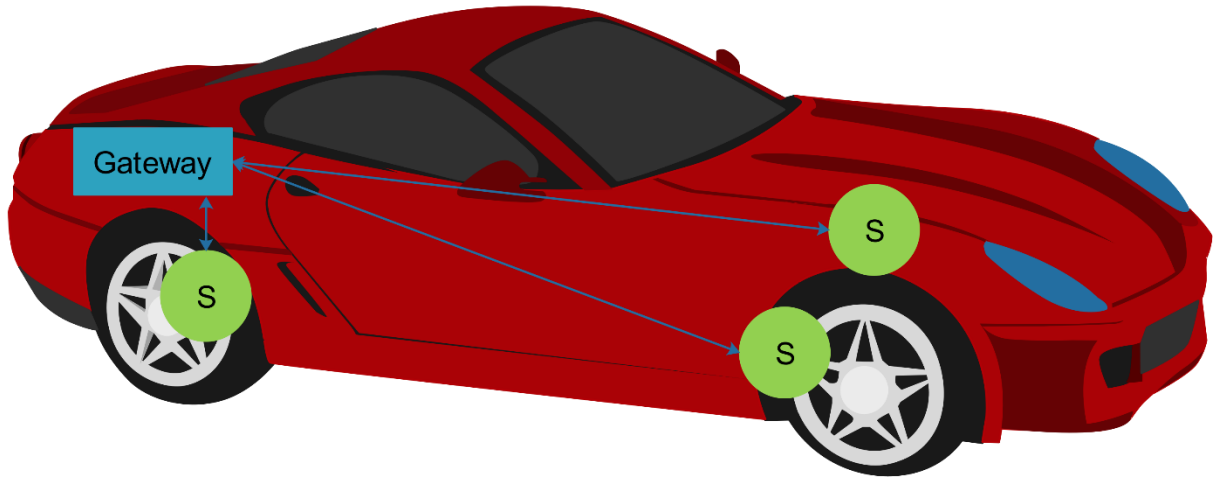
Managed Wireless for Smart Infrastructure Use Case

- Open standard protocol remote management
- Standardization of remote managament
- Improve interoperability of wireless products
- Enhance security and privacy of Remote configuration
  - Assess trust issues and vulnerabilites
  - Privacy labelling
  - Measurable security



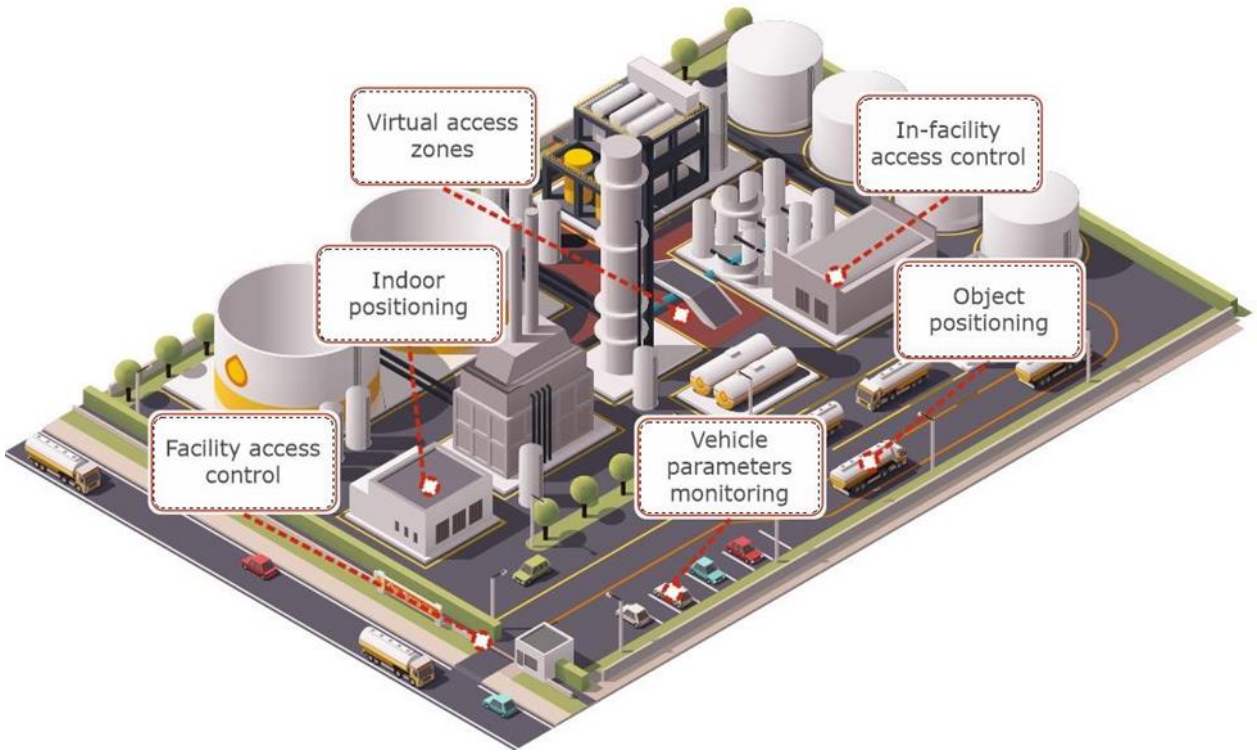
In-Vehicle Wireless Communication

- Connect and pair wireless sensors for in-vehicles measurements
- Trustable pairing of sensors
- Interconnect in-vehicle wireless communication with smart infrastructure



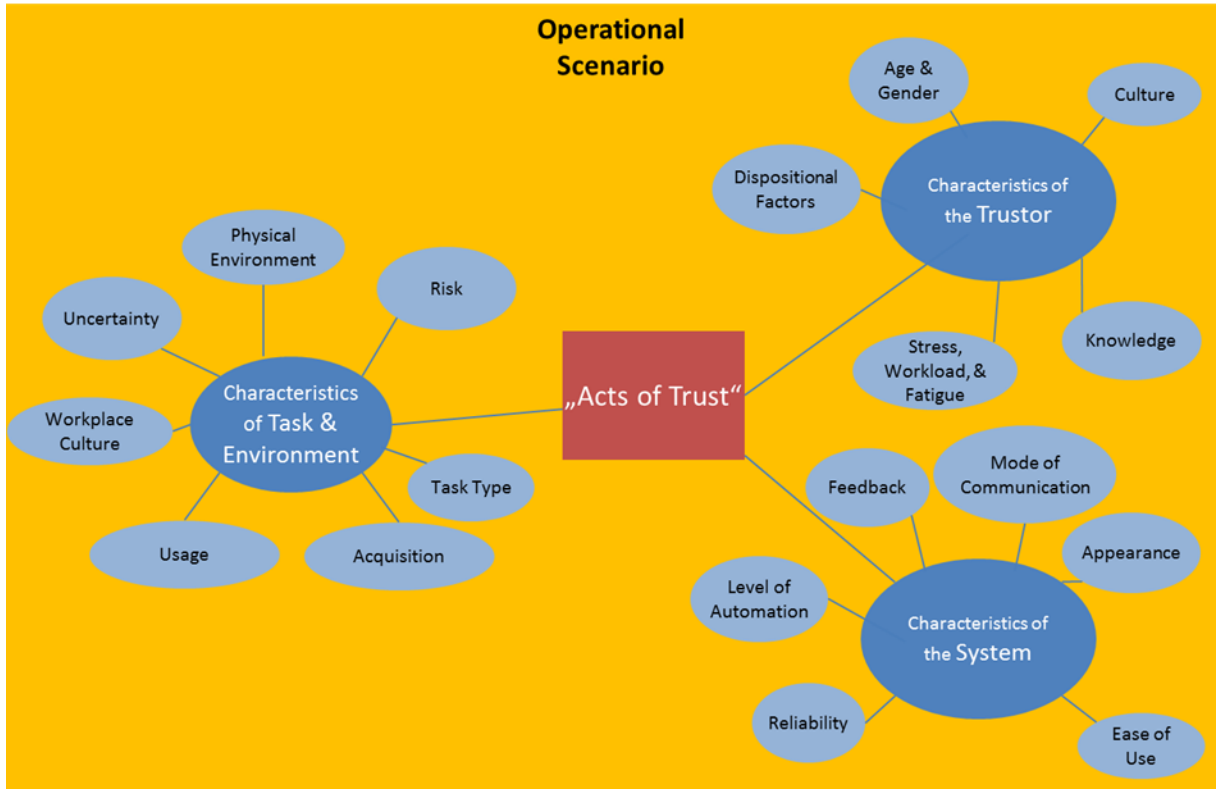
Industrial Facility Management

- Enhance security and safety of industrial facilities with wireless solutions
- Provide mobile authentication and authorization
- Utilize wireless components for critical infrastructure
- Remote monitoring and management of wireless components
- Provide trustable wireless infrastructure



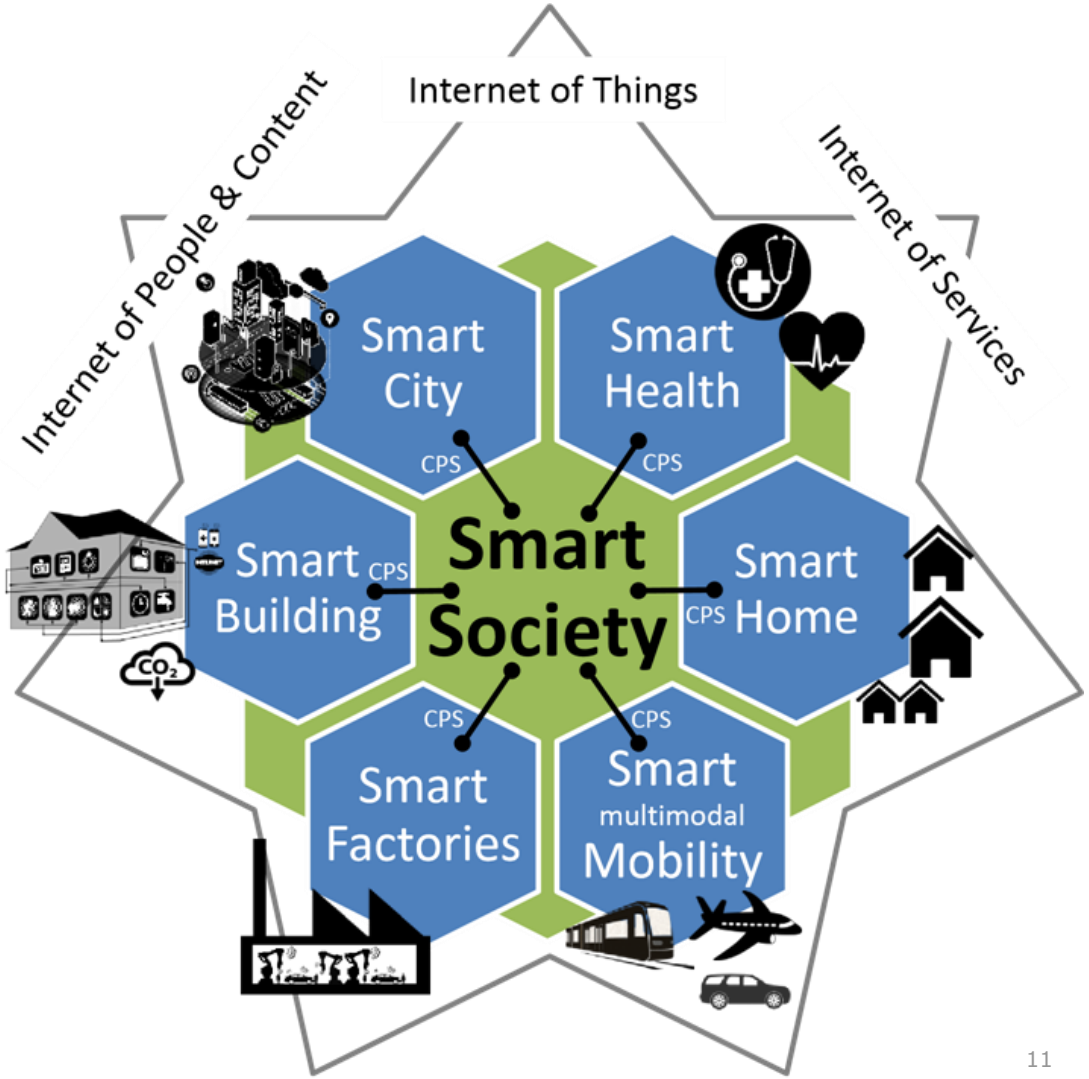
Trust Framework for Wireless Remote Management

- Identify trust issues and vulnerabilities
- Identify trust requirements
- Identify environmental effect on user trust
- Facilitate trust formation by design



Why Should we Care?

- Everything is going to be connected
- We need secured and private interactions
- We need trustable wireless communication
- Prepare our remote configuration solutions for upcoming services and applications



Questions?

mmc@eyenetworks.no

www.scott-project.eu

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

SECURITY

USABILITY

TRUSTABILITY

PRIVACY

SAFETY

www.scott-project.eu

ECSEL Joint Undertaking

SCOTT

Secure Connected Trustable Things

www.scott-project.eu