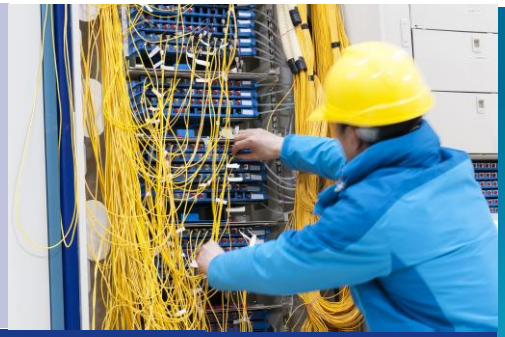


Enhancing infrastructure cybersecurity in Europe

Rossella Mattioli
Secure Infrastructures and Services

European Union Agency for Network and Information Security

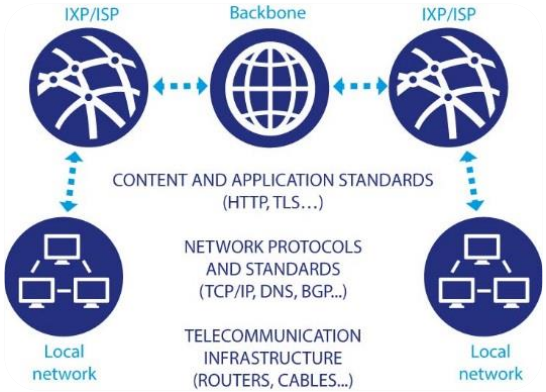
Securing Europe's Information society

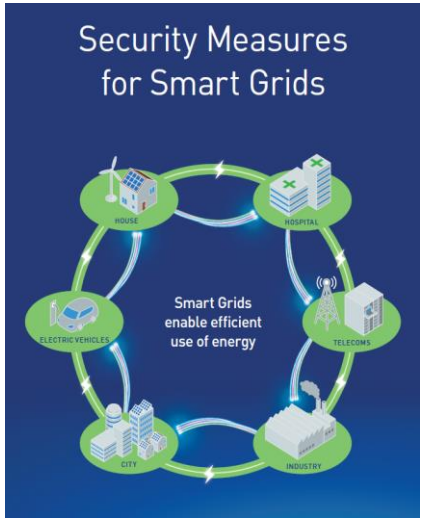
Positioning ENISA activities

https://www.enisa.europa.eu/topics

Secure Infrastructure and Services

Communication networks: Critical Information Infrastructure and Internet Infrastructure



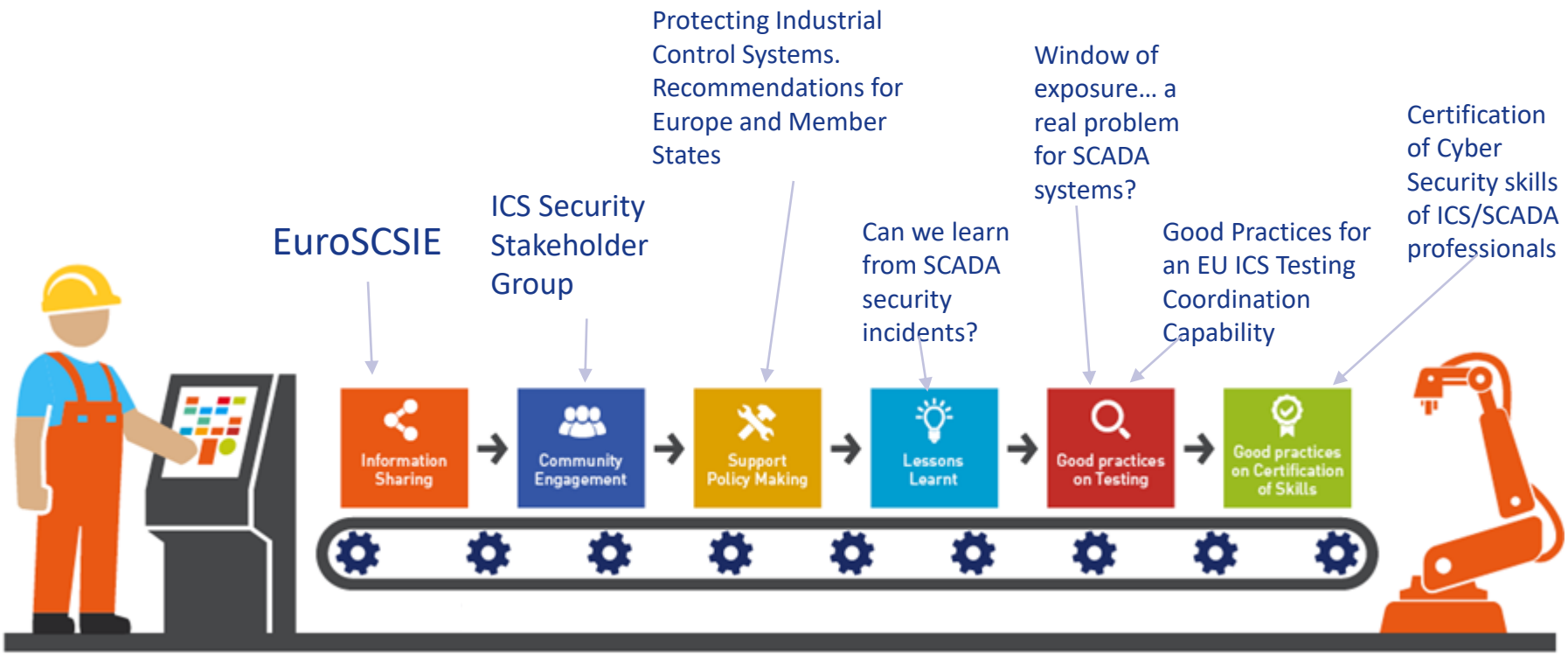


Transport

eHealth and Smart Hospitals

Finance

Cybersecurity for ICS SCADA



https://www.enisa.europa.eu/scada

2015 efforts

Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors

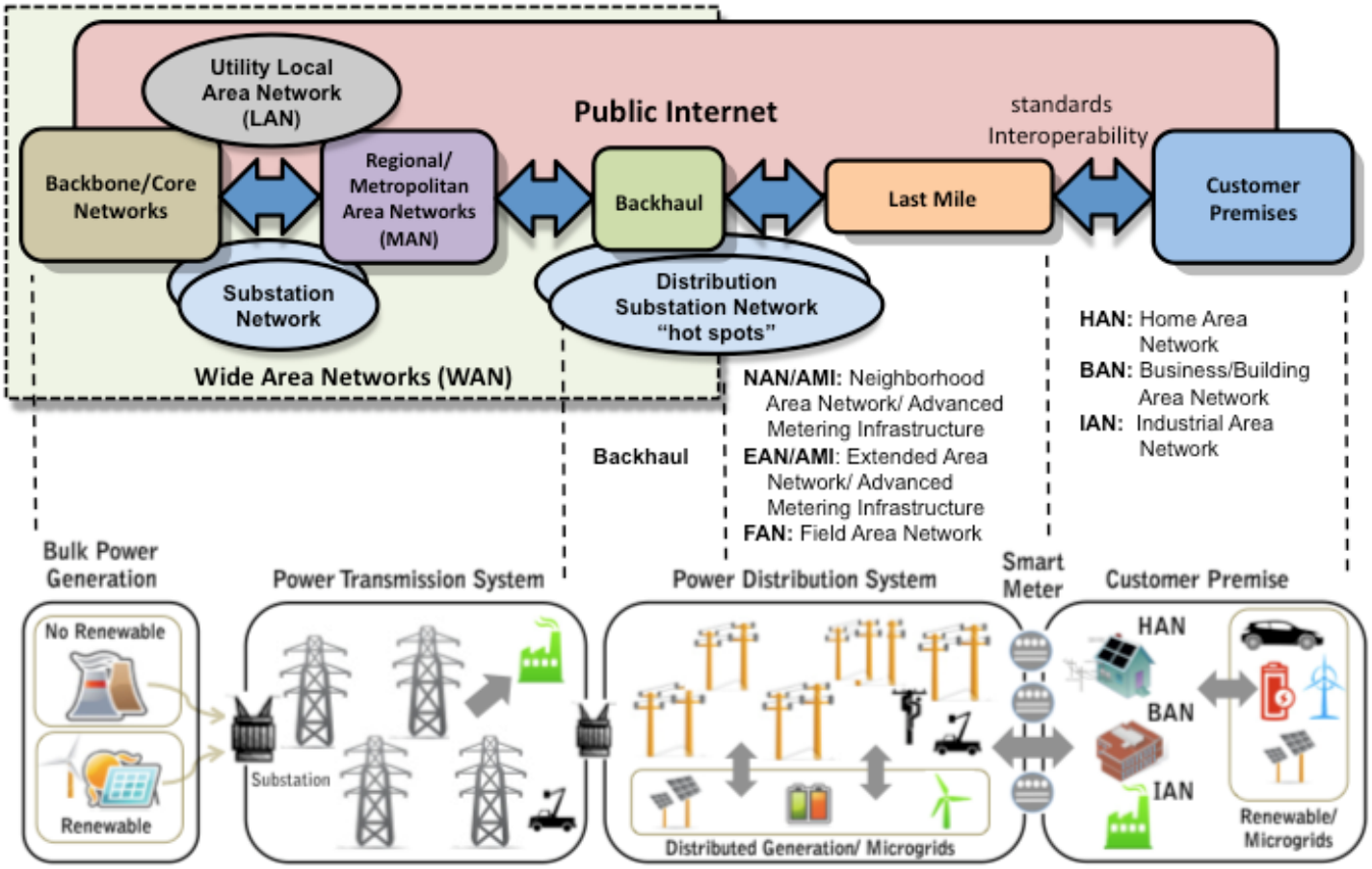
Leading - Member States with a strong legislation and supporting mechanisms dedicated to ICS SCADA cyber security improvement

Reactive Supporters - Member States focus on lessons learned and reactive means of improving ICS SCADA cyber security

Proactive Supporters - Member States focused on strong CI operators support and driving the ICS SCADA cyber security improvement

Early Developers - Member States in the process of developing of legislation and supporting system to protect ICS SCADA in Critical Infrastructure

Communication networks dependencies in smart grids



https://www.enisa.europa.eu/smartgrids

Communication networks dependencies in smart grids

Vulnerable consumers

Massive number of devices

Coexistence of old and new machines

Implicit trust M2M by default

Internet Protocol (IP) dependencies

Commercial hardware and software

Communications protocols vulns

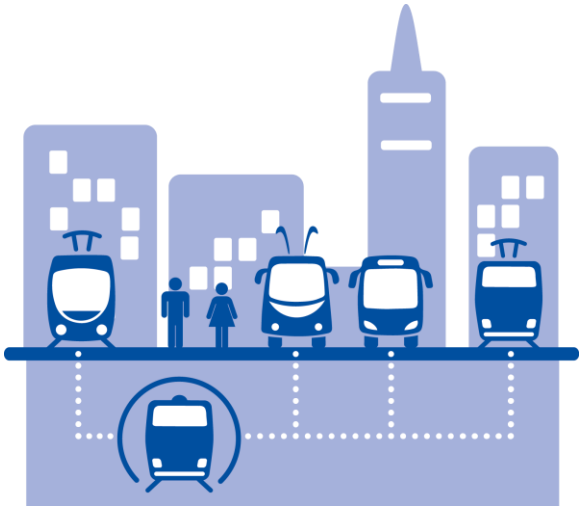
Human factors

- Attacks
- Good practices
- Recommendations for
  - European smart grid operators and relevant authorities
  - Manufacturers and vendors
  - European Commission

https://www.enisa.europa.eu/smartgrids

2016 efforts

2016 efforts on infrastructure security



Ongoing projects in the area of ICS SCADA and smart infrastructure:

- Communication network dependencies on ICS SCADA
- Security requirements for electricity power supply operators
- Smart cars
- Smart hospitals
- Smart airports

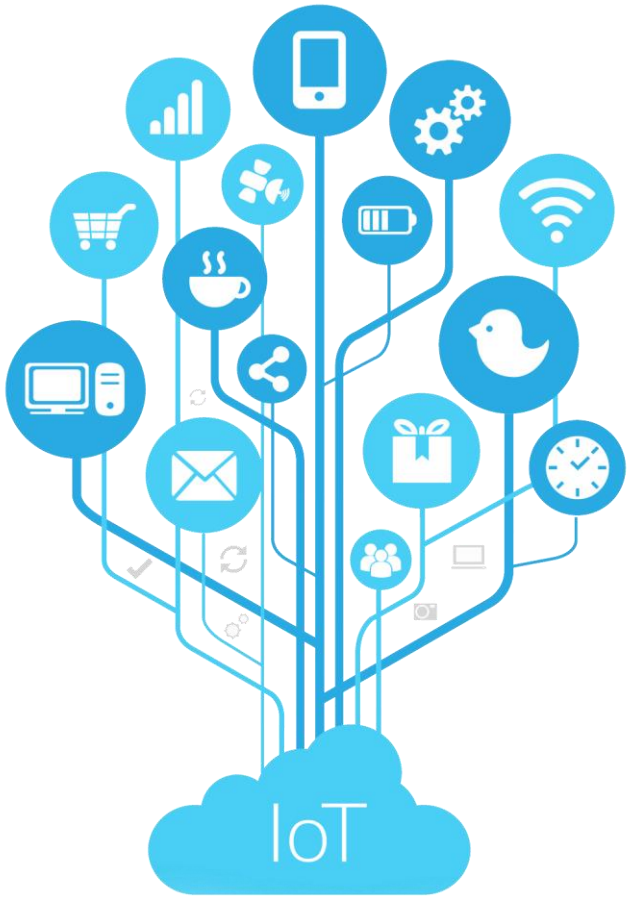
Communication network dependencies for ICS SCADA

- Energy (except smart grids - covered in 2015 study)
- Oil
- Gas
- Transport
- Health sector
- Drinking water supply and distribution
- Manufacturing
- Chemical
- Pharmaceutical

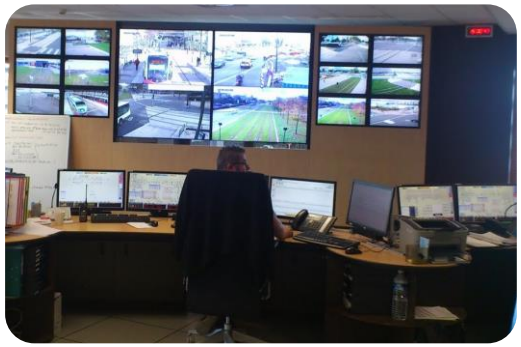
Communication network dependencies for ICS SCADA

- *Outlined scope and perimeter with EICS SG and EUROSCSIE experts*
- Map assets and threats via desktop research and interviews with security researchers and asset owners
- List all possible attacks coming from network exposure
- Examine protocols vulnerabilities
- List good practices
- Develop 3 attack PoCs and mitigation actions
- Define recommendations for
  - Infrastructure operators
  - Vendors
  - EU Member States
  - European Commission

Securing Smart cities and transport infrastructure



Smart Cities as a “system of systems”



New and emerging risks

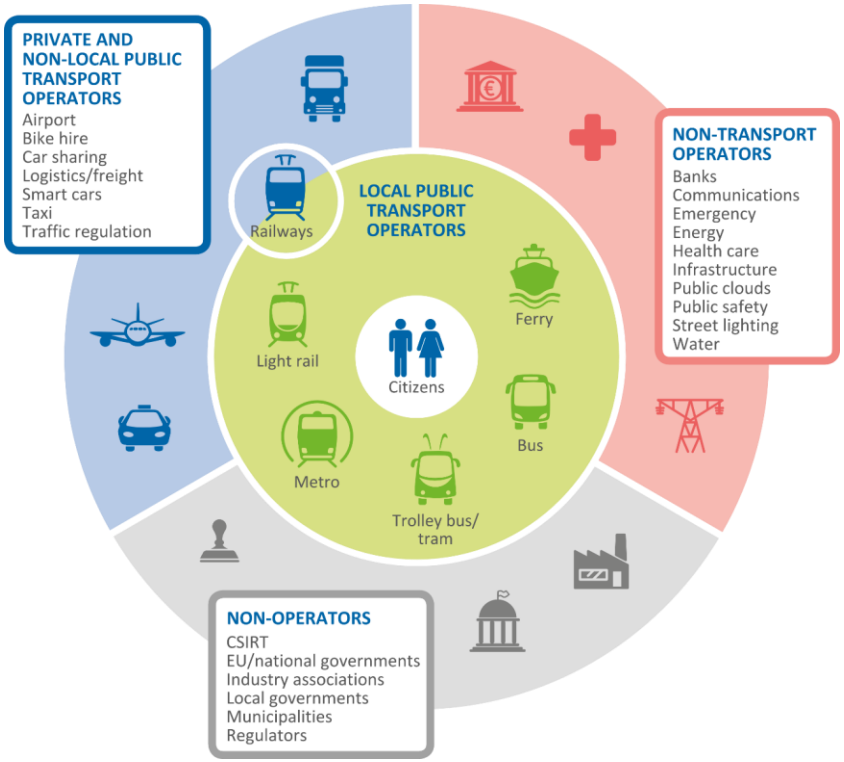
- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (legacy) systems
- Data exchange integrated into business processes

Threats with consequences on the society

- Economical consequences, but not only
- Smart Infrastructures’ operators’ are not security experts
- Lack of clarity on the concept of “cyber security”

Cyber security measures are not only technical but also operational and organisational

Securing transport infrastructure



2015 studies

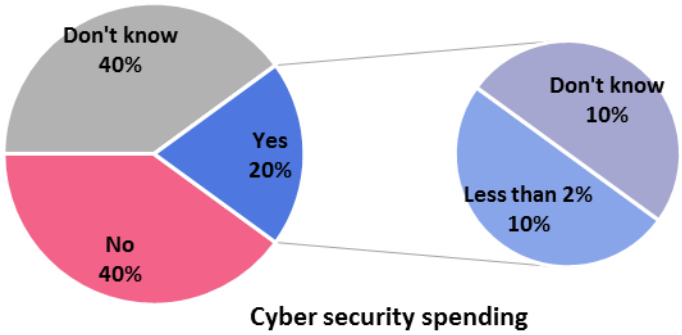
- **Architecture model of the transport sector in Smart Cities**
- **Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations**

Objectives

- Assist IPT operators in their risk assessment
- Raise awareness to municipalities and policy makers
- Invite manufacturers and solution vendors to focus on security

https://www.enisa.europa.eu/smartinfra

Cybersecurity for Intelligent Public Transport



Existing status of security for IPT is limited

- Safety does not integrate security
- Security is not well integrated in organisations
- Awareness level is low

Yet, it is possible to act today

- Understand the threats to critical assets
- Assess applicable security measures
- Collaborate to enhance cyber security

ENISA aims at providing pragmatic solutions to secure transport infrastructure in Europe

Cybersecurity for Smart Cars

- Increased attack surface
- Insecure development in today's cars
- Security culture
- Liability
- Safety and security process integration
- Supply chain and glue code

Preliminary Findings - Smart Cars

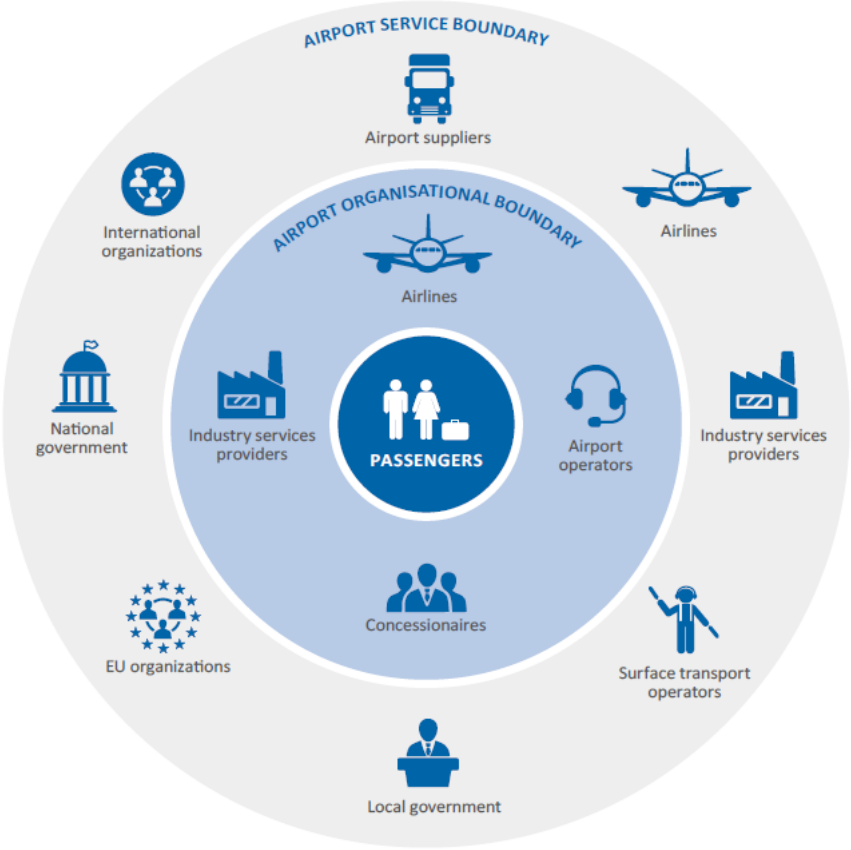
- Improve cyber security in smart cars
- Improve information sharing amongst industry actors
- Improve exchanges with security researchers and third parties
- Clarify liability among industry actors
- Achieve consensus on technical standards for good practices
- Define an independent third-party evaluation scheme
- Build tools for security analysis

Cybersecurity for smart airport

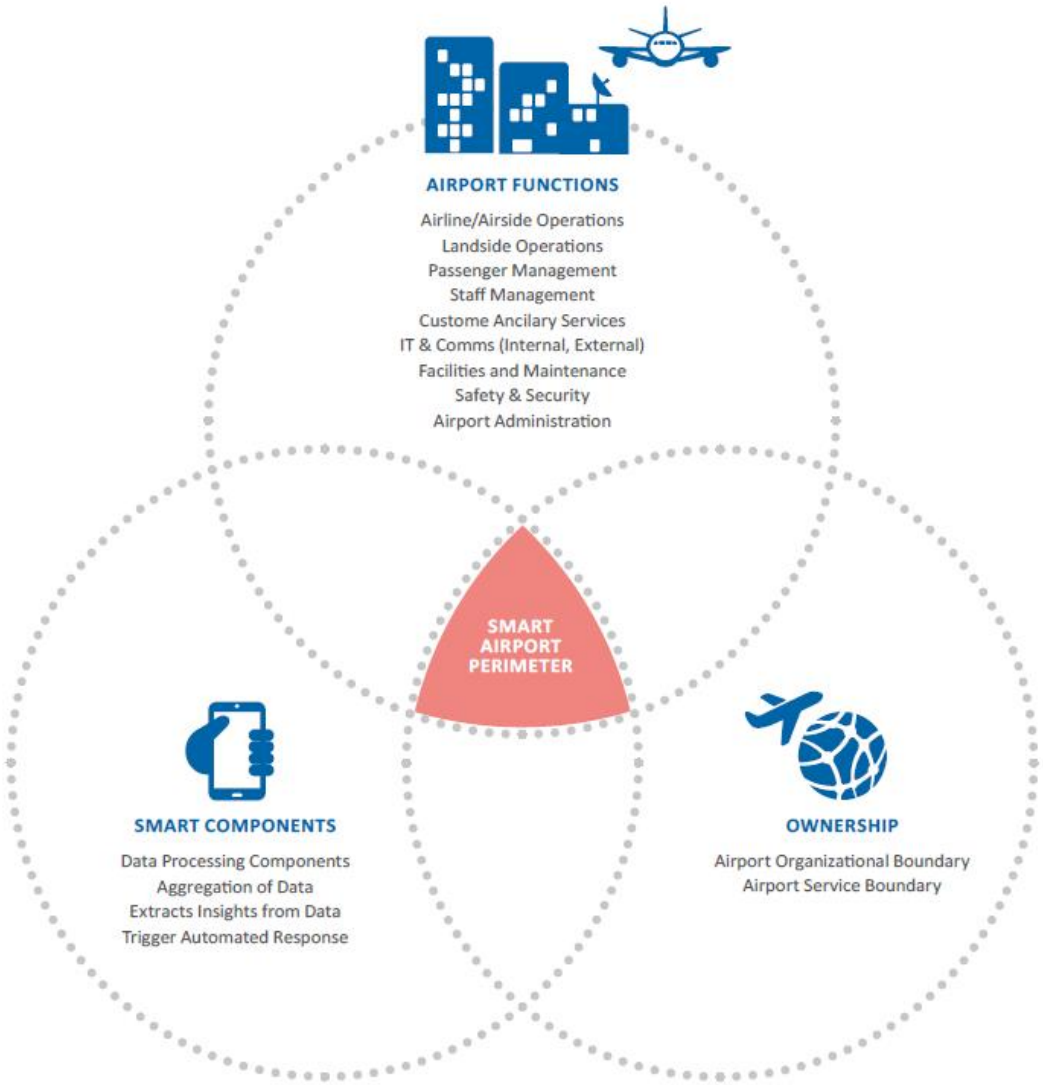
The objective of this study is to improve the security and resilience of airports and air traffic control to prevent disruptions that could have an impact on the service being delivered and on the passengers.

Workshop November 2016

Publication Q4 2016



Perimeter of the study



The goal is to cover the entire IT perimeter of smart airports:

- Assets inside the airport
- Connected assets outside the airport
- Dependencies on the airway

Preliminary Findings – Smart airports

- Variety of cyber security practices in airports
- Lack of EU regulations on cyber security of airports
- Lack of guidelines on network architecture, ownership, and remote management
- Evidence-based vulnerability analysis metrics and priorities
- Threat modelling and architecture analysis
- Information sharing
- Multi-stakeholder enable security technologies
- Appropriate Security Governance model
- Skillset of experts – safety vis a vis security

Recommendations

ENISA recommendations

- Propose solutions to enhance cyber security
- Targeted at Policy makers, transport Operators, Manufacturers and Service providers

Key recommendations (excerpt)

- Promote collaboration on cyber security across Europe
- Integrate security in business processes
- Develop products integrating security for safety

Cyber security for Transport requires *a global effort*

How you can get involved

- Studies
- Events:
  - Network attacks to ICS SCADA - 27th of September - Frankenthal
  - Securing Smart Cars – 10th of October - Munich
  - NISD and ICS SCADA skills - 26/28th of October - Stockholm

Open call for experts:

- CARSEC Smart Car security expert group
- TRANSSEC - Intelligent Public Transport Resilience and Security Expert Group
- ENISA ICS Security Stakeholder Group
- EuroSCSIE - European SCADA and Control Systems Information Exchange

https://resilience.enisa.europa.eu/

The road ahead

The Network and Information Security Directive

Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

Status: 17 May 2016, the Council approved its position at first reading. The next step is approval of the legal act by the European Parliament at second reading. The directive entered into force in August 2016. 21 months after entry into force from transposition

Provisions:

- Obligations for all MS to adopt a national NIS strategies and designate national authorities.
- Creates first EU cooperation group on NIS, from all MS.
- Creates a EU national CSIRTs network.
- Establishes security and notification requirements for operators of essential services and digital service providers

The NIS Directive

National Cyber Security Strategies

enisa

Cloud Computing Services

Strategic Cooperation Network

Transport

Digital Service Providers

Operators of Essential Services

Incident Reporting

Security Requirements

Energy

Healthcare

Online Marketplaces

Banking and Financial market infrastructures

Search Engines

Tactical/Operational CSIRT Network

Digital Infrastructure

http://www.consilium.europa.eu/en/policies/cyber-security/

ENISA's overall role and contribution

- Assist MS and EU Comm by providing expertise/advice and by developing/facilitating exchange of good practices, e.g.
  - assist MS in developing national NIS Strategies (NCSS)
  - assist EU Commission and MS in developing min security requirements for ESOs and DSPs
  - assist EU Commission and MS in developing incident reporting frameworks for ESOs and DSPs
  - assist MS in the defining criteria for the designation of ESOs
- Be the secretariat of the CSIRT network and develop with members the network
- Participate/contribute to the work of the Cooperation Group (CG)
- Elaborate advices and guidelines regarding standardization in NIS security, together with MS

NISD Timeline

Date	entry into force + …	Milestone
August 2016	-	Entry into force
February 2017	6 months	Cooperation Group begins tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
May 2018	21 months	Transposition into national law
November 2018	27 months	**Member States to identify operators of essential services**
May 2019	33 months (i.e. 1 year after transposition)	**Commission report assessing the consistency of Member States' identification of operators of essential services**
May 2021	57 months (i.e. 3 years after transposition)	Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers

Goals

01 Raise the level of awareness on Infrastructure security in Europe

02 Support Private and Public Sector with focused studies and tools

03 Facilitate information exchange and collaboration

04 Foster the growth of communication networks and industry

05 Enable higher level of security for Europe's Infrastructures

Thank you,

Rossella Mattioli

resilience@enisa.europa.eu

https://www.enisa.europa.eu/