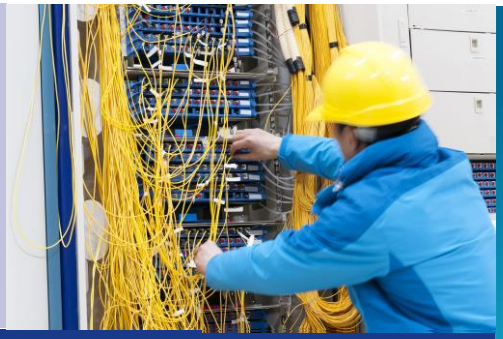


Enhancing infrastructure cybersecurity in Europe

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

EUROPEAN CYBER SECURITY MONTH

enisa

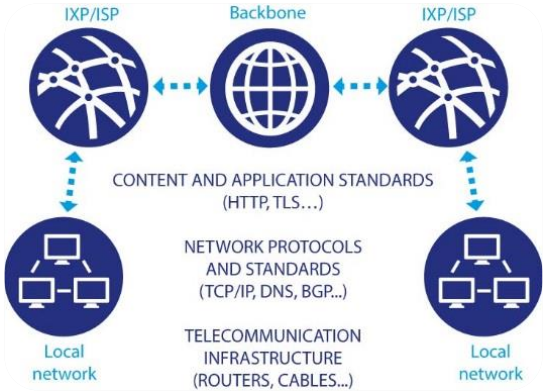
October is CyberSecMonth

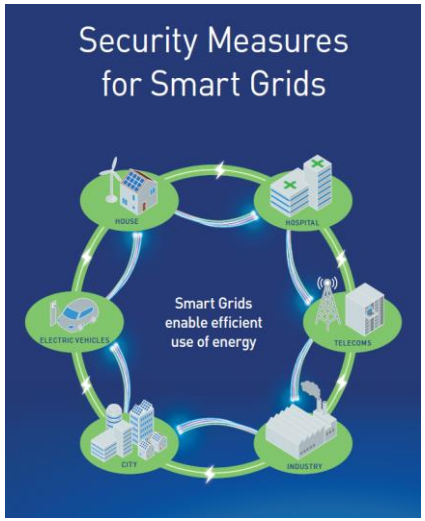
1st – 31st October 2016

https://cybersecuritymonth.eu/

Secure Infrastructure and Services

Communication networks: Critical Information Infrastructure and Internet Infrastructure

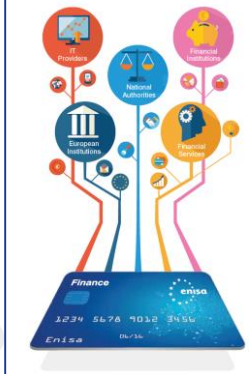




Transport

eHealth and Smart Hospitals

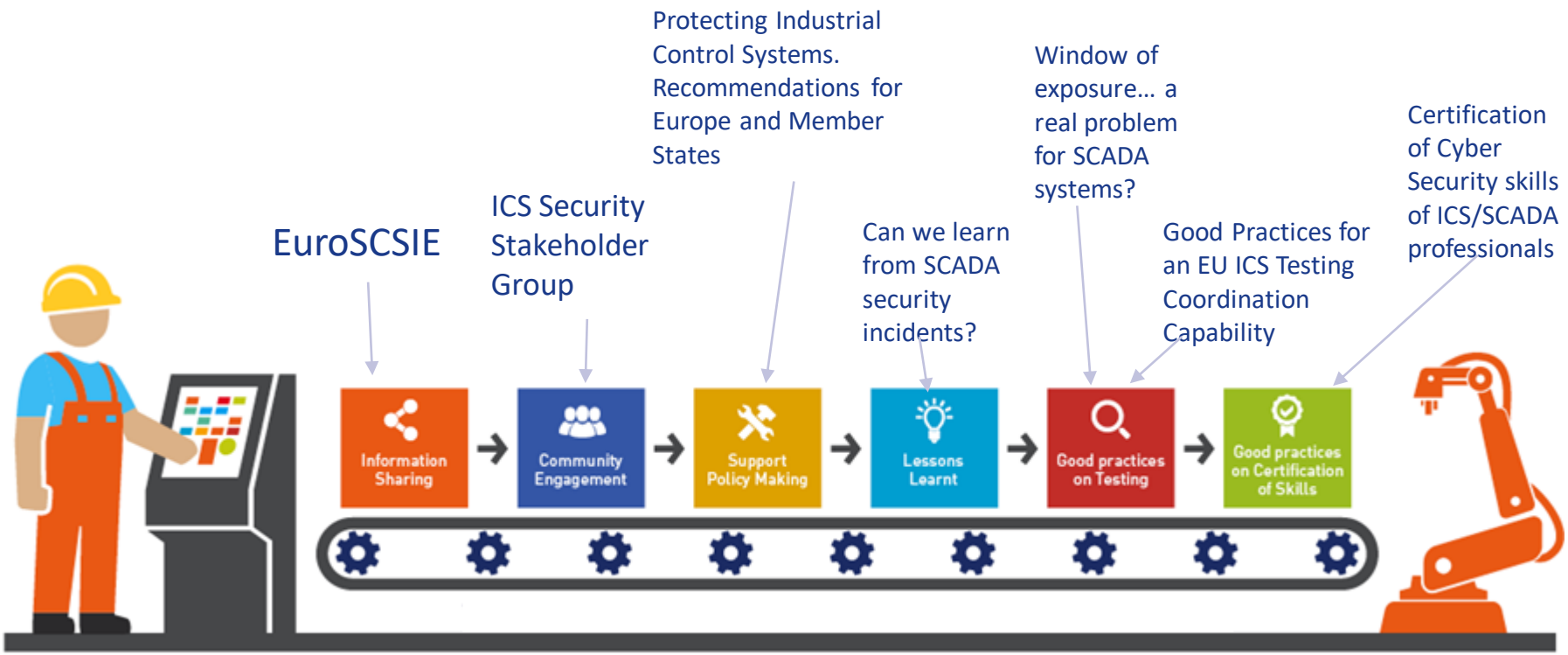
Finance



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

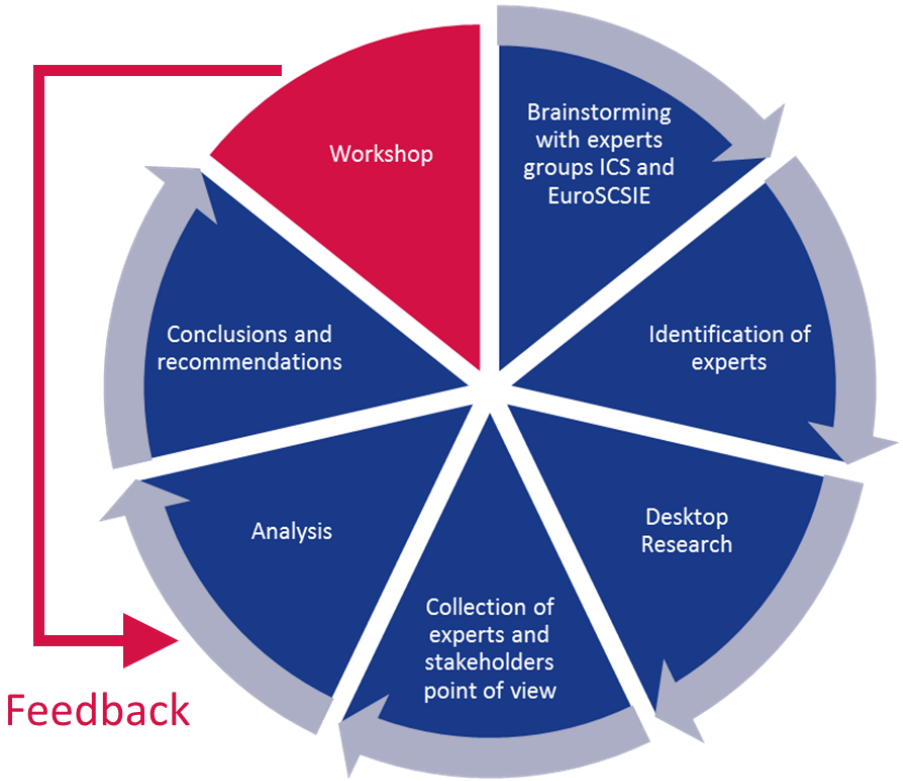
ENISA 2016 efforts

Cybersecurity for ICS SCADA



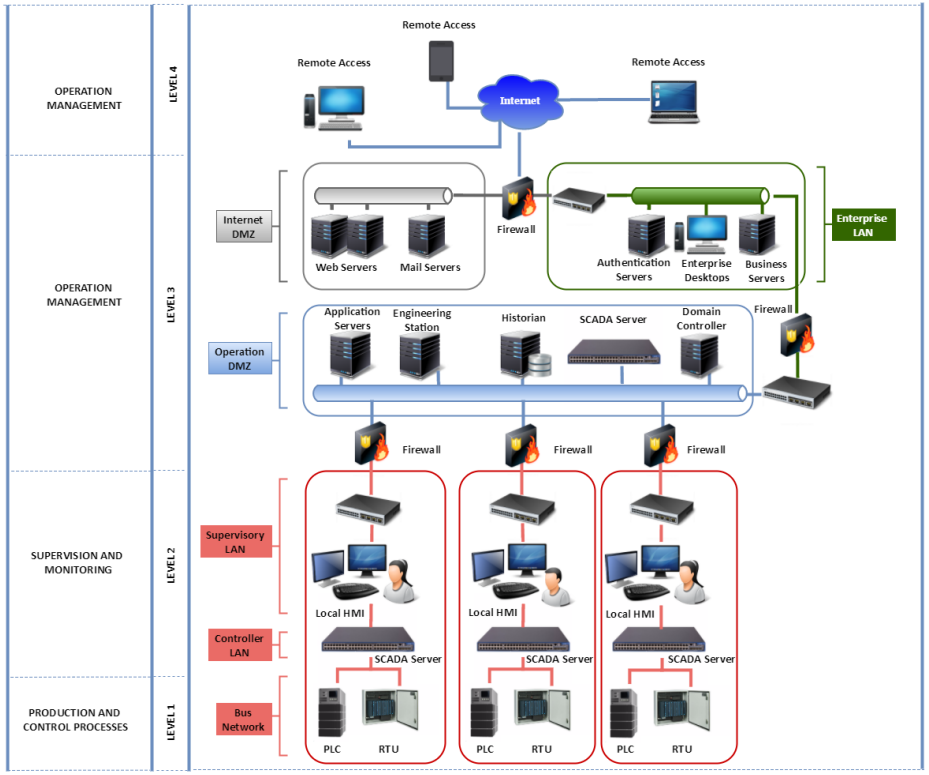
https://www.enisa.europa.eu/scada

Communication network dependencies for ICS/SCADA

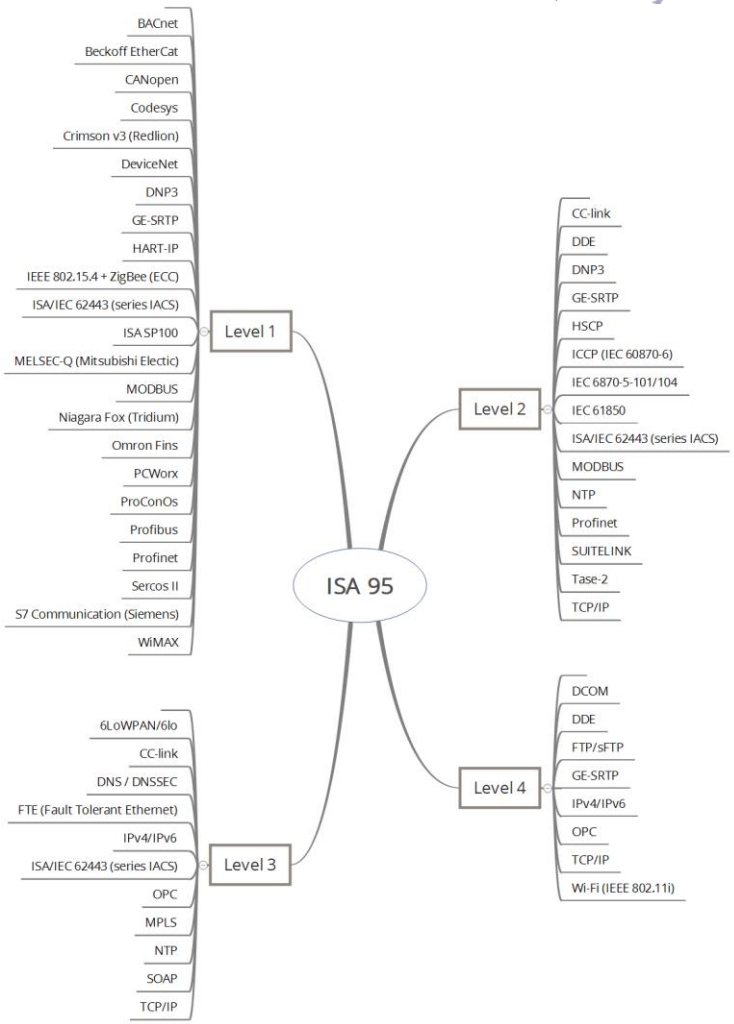


- Map assets and threats via desktop research, and interviews with security researchers and asset owners.
- Identify all possible attacks coming from network exposure.
- Examine and list existing protocols' security vulnerabilities.
- Collect good security practices and security measures.
- Develop three attack scenarios and possible mitigation actions.
- Define recommendations for Europe

Perimeter & protocols



ISA95 levels applied to a SCADA architecture



Protocols

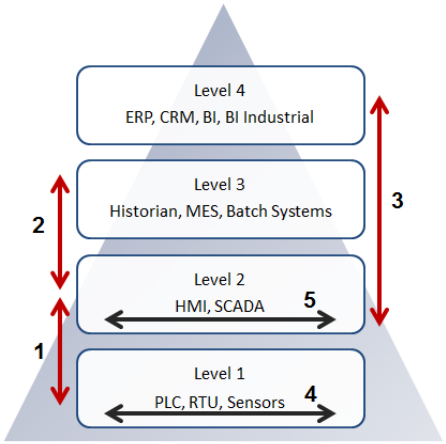
Communications dependencies

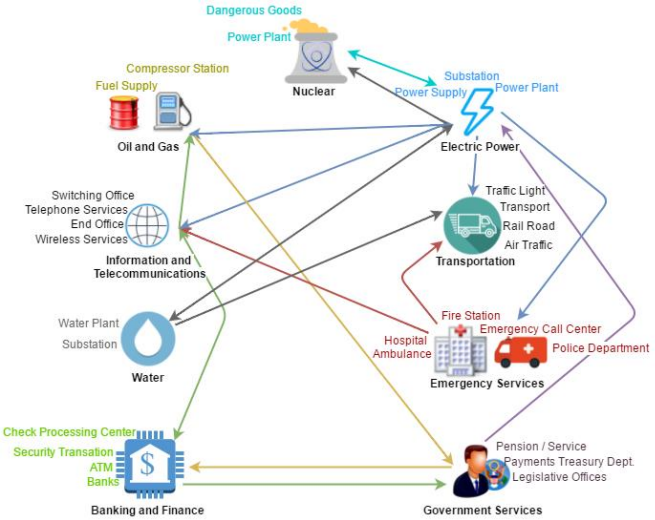
Vertical communications (bi-directional)

- Exchange between sensors and processing systems.
- Between SCADA systems (Data Historian, MES, process transfer, etc.).
- Between SCADA and ERP or BI systems.

Horizontal communications

- Between sensors PLCs, etc.
- Between SCADA systems (HMIs, local…).





External interdependencies (bi-directional)

- Physical
- Geographical
- Cyber
- Logical

Threats affecting ICS/SCADA systems

THREAT	LIKELYHOOD	IMPACT
Malware (*Virus, Trojan, Worms*)	**Very High**	**High**
Exploit Kits (*including rootkits*)	**Medium**	**High**
Advanced Persistent Threats (*APTs*)	**Low**	**High**
Insider Threats (*e.g. Employee incidents*)	**Low**	**Crucial**
Eavesdropping (*e.g. MitM*)	**Low**	**High**
Communication System/Network Outage	**Low**	**High**
(*Distributed*) **Denial of Service**	**Low**	**Medium**
(*Internal/Sensitive*) **Information Leakage**	**Low**	**Medium**

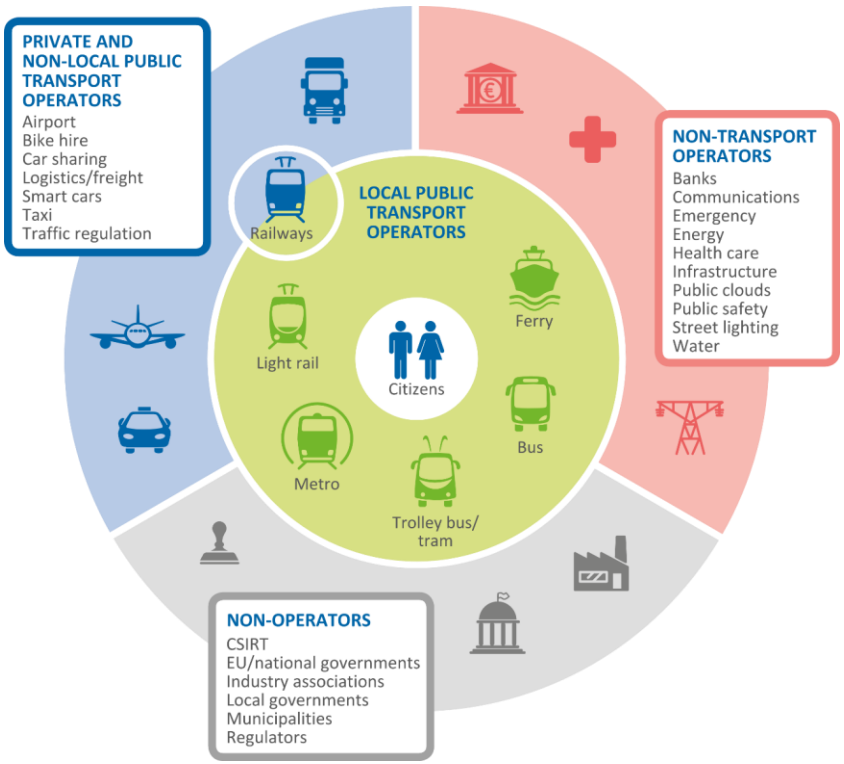
Attacks scenarios and PoCs

- Against the administration systems of SCADA
- Against actuators
- Against the network link between sensors/actuators and HMI or controller
- Against sensors
- Against the information transiting the network
- Compromised ICT components as backdoors
- Exploit Protocol vulnerabilities
- Against Control data historian, HMI or controllers

Recommendations

- *Include security as a main consideration during the design phase of ICS/SCADA systems*
- *Identify and establish roles of people operating in ICS/SCADA systems*
- *Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements*
- *Define network communication technologies and architecture with interoperability in mind*
- *Establish brainstorming and communication channels for the different participants on the lifecycle of the devices to exchange needs and solutions*
- *Include the periodic SCADA device update process as part of the main operations of the systems*
- *Establish periodic ICS/SCADA security training and awareness campaign within the organization*

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**

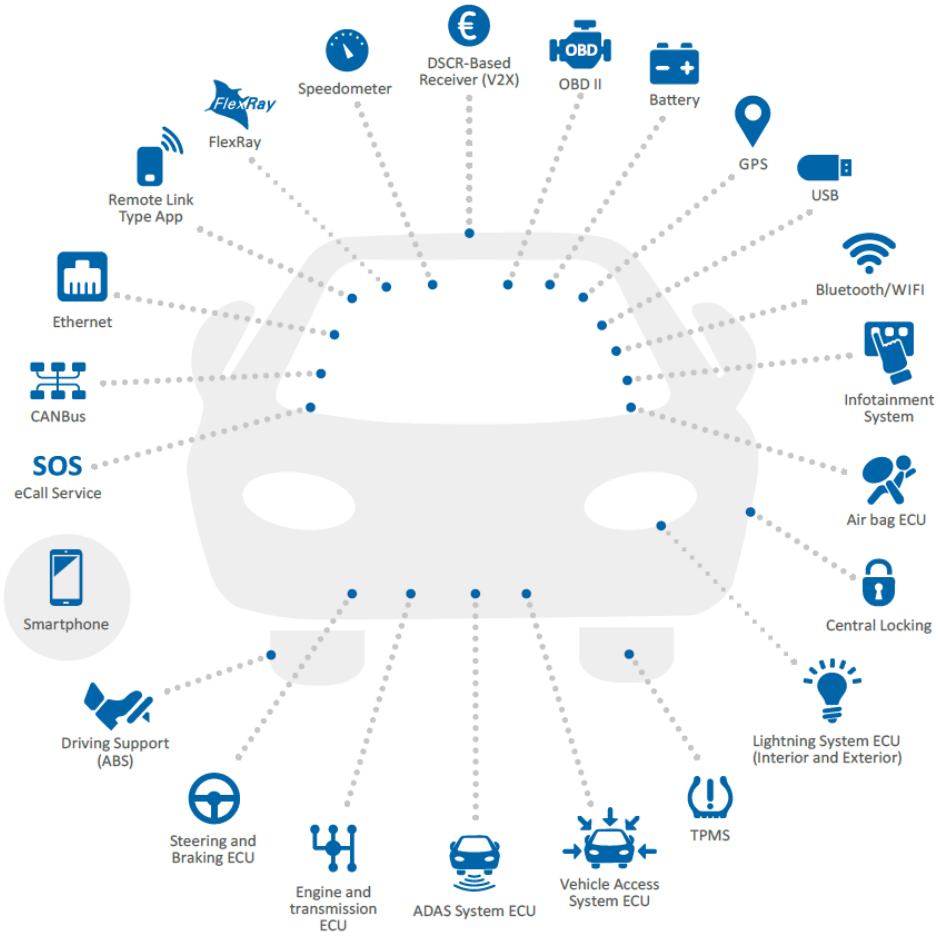
Objectives

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

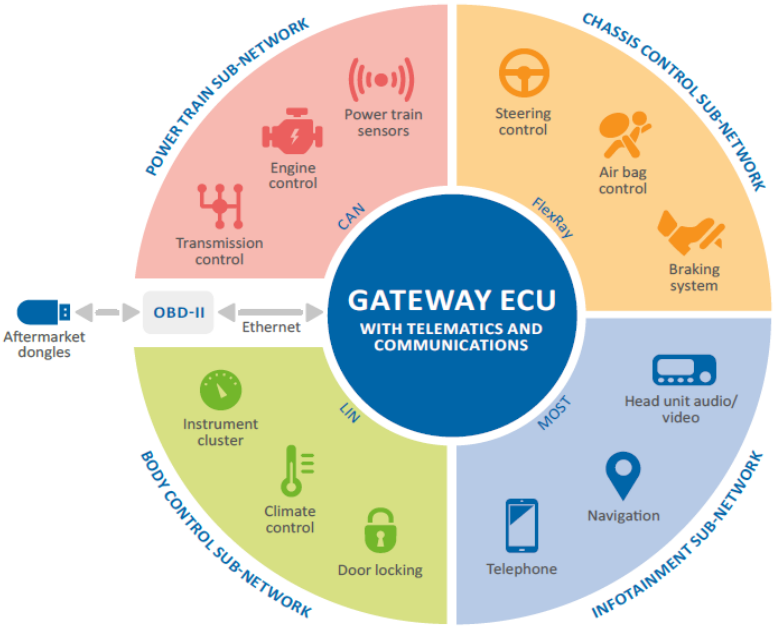
https://www.enisa.europa.eu/smartinfra

Cybersecurity for Smart Cars

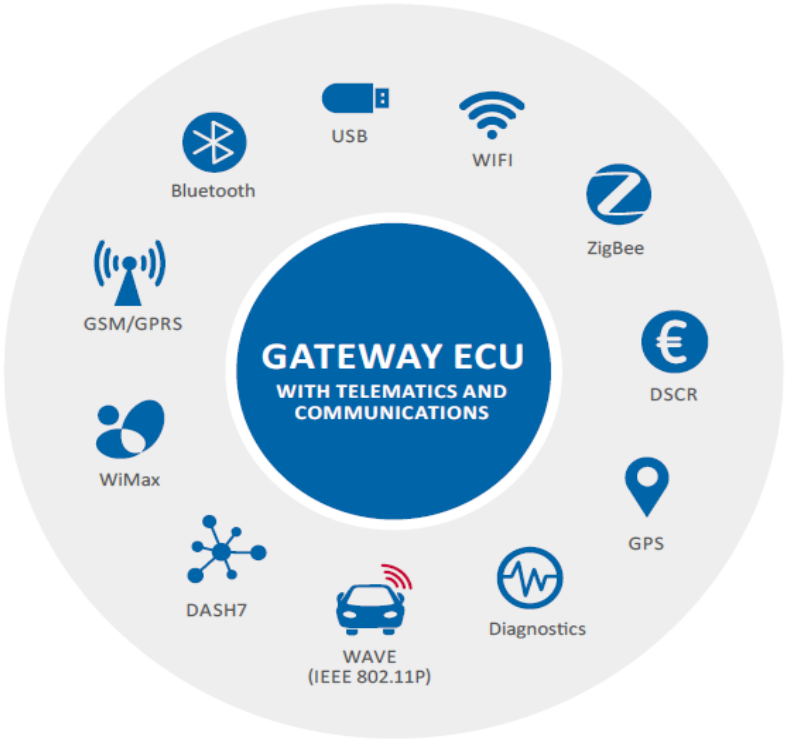
- Increased attack surface
- Insecure development in today's cars
- Security culture
- Liability
- Safety and security process integration
- Supply chain and glue code



Communications dependencies



Internal communication sub-networks



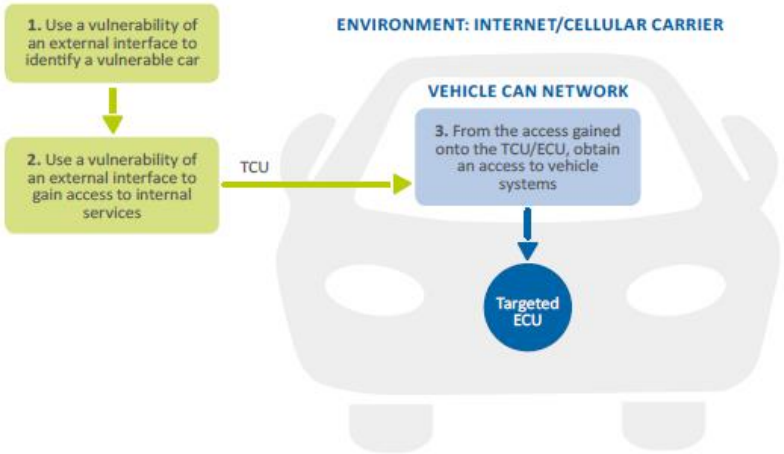
External communication interfaces

Threats

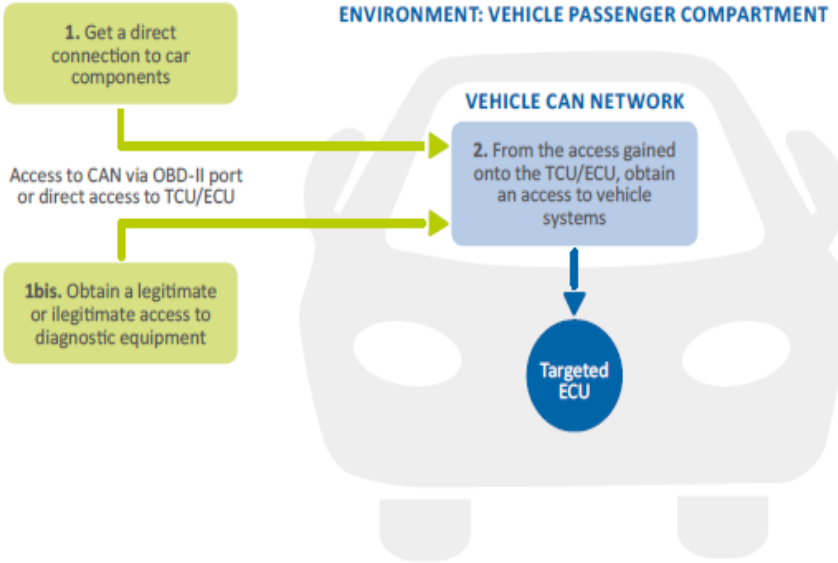

DAMAGE / LOSS (IT ASSETS)
Loss of information in the cloud
Loss of (integrity of) sensitive information
Damage caused by a third party
Loss from DRM conflicts
Information leakage
PHYSICAL ATTACKS
Fault injection / glitching
Side channel
Access to HW debug ports
UNINTENTIONAL DAMAGES (ACCIDENTAL)
Information leakage or sharing
Erroneous use or administration of devices and systems
Using information from an unreliable source
Unintentional change of data in an information system
Inadequate design and planning or lack of adaption
ADVANCED PERSISTENT THREATS
NETWORK OUTAGE
THREATS
FAILURES / MALFUNCTIONS
Failures / malfunctions of devices or systems
Failures or disruptions of the power supply
Software bugs
Failures / malfunctions of parts of devices
Failures or disruptions of communication links
Failures or disruptions of main supply
NEFARIOUS ACTIVITY / ABUSE
Denial of service
Malicious code / software activity
Manipulation of hardware & software
Manipulation of information
Unauthorised access to information system / network
Compromising confidential information
Identity fraud
Abuse of information leakage
Unauthorized use of administration of devices & systems
Unauthorized use of software
Unauthorized installation of software
Abuse of authorizations
Malicious software
Remote activity (execution)
EAVESDROPPING / INTERCEPTION / HIJACKING
Interception of information
Replay of messages
Interfering radiations
Man in the middle / session hijacking
Network reconnaissance and information gathering
Repudiation of actions

Attack scenarios

- **Remote attack** (threatening safety)



- **Persistent vehicle alteration** (by the legitimate user or by the use of diagnostic equipment)

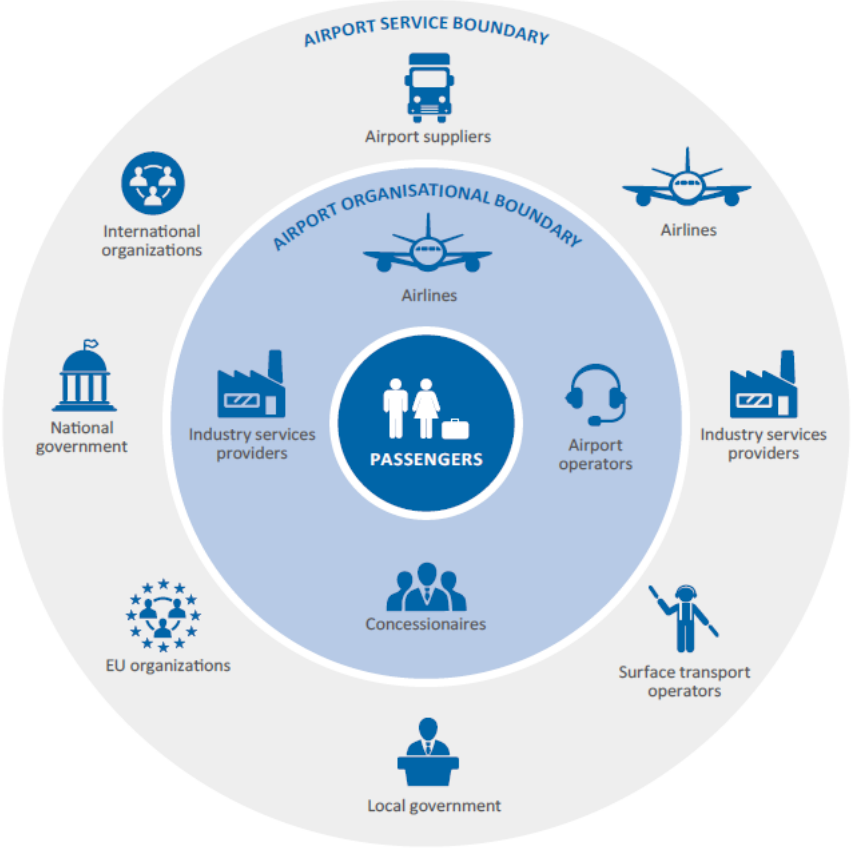


Preliminary Findings - Smart Cars

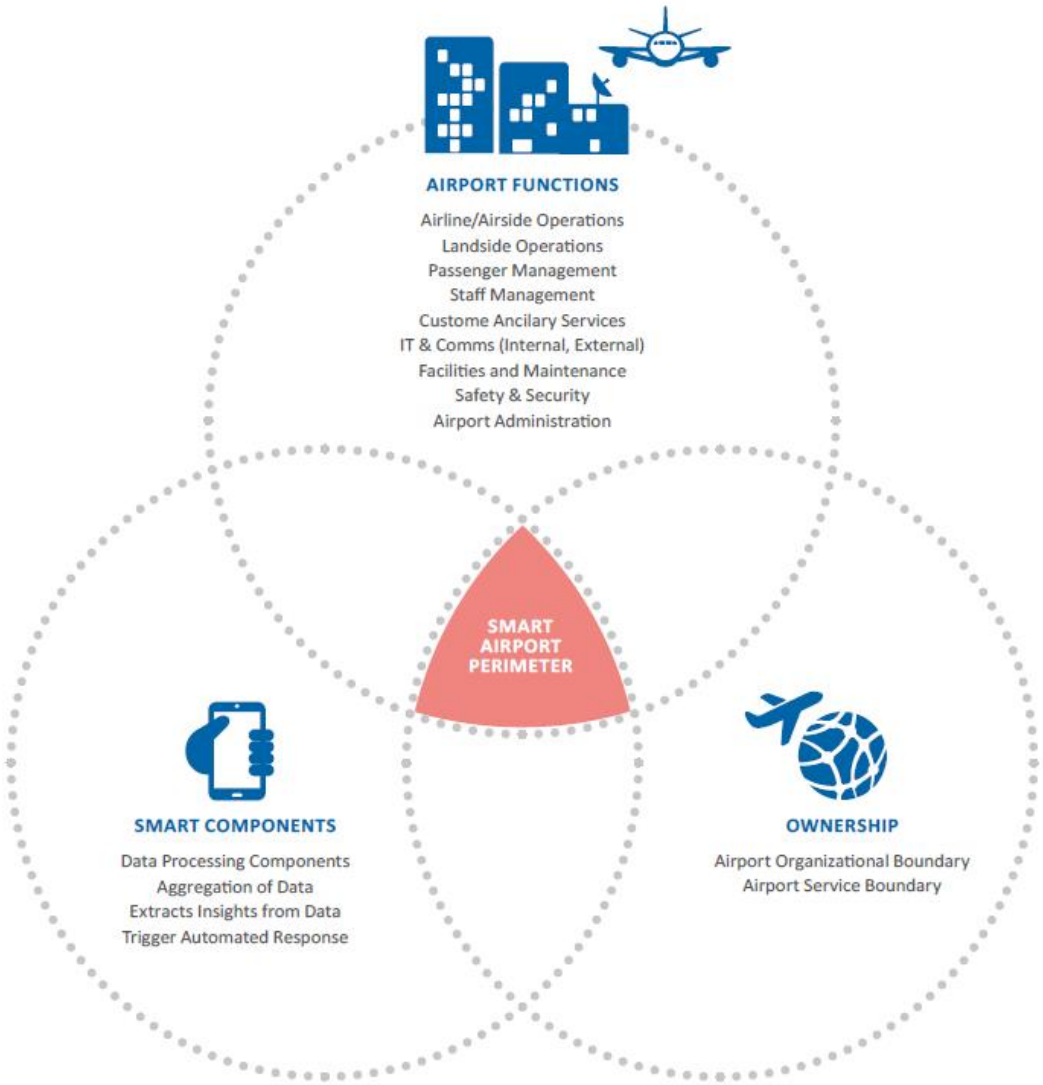
- *Improve cyber security in smart cars.*
- *Improve information sharing amongst industry actors. Improve exchanges with security researchers and third parties.*
- *Clarify liability among industry actors.*
- *Achieve consensus on technical standards for good practices.*
- *Define an independent third-party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



Perimeter of the study



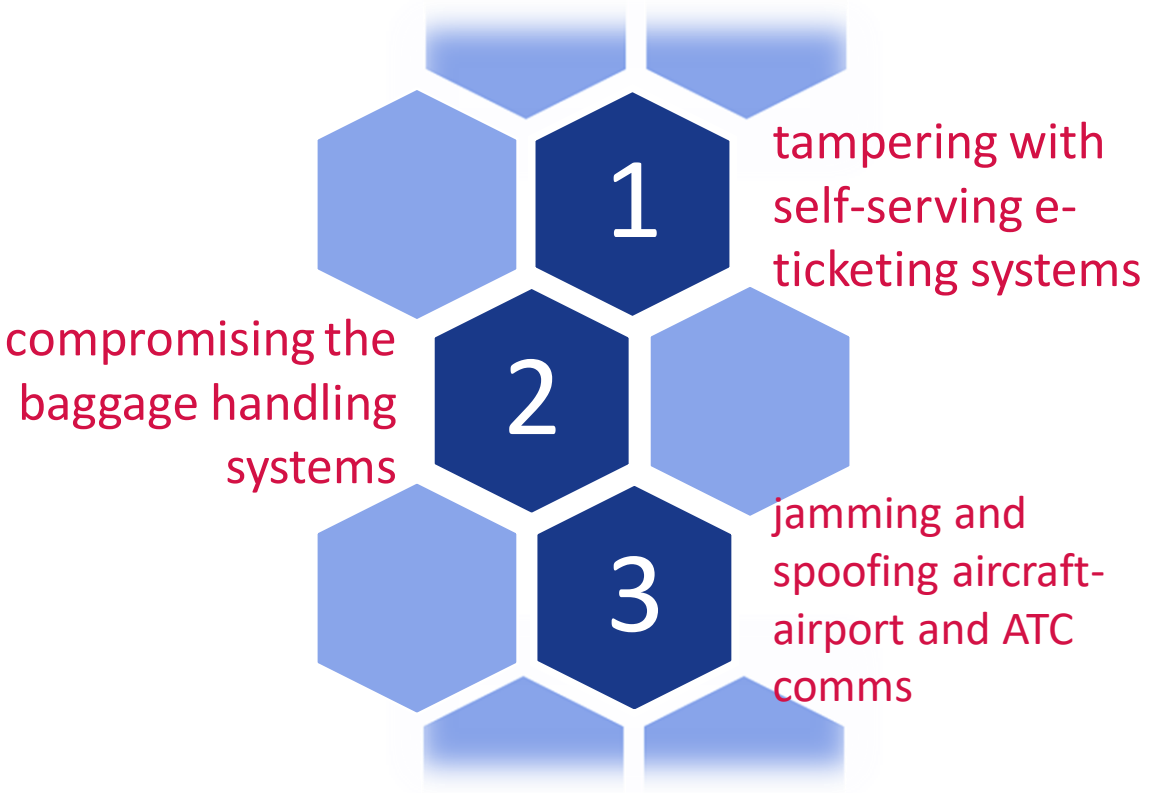
The goal is to cover the entire IT perimeter of smart airports:

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

Threat modelling

Attacks scenarios and PoCs

- Social engineering spear phishing attacks against Airport Administration / ERP
- Network / interception attacks against Airline/Airside Operations (ATM comms)
- Misuse of authority / authorization within landside ops
- Tampering with airport devices to compromise passenger management
- Network / interception attacks against SCADA systems
- Malware on POS
- DDoS on Cloud



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, infrastructure 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 requires *a global effort*

How you can get involved

- Studies
- Events:
  - ENISA session @4SICS 26th of October – Stockholm
  - EICS and EUROSCSIE meeting - 28th of October – Stockholm
  - Mobile offense and defense – 10th of November- Berlin

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

Open call for experts:

- TRANSSEC - Intelligent Public Transport Resilience and Security Expert Group
- CARSEC – Smart cars cyber security expert group
- ENISA ICS Security Stakeholder Group
- INFRASEC Internet Infrastructure security and resilience

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

Upcoming ENISA studies on infrastructure cybersecurity

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/