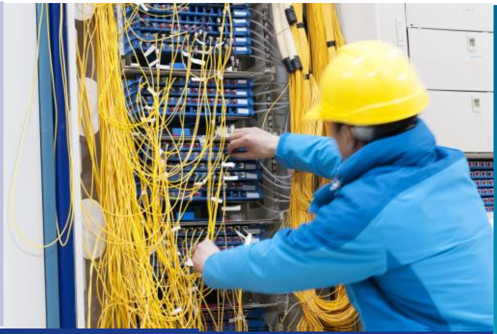


Enhancing infrastructure cybersecurity in Europe

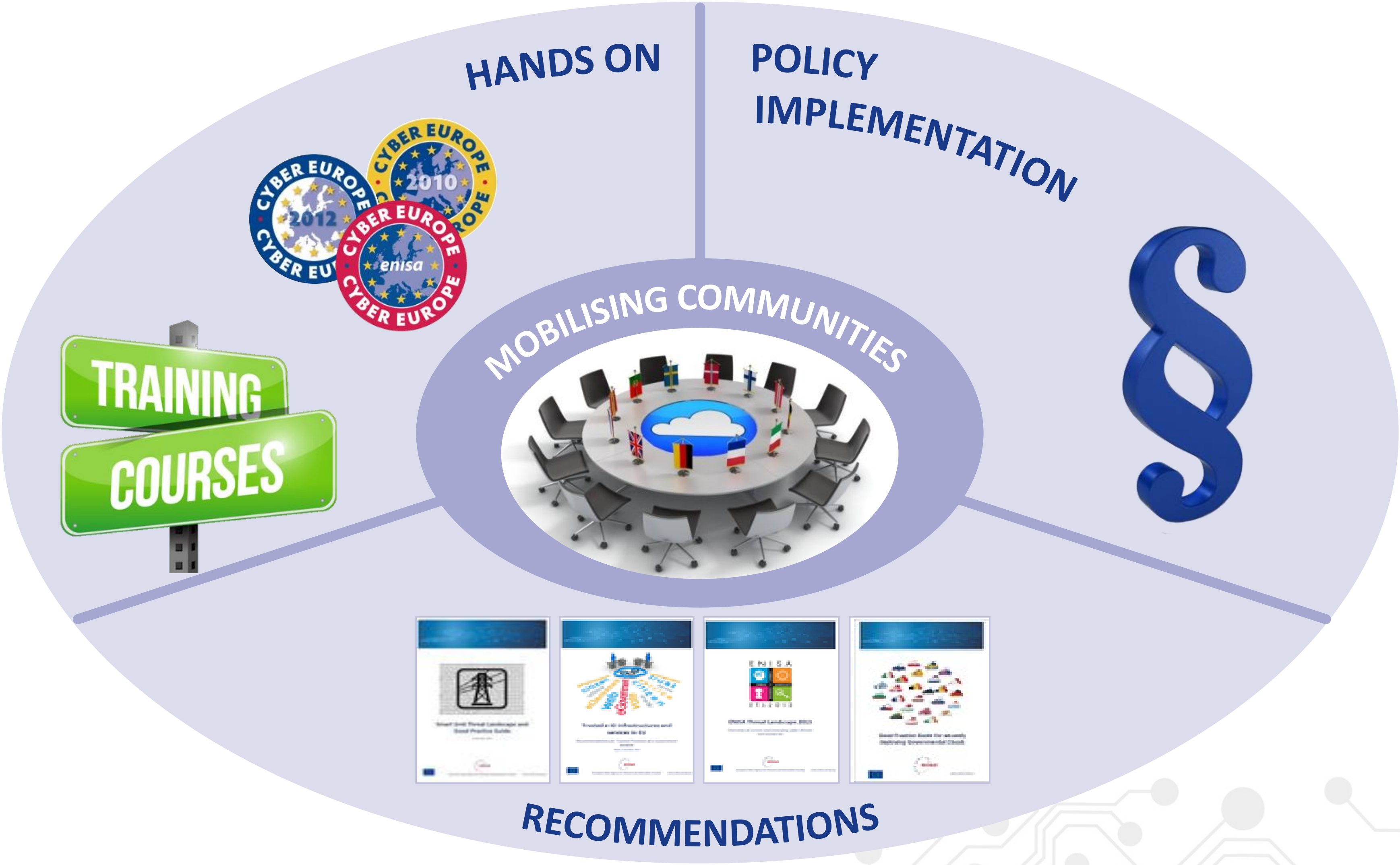
Rossella Mattioli

Secure Infrastructures and Services

European Union Agency for Network and Information Security

Securing Europe’s Information society

Positioning ENISA activities



HANDS ON

POLICY IMPLEMENTATION

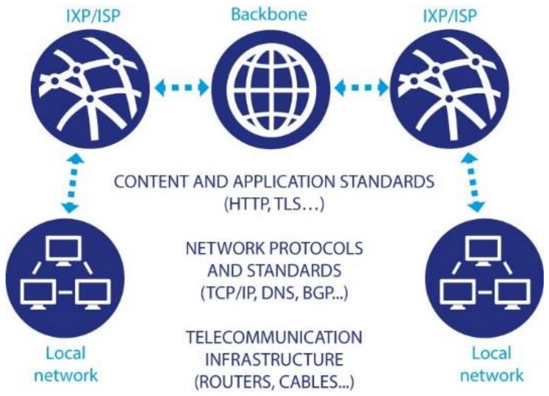
MOBILISING COMMUNITIES

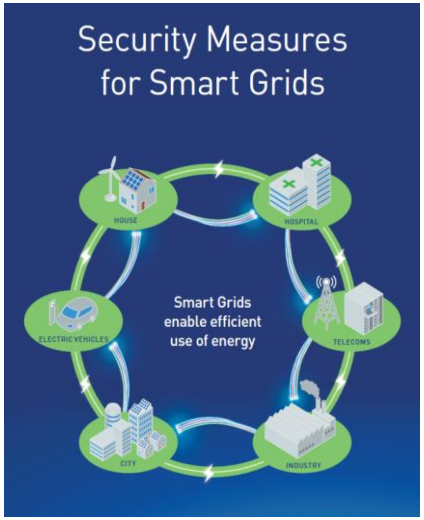
RECOMMENDATIONS

Secure Infrastructure and Services

enisa
Annual studies
Community engagement
SECURING EUROPEAN NETWORKS
INFRASEC
ENISA Internet infrastructure security and resilience reference group
Workshops

Communication networks: Critical Information Infrastructure and Internet Infrastructure



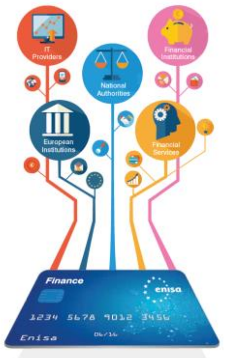

Security Measures for Smart Grids
HOUSE
HOSPITAL
ELECTRIC VEHICLES
TELECOMS
CITY
INDUSTRY
Smart Grids enable efficient use of energy

Transport

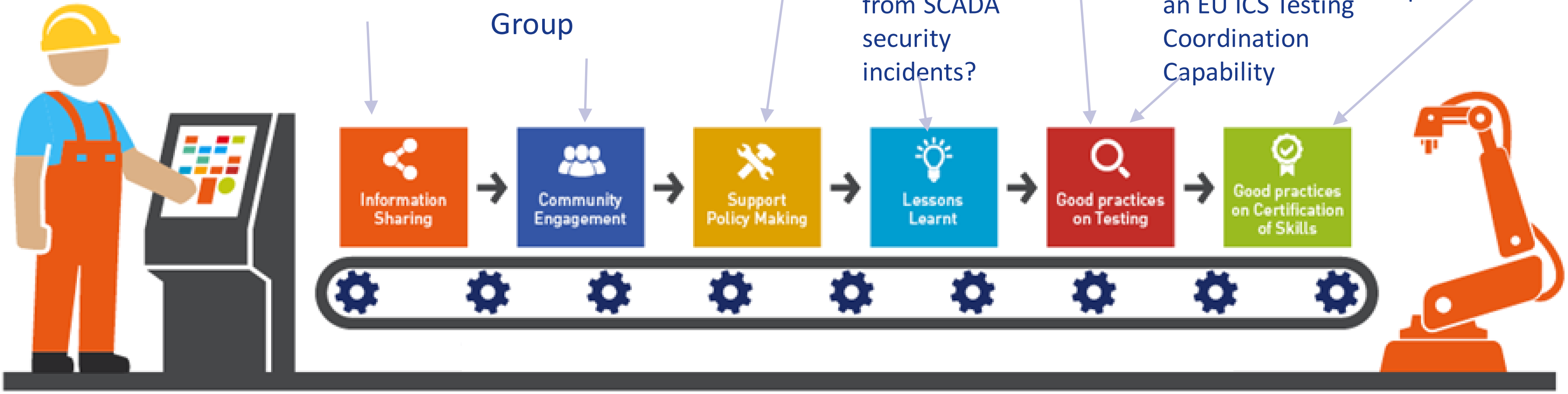
ENHANCING THE SECURITY OF ICS SCADA IN EUROPE
ENERGY
WATER
TRANSPORT
SHIPPING
CHEMICALS
MANUFACTURING
INDUSTRIAL CONTROL SYSTEMS
SUPERVISORY CONTROL AND DATA ACQUISITION

eHealth and Smart Hospitals

Finance



Cybersecurity for ICS SCADA



EuroSCSIE

ICS Security Stakeholder Group

Protecting Industrial Control Systems. Recommendations for Europe and Member States

Can we learn from SCADA security incidents?

Window of exposure… a real problem for SCADA systems?

Good Practices for an EU ICS Testing Coordination Capability

Certification of Cyber Security skills of ICS/SCADA professionals

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

Communication network dependencies for ICS SCADA

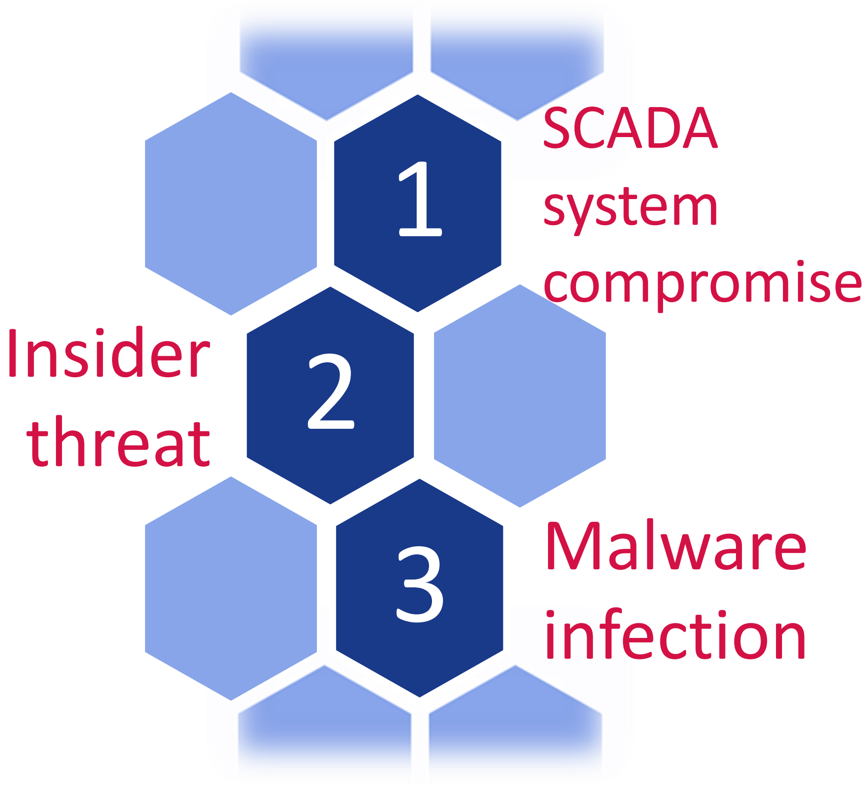
- *Outlined scope and perimeter with EICS SG and EUROSCSIE experts*
- Map assets and threats via desktop research and interviews with security researchers and asset owners
- List all possible attacks coming from network exposure
- Examine protocols vulnerabilities
- List good practices
- Develop 3 attack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

Threats affecting ICS/SCADA systems

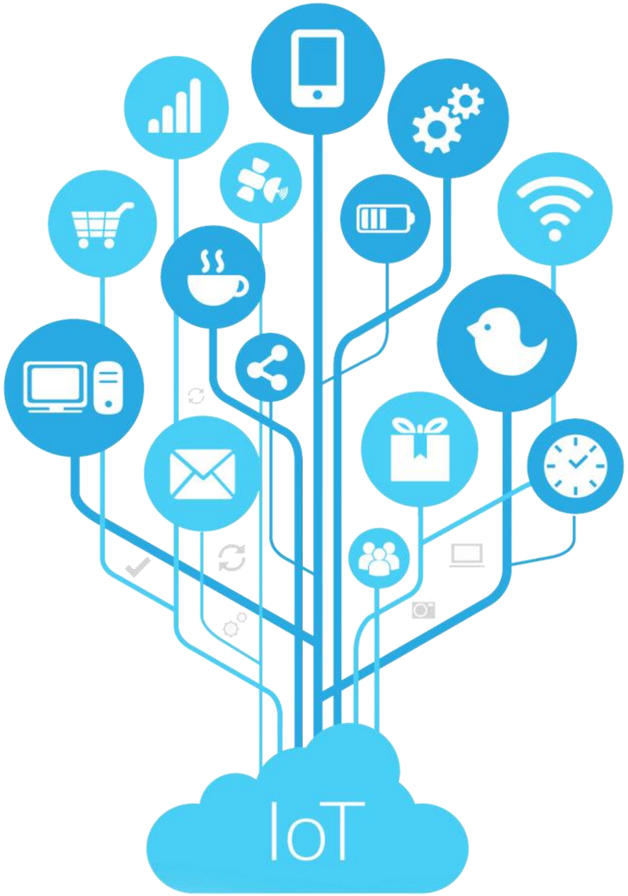
THREAT	LIKELIHOOD	IMPACT
Malware (*Virus, Trojan, Worms*)	Very High	High
Exploit Kits (*including rootkits*)	Medium	High
Advanced Persistent Threats (*APTs*)	Low	High
Insider Threats (*e.g. Employee incidents*)	Low	Crucial
Eavesdropping (*e.g. MitM*)	Low	High
Communication System/Network Outage	Low	High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

Attacks scenarios and PoCs

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



Securing Smart cities and transport infrastructure



Smart Cities as a “system of systems”

New and emerging risks

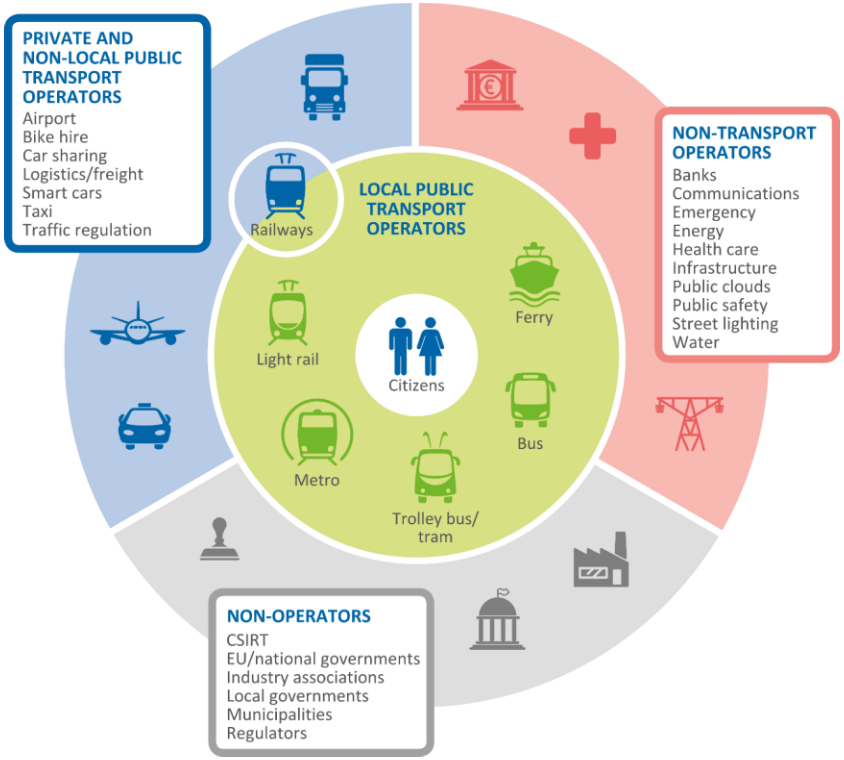
- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (legacy) systems
- Data exchange integrated into business processes

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 <u>operational</u> and organisational

Securing transport infrastructure



2015 studies

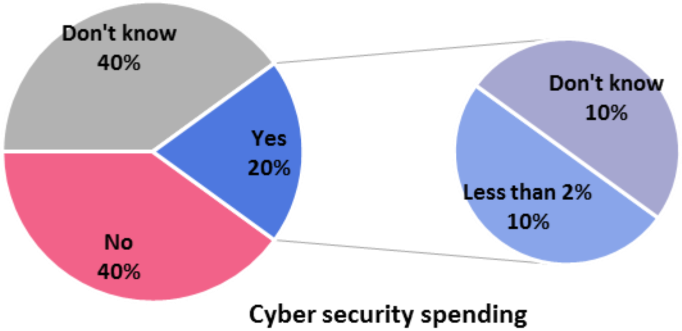
- **Architecture model of the transport sector in Smart Cities**
- **Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations**

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



Cyber security spending

Existing status of security for IPT is limited

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

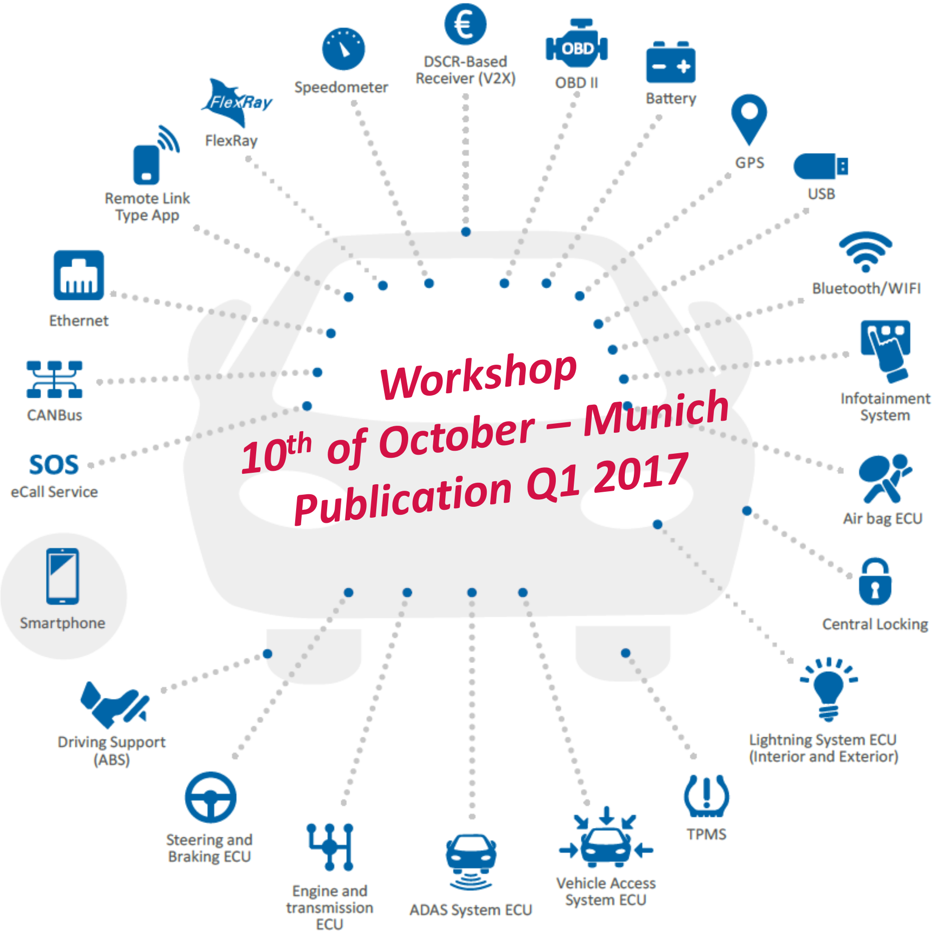
Yet, it is possible to act today

- 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



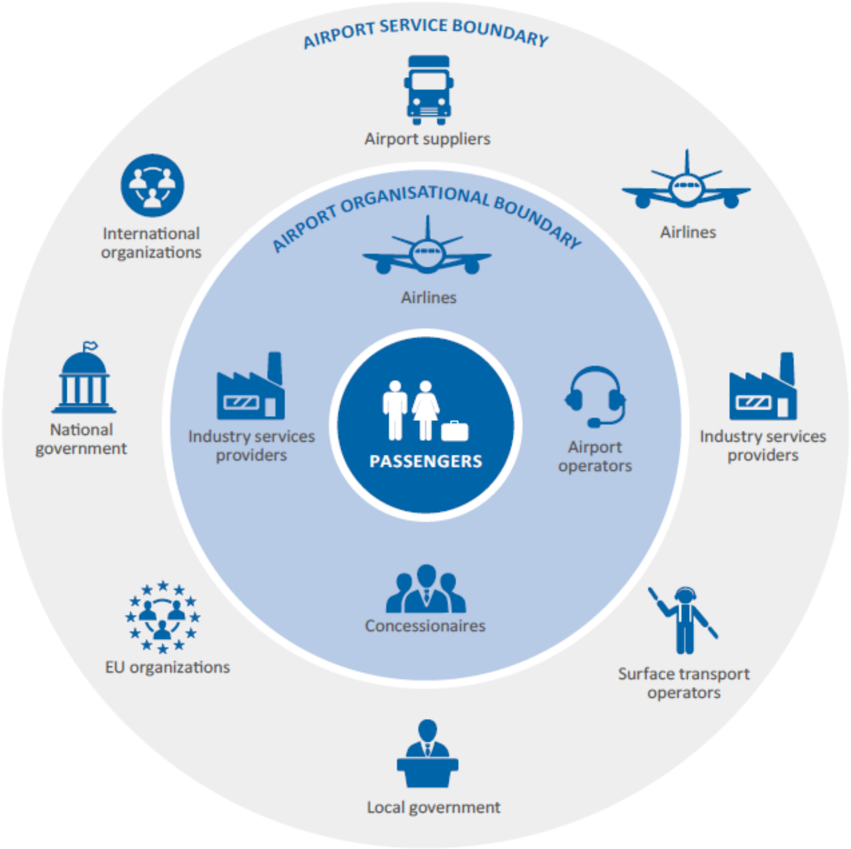
Workshop
10th of October – Munich
Publication Q1 2017

Preliminary Findings - Smart Cars

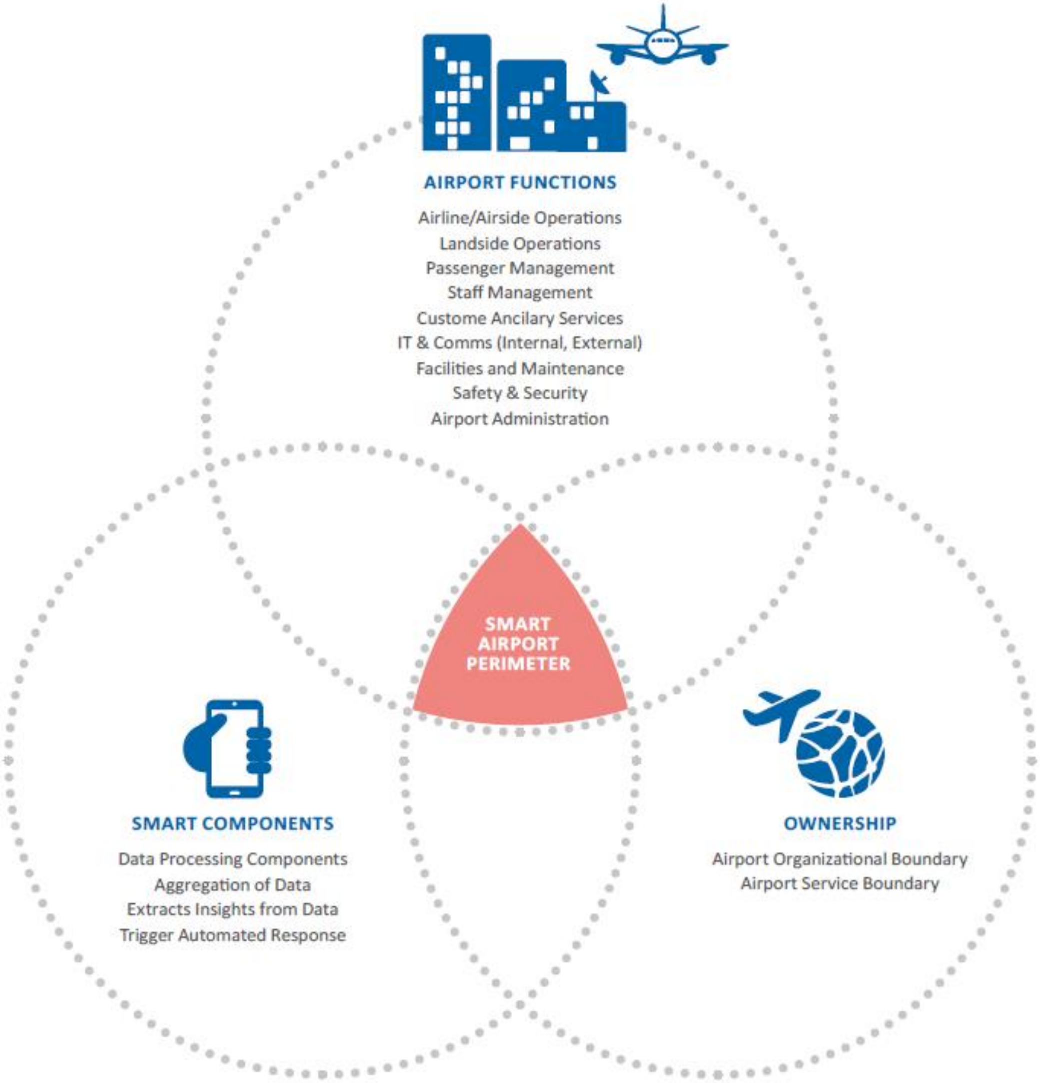
- Improve cyber security in smart cars
- Improve information sharing amongst industry actors
- Improve exchanges with security researchers and third parties
- Clarify liability among industry actors
- Achieve consensus on technical standards for good practices
- Define an independent third-party evaluation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



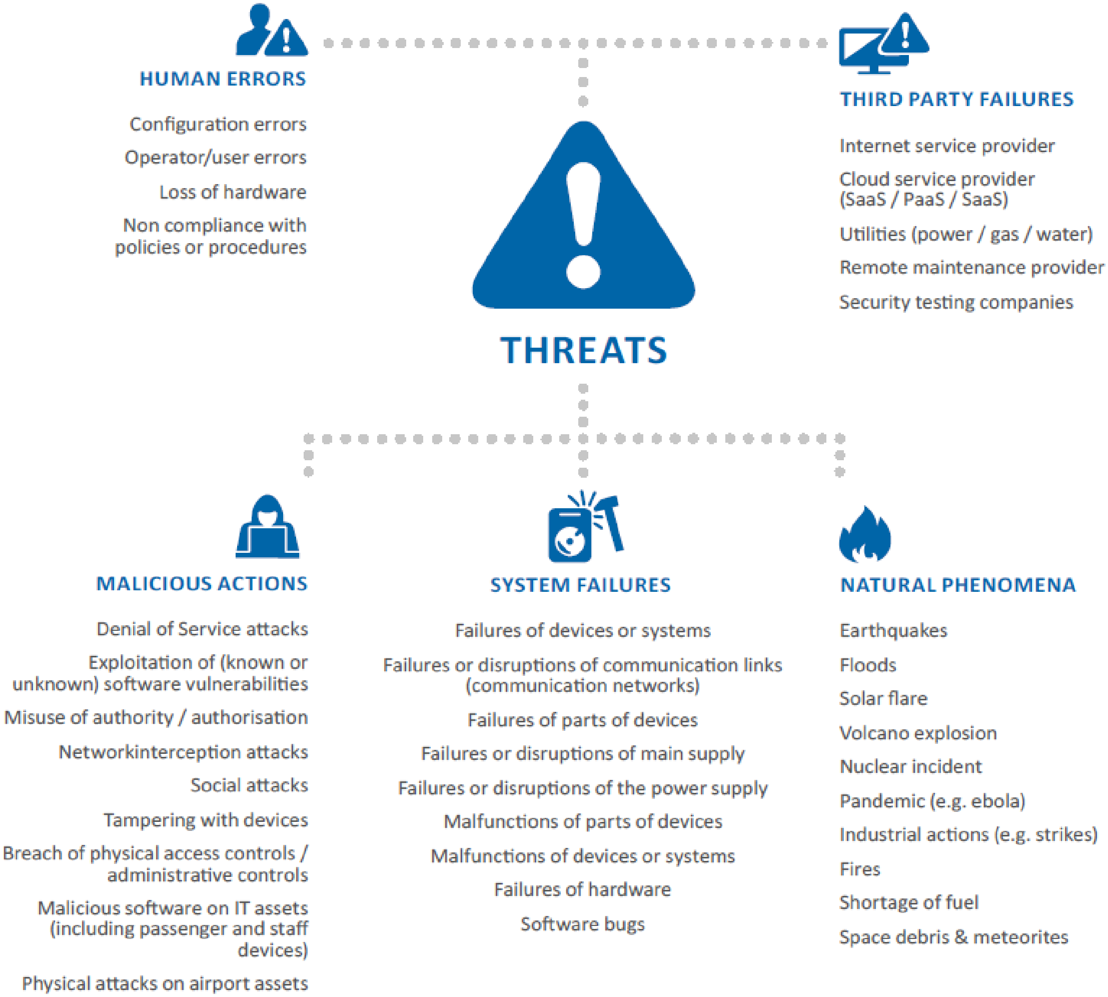
Perimeter of the study


AIRPORT FUNCTIONS
Airline/Airside Operations
Landside Operations
Passenger Management
Staff Management
Custome Ancilary Services
IT & Comms (Internal, External)
Facilities and Maintenance
Safety & Security
Airport Administration
SMART AIRPORT PERIMETER
SMART COMPONENTS
Data Processing Components
Aggregation of Data
Extracts Insights from Data
Trigger Automated Response
OWNERSHIP
Airport Organizational Boundary
Airport Service Boundary

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



THREATS

HUMAN ERRORS

- Configuration errors
- Operator/user errors
- Loss of hardware
- Non compliance with policies or procedures

THIRD PARTY FAILURES

- Internet service provider
- Cloud service provider (SaaS / PaaS / SaaS)
- Utilities (power / gas / water)
- Remote maintenance provider
- Security testing companies

MALICIOUS ACTIONS

- Denial of Service attacks
- Exploitation of (known or unknown) software vulnerabilities
- Misuse of authority / authorisation
- Networkinterception attacks
- Social attacks
- Tampering with devices
- Breach of physical access controls / administrative controls
- Malicious software on IT assets (including passenger and staff devices)
- Physical attacks on airport assets

SYSTEM FAILURES

- Failures of devices or systems
- Failures or disruptions of communication links (communication networks)
- Failures of parts of devices
- Failures or disruptions of main supply
- Failures or disruptions of the power supply
- Malfunctions of parts of devices
- Malfunctions of devices or systems
- Failures of hardware
- Software bugs

NATURAL PHENOMENA

- Earthquakes
- Floods
- Solar flare
- Volcano explosion
- Nuclear incident
- Pandemic (e.g. ebola)
- Industrial actions (e.g. strikes)
- Fires
- Shortage of fuel
- Space debris & meteorites

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

tampering with self-serving e-ticketing systems

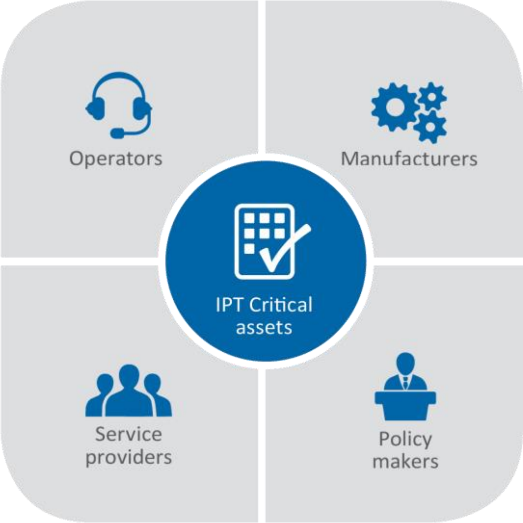
compromising the baggage handling systems

jamming and spoofing aircraft-airport and ATC comms

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:
  - Mobile offense and defense – 10th of November- Berlin
  - ENISA @ HUB – 22/11 - Berlin
  - ENISA eHealth Cyber Security workshop - 23/11 - Wien

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

ENHANCING THE SECURITY OF ICS SCADA IN EUROPE

INDUSTRIAL CONTROL SYSTEMS

SUPERVISORY CONTROL AND DATA ACQUISITION

The Network and Information Security Directive

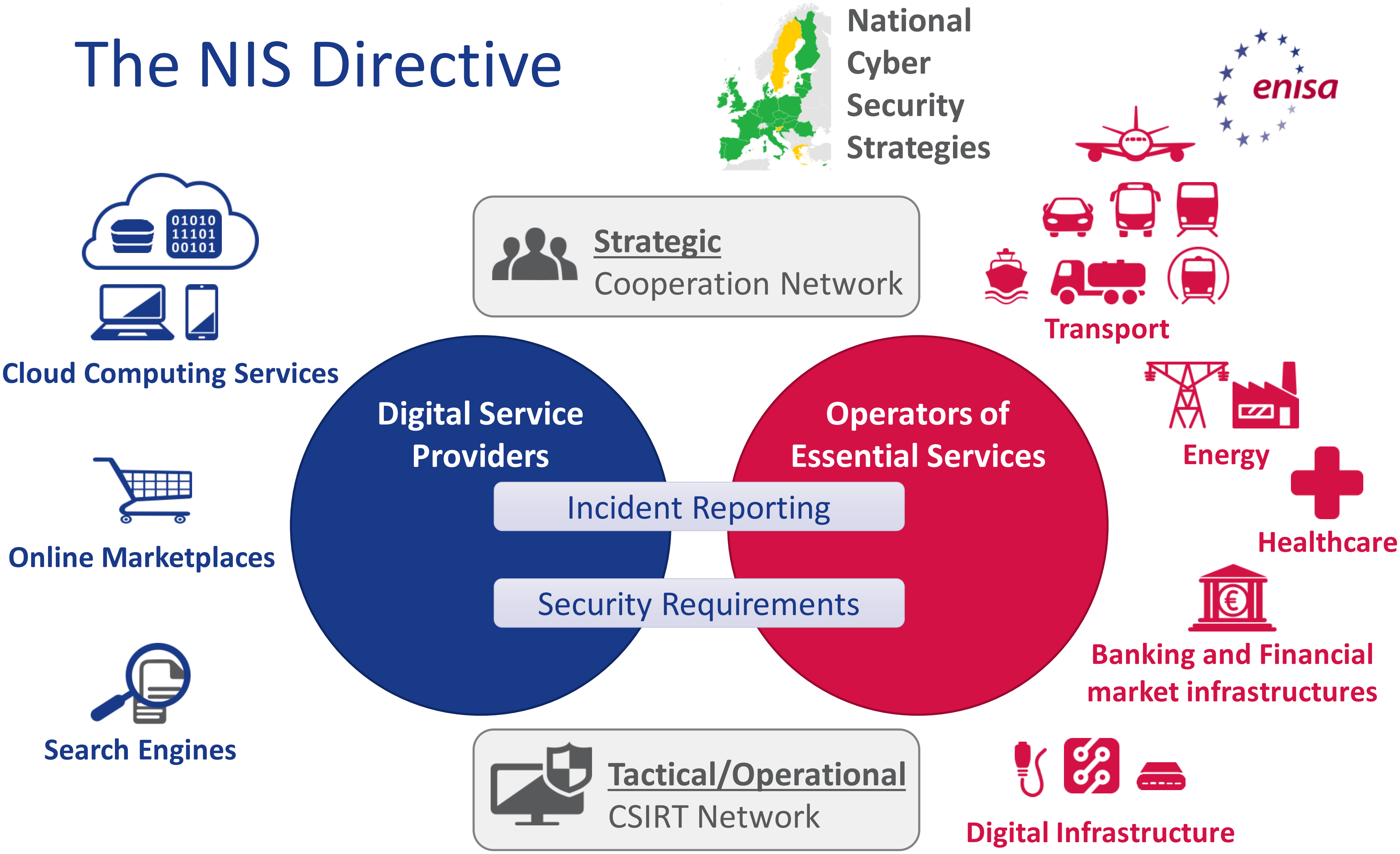
Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).

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

Strategic
Cooperation Network

Digital Service Providers

Operators of Essential Services

Incident Reporting

Security Requirements

Tactical/Operational
CSIRT Network

Cloud Computing Services

Online Marketplaces

Search Engines

Transport

Energy

Healthcare

Banking and Financial market infrastructures

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/