Enhancing the cyber security & resilience of transport infrastructure in Europe

European Union Agency for Network and Information Security

Securing Europe's Information society

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

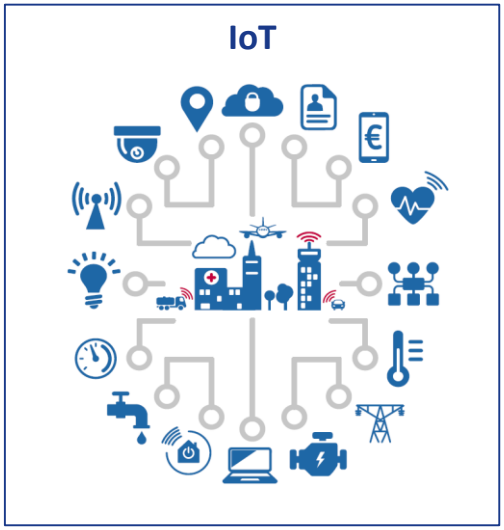
COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

Secure Infrastructure and Services



www.enisa.europa.eu/topics

What could possibly go wrong?

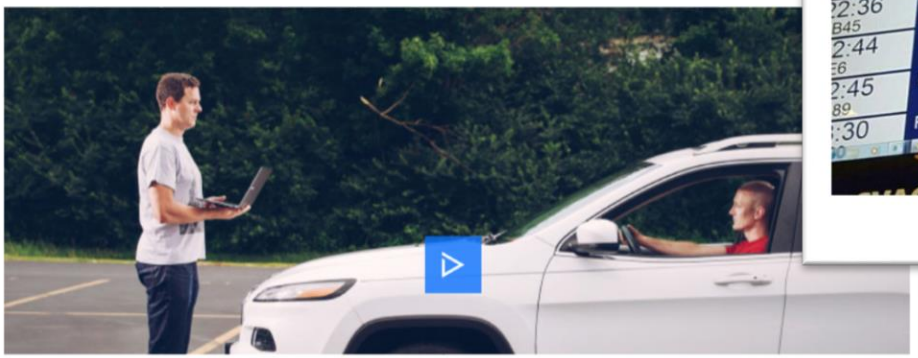
Hackers are holding San Francisco's light-rail system for ransom

'You Hacked, ALL Data Encrypted'

by Andrew Liptak | @AndrewLiptak | Nov 27, 2016, 4:16pm EST

SHARE TWEET LINKEDIN

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



News

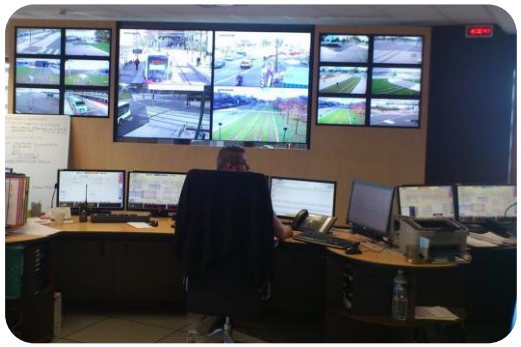
Cyber attack hits German train stations as hackers target Deutsche Bahn

share

1

An information monitor at a German train station displays the ransomware message CREDIT: @ZEICHENTATEN/TWITTER

Smart Cities as a “system of systems”



New and emerging risks

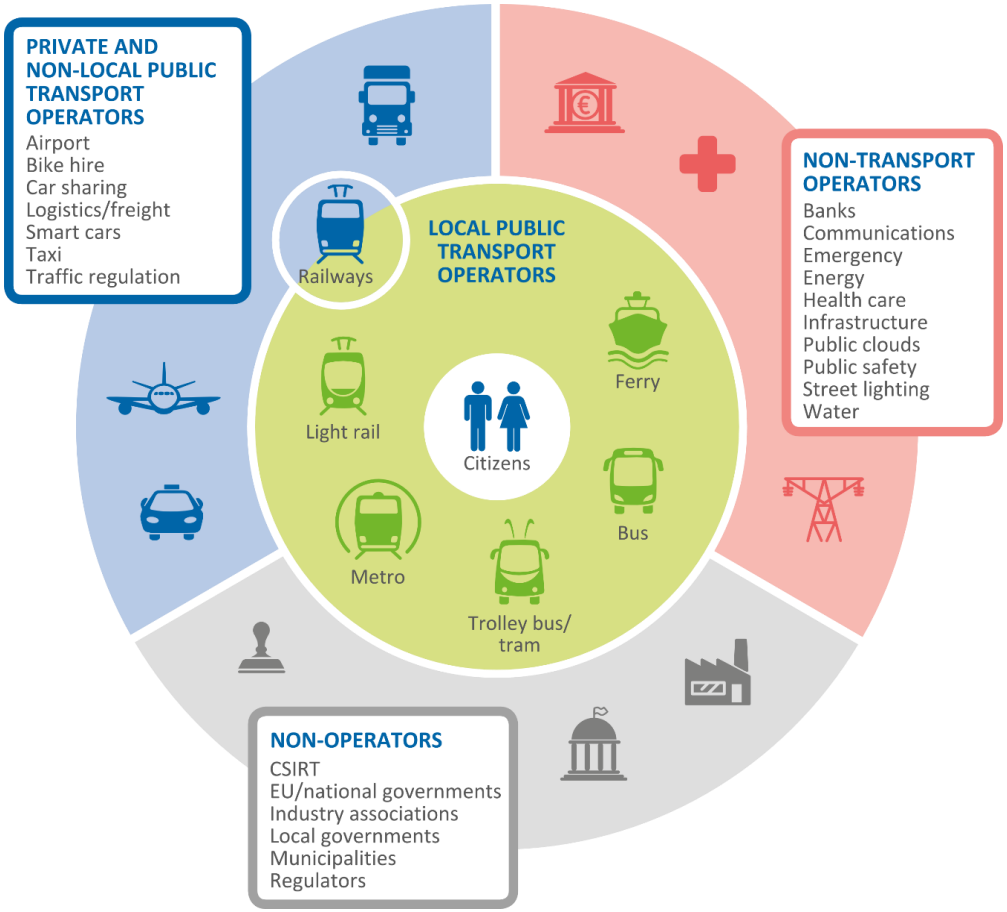
- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (legacy) systems
- Data exchange integrated into business processes

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 the transport infrastructure



2015 studies:

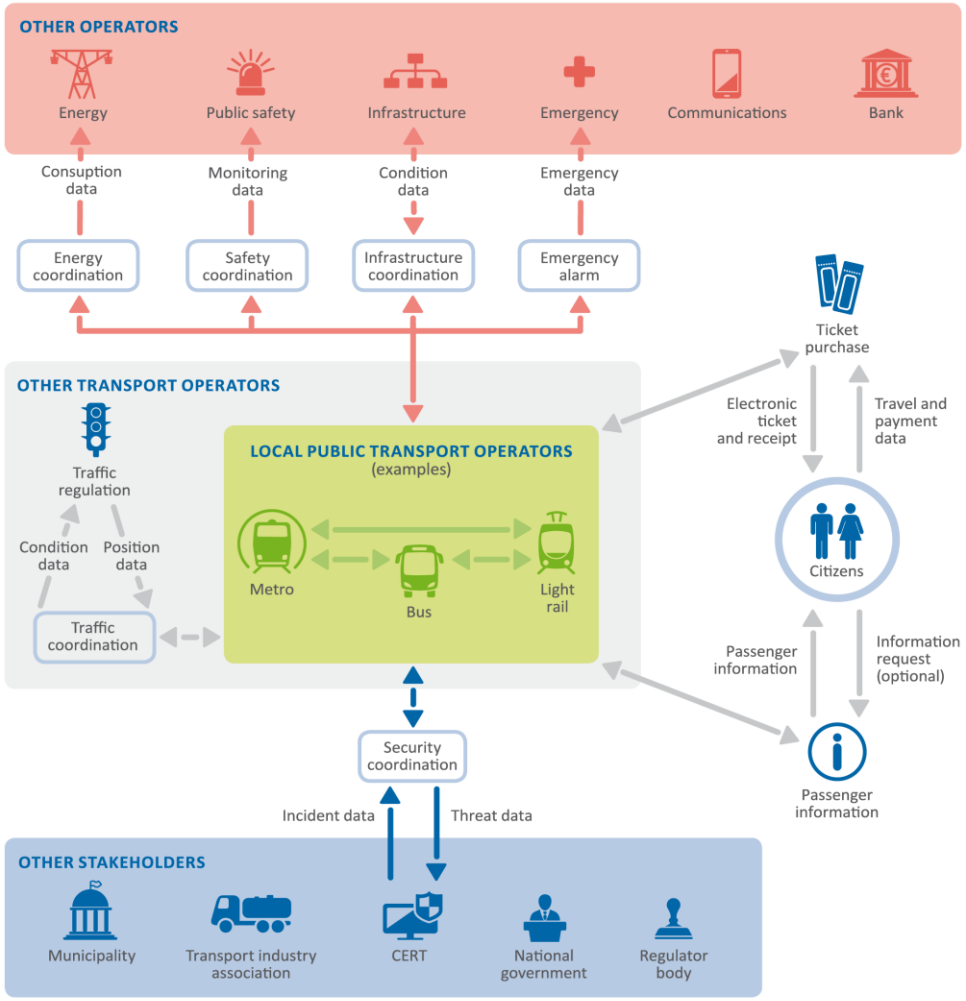
- **Architecture model of the transport sector in Smart Cities**
- **Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations**

Objectives

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

https://enisa.europa.eu/smartinfra

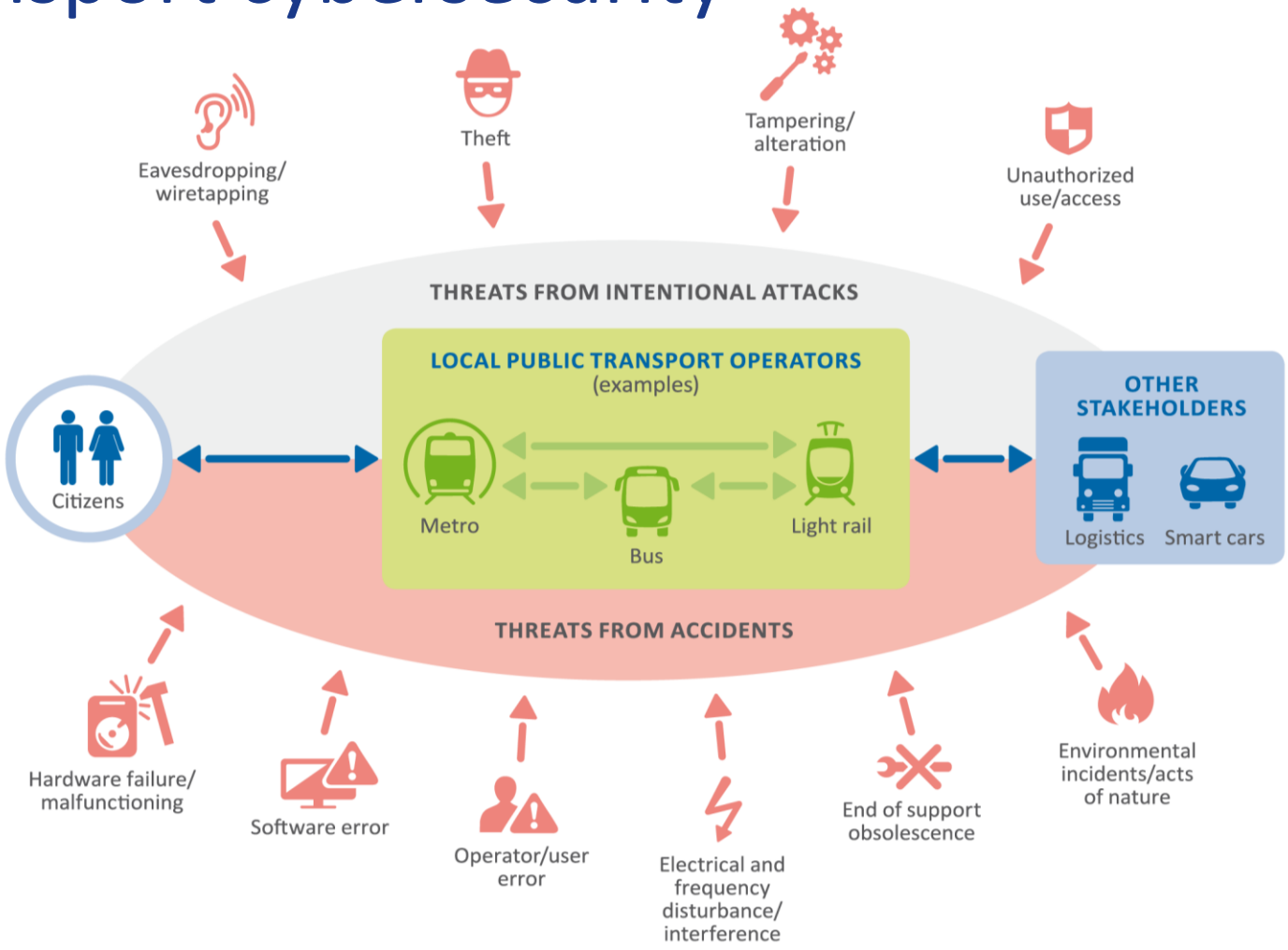
2015 study: Architecture model of the transport sector in Smart Cities



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

All studies are available for free download on ENISA website
https://enisa.europa.eu/smartinfra

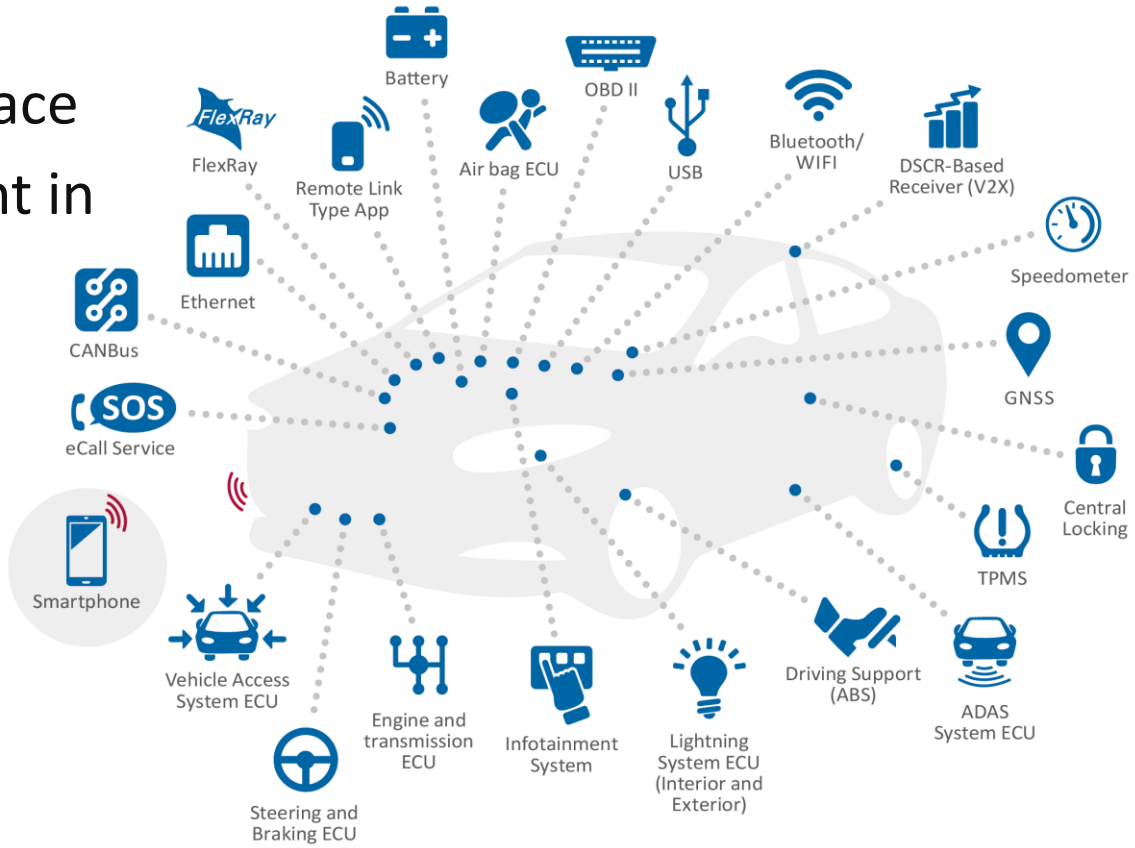
2015 study: Intelligent public transport cybersecurity



https://enisa.europa.eu/smartinfra

Smart Cars cybersecurity

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

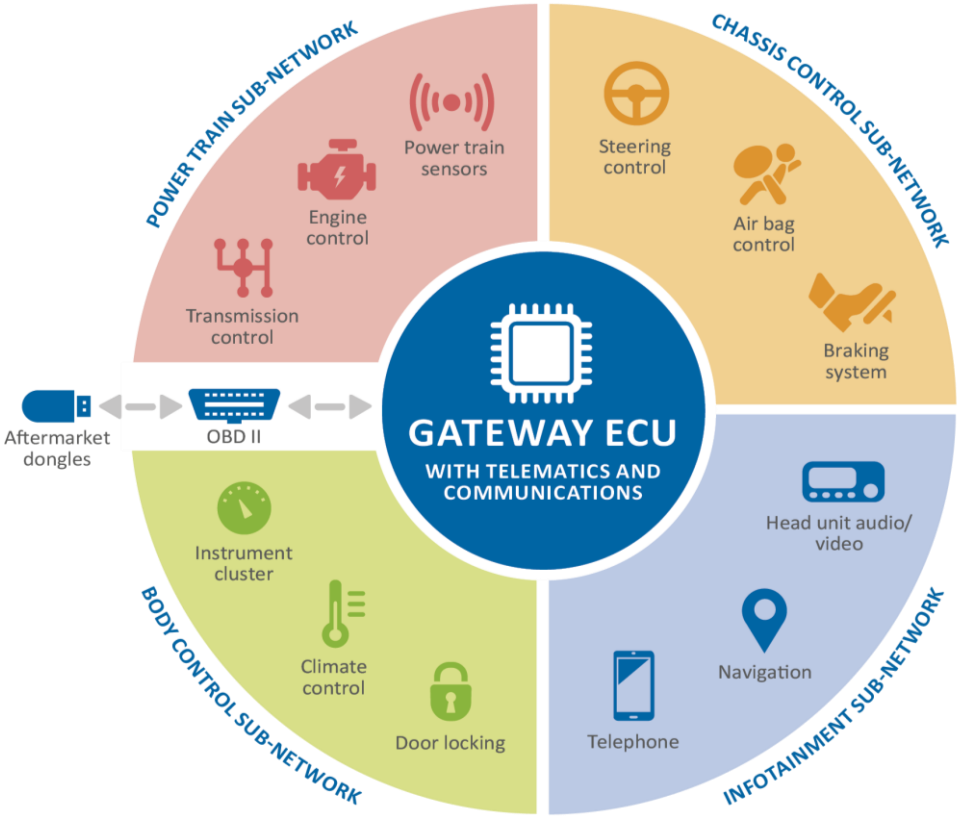


https://www.enisa.europa.eu/road

2016 study: Securing Smart Cars

Recommendations:

- Cybersecurity by design
- Improve information sharing amongst industry actors
- Achieve consensus on technical standards for good practices
- Clarify cyber security liability among industry actors



Download the report at
https://www.enisa.europa.eu/road

IoT + Airports = smart airports

List of past incidents

List of all possible threats

3 detailed description of attacks:

- Tampering with airport self-serving e-ticketing systems
- Network attack to the baggage handling
- Drone intercept as mobile vehicle for jamming and spoofing aircraft-airport and traffic control-airline communications

Attacks tools and techniques available

Security good practices

- Technical/tool-based good practices
- Policies and standards
- Organisational, people and processes

Gap Analysis

Recommendations

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

2016 study: Securing Smart Airports

Recommendations:

- Prioritizing cyber security for safety
- Establishing a clear airport cyber security posture and allocating cybersecurity experts and resources
- Constant revision of cyber security policies and practices based on good practices monitoring
- Implementing network-based, holistic risk and threat management policies and processes for cyber security

Download the report at
https://www.enisa.europa.eu/air

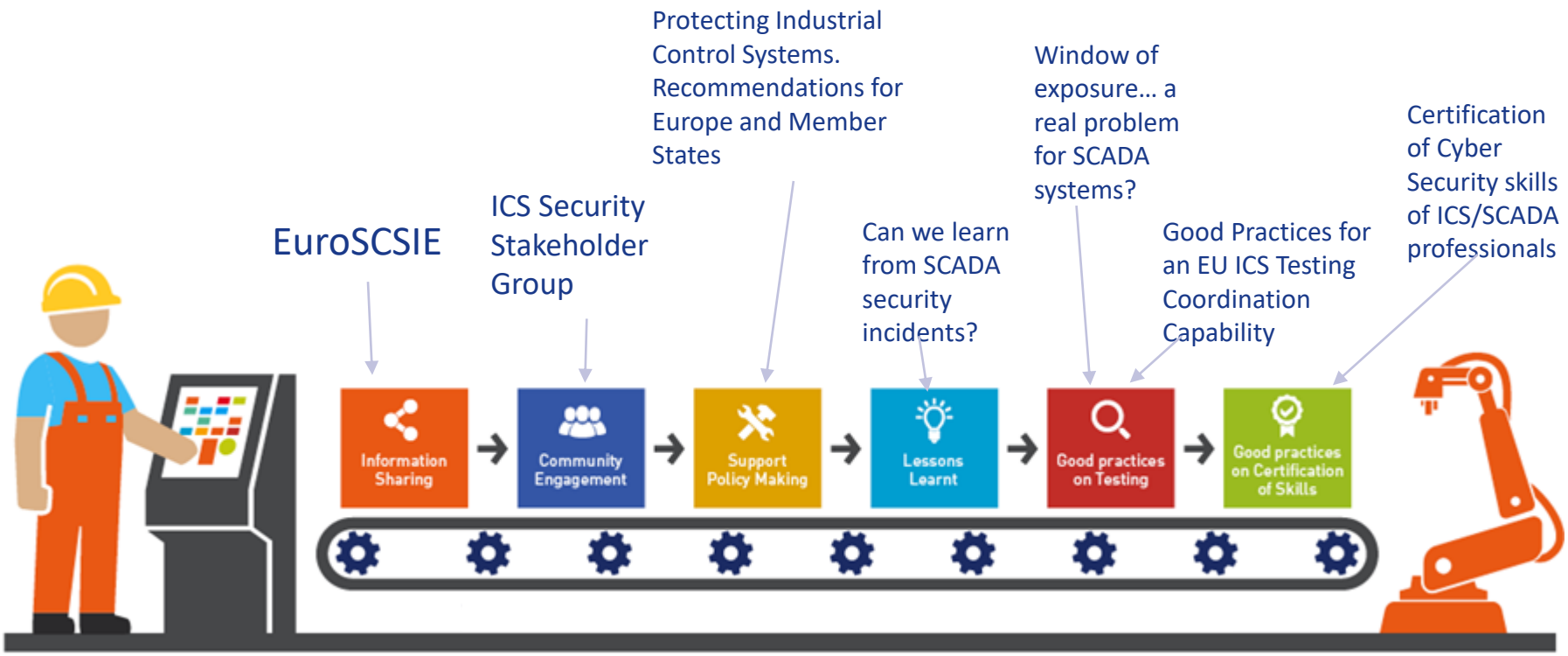
ENISA training on aviation cybersecurity co-organized with EASA

EASA, in collaboration with ENISA, will host the first ENISA training on cybersecurity in aviation on the **20th and 21st of November in Brussels**:

- overview of the cybersecurity threat landscape for aviation's information infrastructures,
- introduction of the Network and Information Security Directive
- first ENISA training on Incident Handling, customized for the aviation sector.

The training is a **customization of ENISA trainings** based on the 2016 ENISA report on threat modeling and security measures for airports and relevant stakeholders "**Securing smart airports**".

Cybersecurity for ICS SCADA



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

What you can do from today:

- Consider the cybersecurity impact on safety
- Include cyber security in your governance model in order to define liabilities
- Ensure you consider cyber security in all stages of the life cycle of products and services
- Consider network connectivity and interdependencies and cascading effects
- Start reusing existing good practices from other sectors, for example for SCADA

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/iot