ENISA efforts on Securing Smart Infrastructures and Internet of Things

Dr Apostolos MALATRAS

Secure Infrastructure and Services Unit, ENISA

X Congress of ISACA Valencia, 27.10.2016

European Union Agency for Network and Information Security

Outline

Overview of ENISA

- Activities
- Secure Infrastructure and Services

IoT Security

- Significance
- Challenges

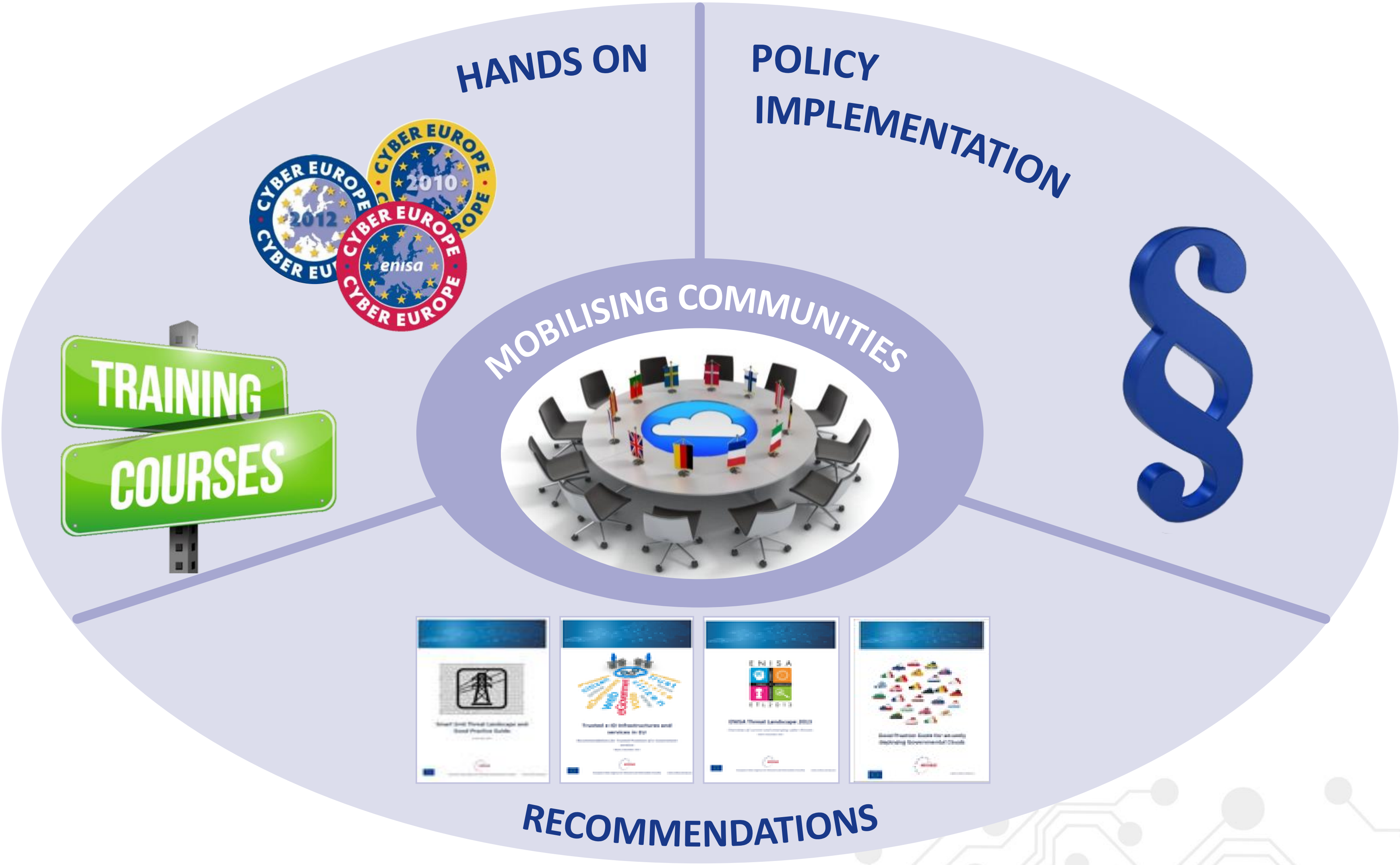
ENISA and IoT Security

- Smart Homes
- Smart Cars
- Smart Airports
- Smart Infrastructures
- Smart Hospitals

Discussion

Securing Europe’s Information society

Positioning ENISA activities



HANDS ON

POLICY IMPLEMENTATION

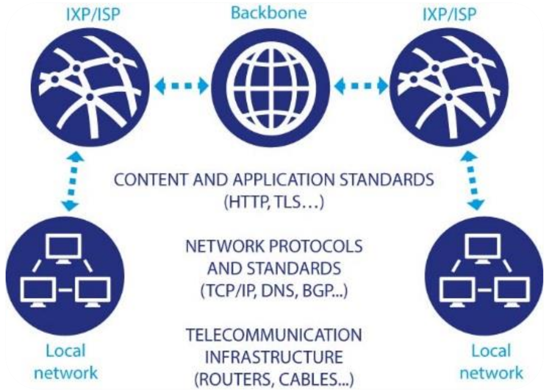
MOBILISING COMMUNITIES

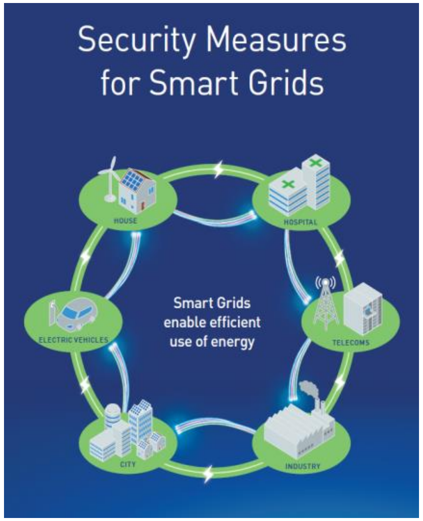
RECOMMENDATIONS

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



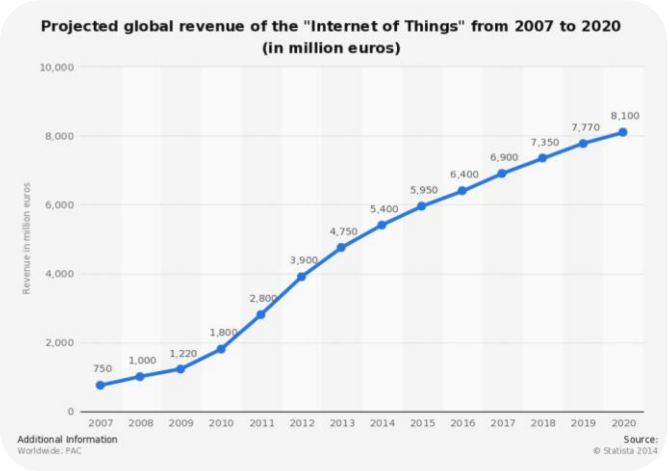


Transport

eHealth and Smart Hospitals

Finance

Everything is connected



Projected global revenue of the "Internet of Things" from 2007 to 2020 (in million euros)

Additional Information
Worldwide; PAC

Source:
© Statista 2014

Manufacturers have an economic interest

- Data collection and processing
- New business models: data reseller, targeted ads, etc.
  - Competitors do IoT, hence we must do IoT
  - Competitors don’t do IoT, let’s be the first one!

Customers have their own interests (do they?)

- Connectivity is needed, mobility is important
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities than non-IoT product, reasonable price
- Non-connected version is not available

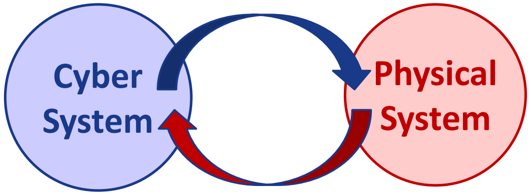
Connected products are the new normal

Why IoT security matters?

Security of IoT is important

- Rapid technological evolution
- Reliance on third-party components, hardware and software
- Many vulnerabilities with impact on EU citizens
- Security required for the whole lifecycle of IoT products and services

IoT security is currently limited



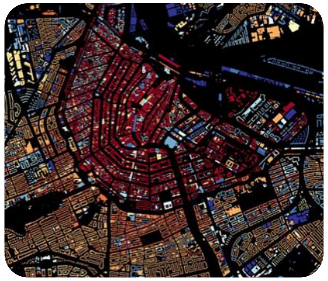
- Investments on security are limited
- Functionalities before security
- Real physical threats with risks on health and safety
- No legal framework for liabilities
- Security is difficult to assess (multiple dependencies, 3rd-party APIs, etc.)

IoT brings smartness and new security challenges

IoT at the heart of Smart Infrastructures

Current challenges of IoT

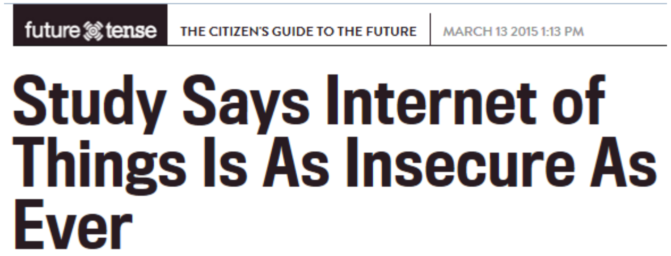
- Capacity-limited devices
- Data exchange with other devices and remote services
- No regulation on data ownership
- Interaction with the physical world (*cyber-physical systems*)



Threats and risks of IoT devices and services

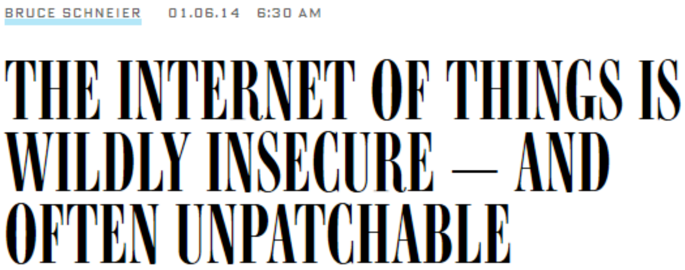
- Threats are diverse and evolve rapidly
- Several IoT manufacturers are not expert in security
- Data collection and processing may be unclear to users
- Impact on citizens' health, safety and privacy

An increasing number of threats



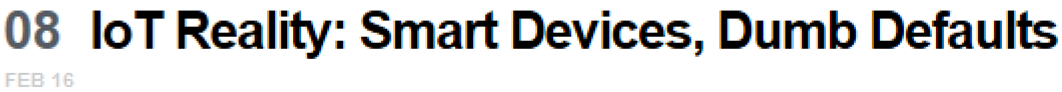
future tense | THE CITIZEN'S GUIDE TO THE FUTURE | MARCH 13 2015 1:13 PM

Study Says Internet of Things Is As Insecure As Ever



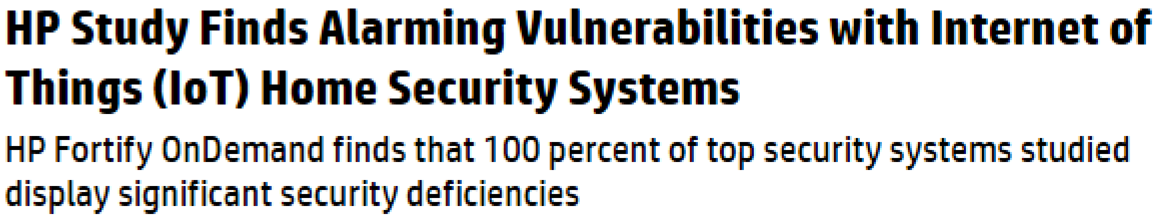
BRUCE SCHNEIER 01.06.14 6:30 AM

THE INTERNET OF THINGS IS WILDLY INSECURE — AND OFTEN UNPATCHABLE



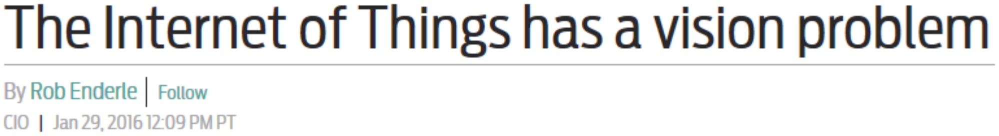
08 FEB 16

IoT Reality: Smart Devices, Dumb Defaults



HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems

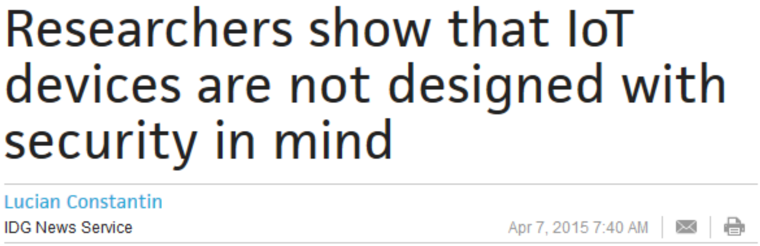
HP Fortify OnDemand finds that 100 percent of top security systems studied display significant security deficiencies



The Internet of Things has a vision problem

By Rob Enderle | Follow

CIO | Jan 29, 2016 12:09 PM PT

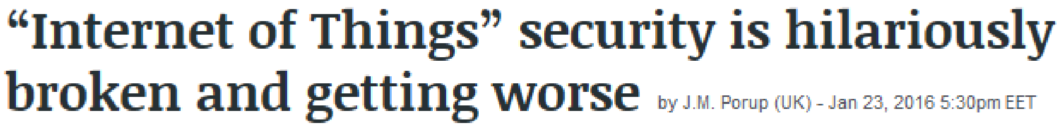


Researchers show that IoT devices are not designed with security in mind

Lucian Constantin

IDG News Service

Apr 7, 2015 7:40 AM



“Internet of Things” security is hilariously broken and getting worse

by J.M. Porup (UK) - Jan 23, 2016 5:30pm EET

Threat taxonomy for IoT

Failures
Malfunctions

Acts of Nature
Disasters

Physical
attacks

Unintentional damage
(accidental)

Nefarious Activity
Abuse

Damage/Loss
(IT Assets)

Outages

Eavesdropping
Interception
Hijacking

Legal

Insider threat

ENISA and IoT security

Smart Cities

SCADA
and Industry 4.0

Smart Homes

eHealth

Intelligent
Public Transport

Smart Cars

Smart Airports

Definition of the perimeter

- Devices
- Data exchange (including network infrastructure)
- Local and remote services (*e.g.* Cloud, etc.)

ENISA develops expertise to secure IoT

- Evaluation of threats
- Promotion of security good practices
- Stakeholders engagement
- Awareness raising
- Community expert groups
- Liaison with policy makers

ENISA provides guidance to secure IoT against cyber threats

Smart Cities as a "system of systems"

New and emerging risks

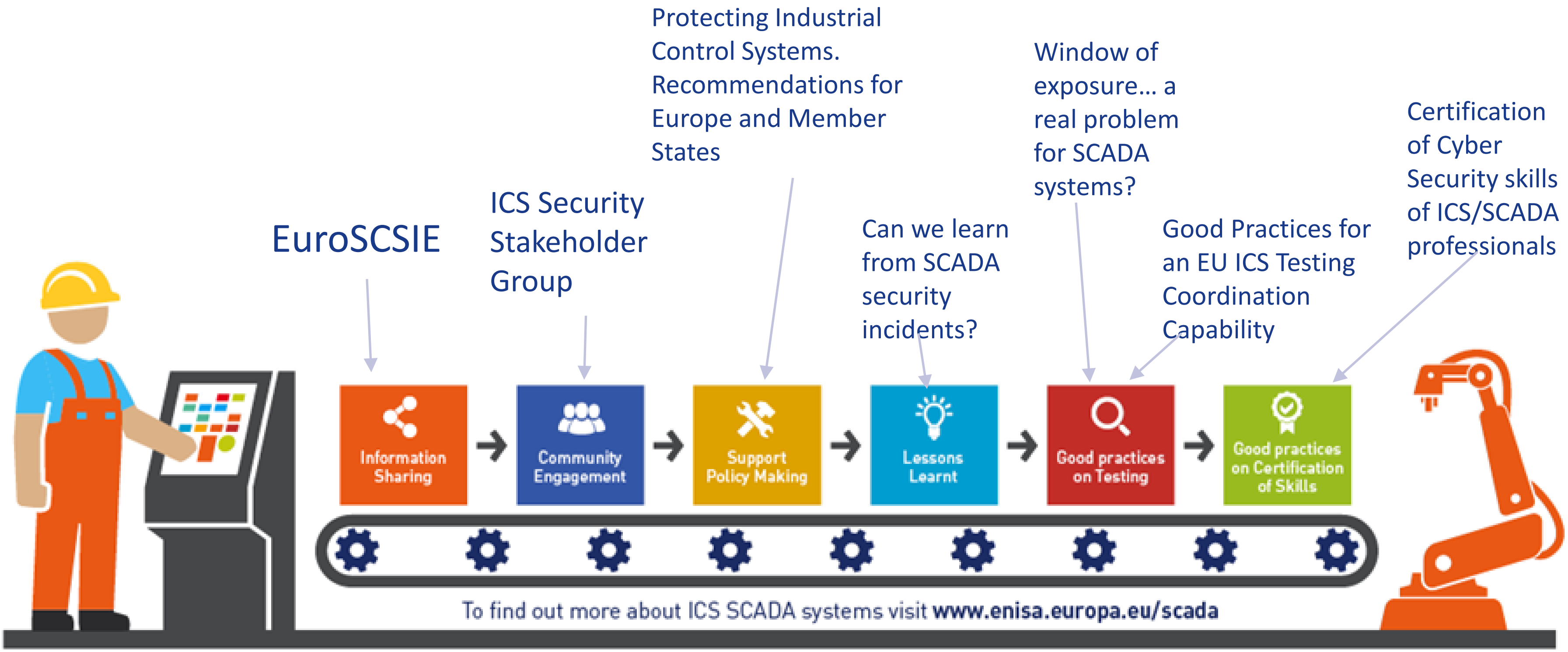
- ICT Dependency is generalised
- Cohabitation between IP-connected systems and older (legacy) systems
- Data exchange integrated into business processes

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

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?

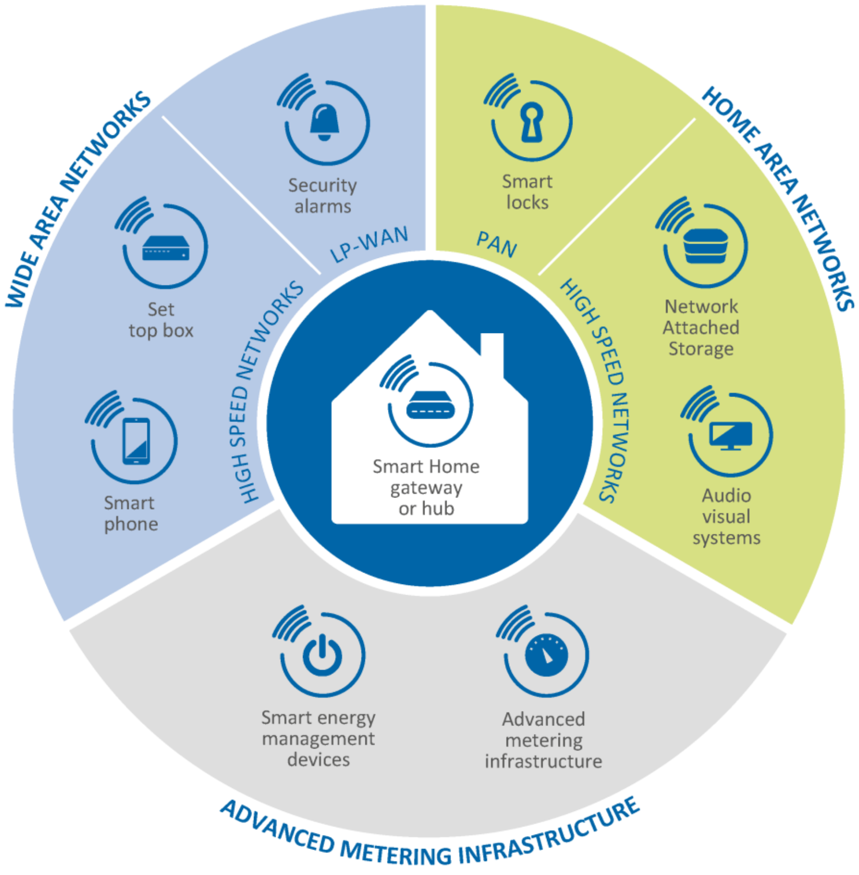
Good Practices for an EU ICS Testing Coordination Capability

Certification of Cyber Security skills of ICS/SCADA professionals

To find out more about ICS SCADA systems visit **www.enisa.europa.eu/scada**

Latest study on ICS SCADA maturity models released in December 2015

IoT in Smart Homes



Connected devices

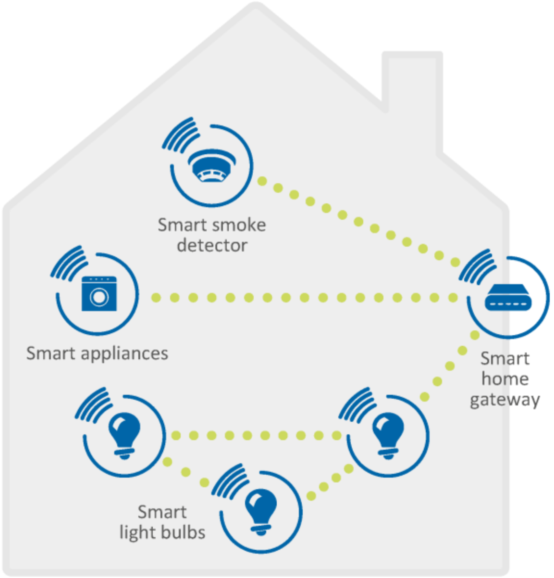
- Data acquisition and processing
- Actions on the environment

Connected users

- Interface for command & control
- Adaption to the environment

Towards an automation of the home for an improved quality of life (comfort, energy reduction…)

Securing Smart Homes



Security concerns

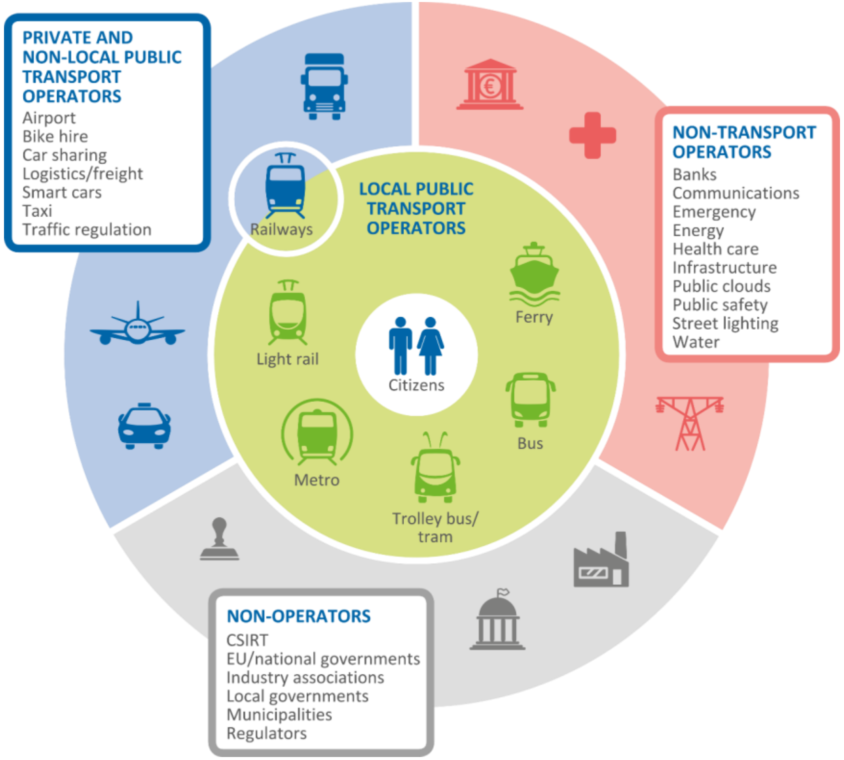
- Manufacturers don’t invest in security
- Security and privacy are closely linked
- Difficult to secure the entire lifecycle of products

ENISA proposes to:

- Establish security procurement guidelines
- Define a framework to evaluate the security of products
- Support security-driven business models

Smart Homes present a real risk to the safety and privacy of citizens

IoT in Intelligent Public Transport



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

Securing Intelligent Public Transport

ENISA good practices

- Secure organisation, people, processes
- Secure third-party dependencies
- Applicable before, during or after an incident

enisa
Cyber securi
An architecture mod
DECEMBER 2015
enisa
Cyber Security and Resilience of Intelligent Public Transport
Good practices and recommendations
DECEMBER 2015

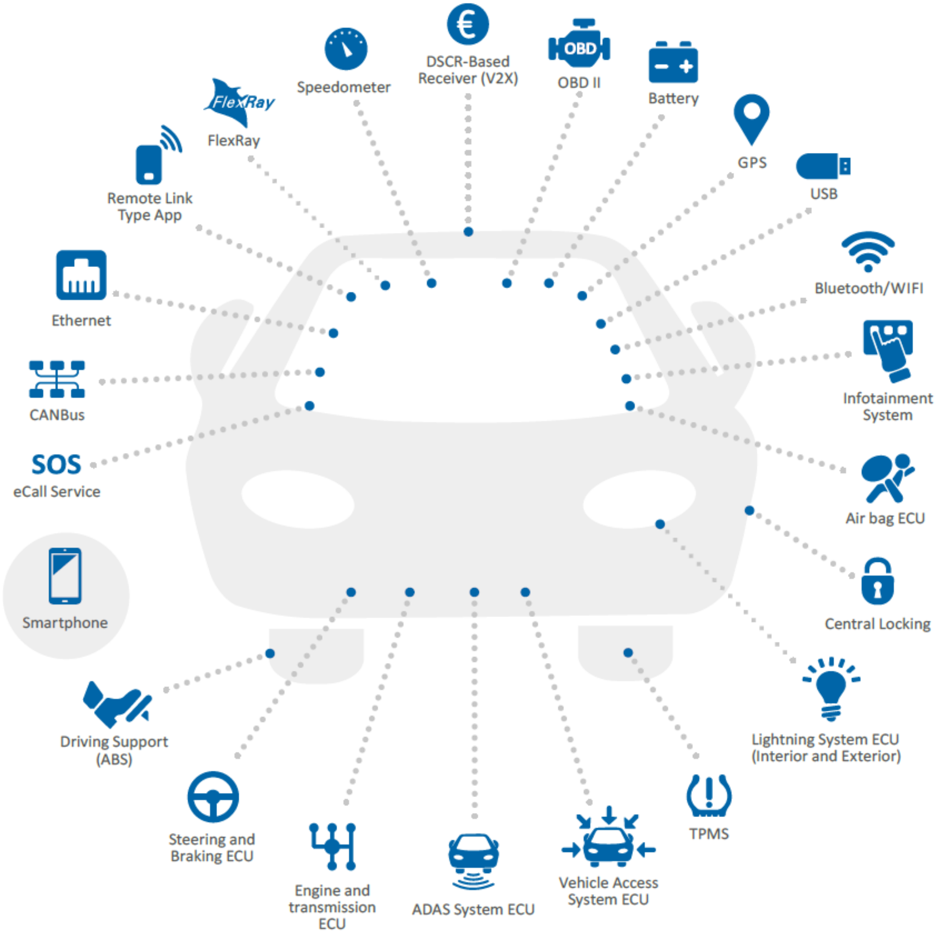
ENISA recommends operators and deciders to:

- Develop a clear definition of security requirements
- Integrate cyber security in corporate governance
- Promote public/private collaboration on cyber security

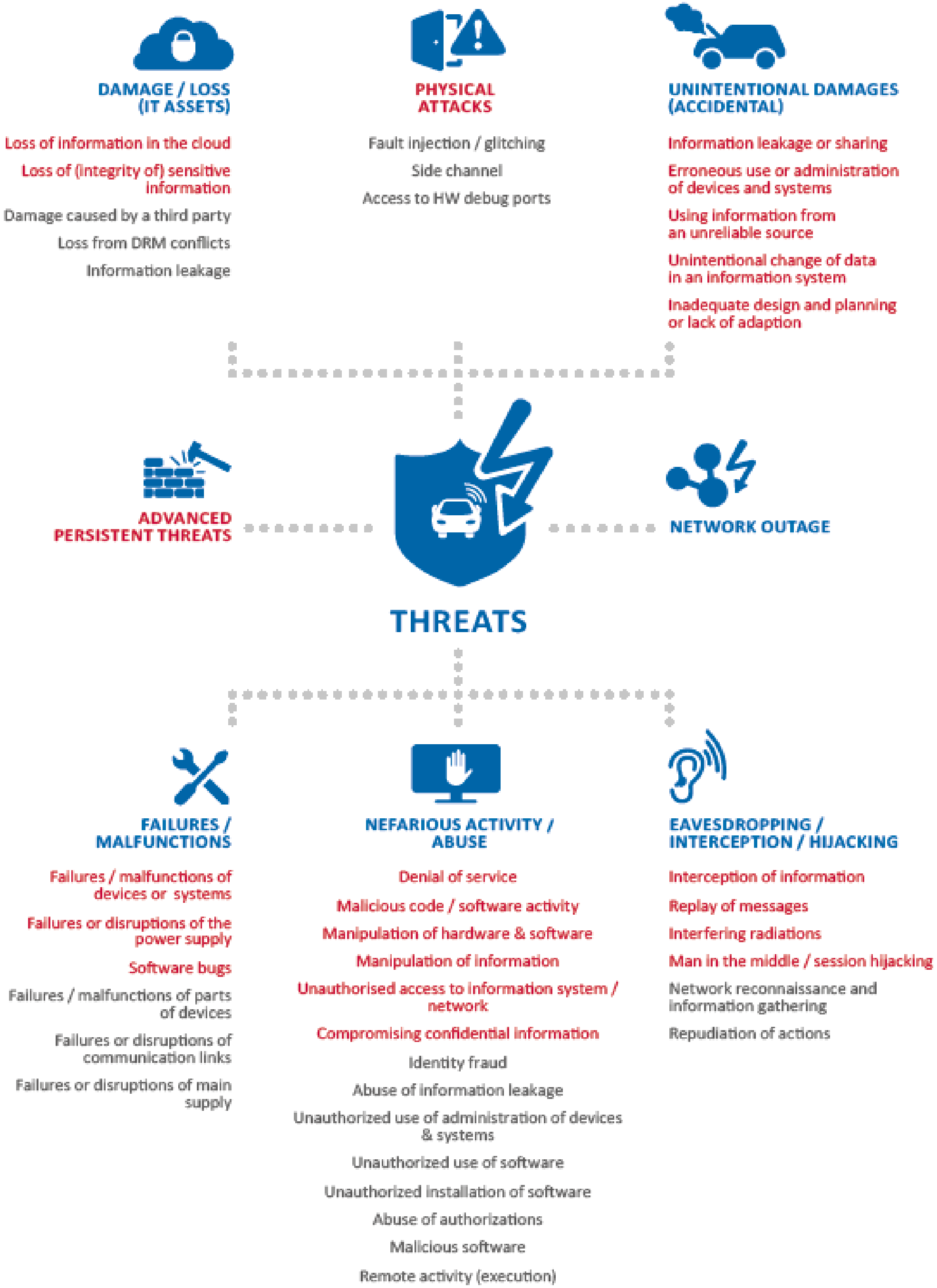
To be efficient, good practices require support by all actors (manufacturers/vendors/service providers/other operators…)

IoT in Smart Cars

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



Smart Cars 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

THREATS

NETWORK OUTAGE

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

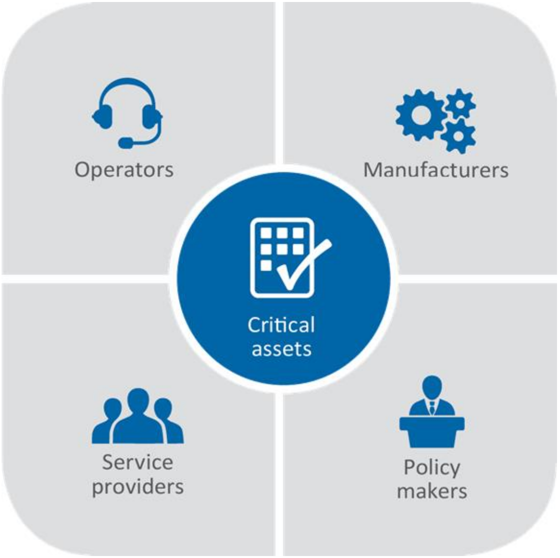
Interfering radiations

Man in the middle / session hijacking

Network reconnaissance and information gathering

Repudiation of actions

Securing Smart Cars



Importance of security for safety

- Several threats
- Manufacturers need guidance to act
- ENISA to identify and promote good practices

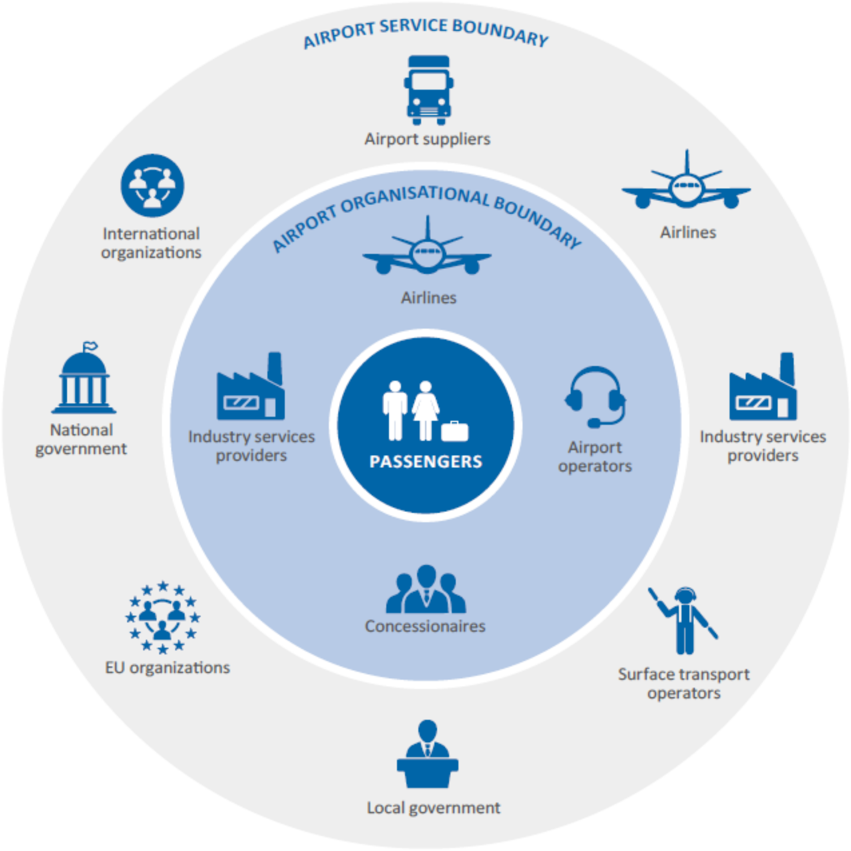
Cyber security for smart cars is gaining attention

- Lots of security guidelines in development
- Standardisation effort is too long
- Lack of expertise safety+security with a vehicular background

Secure Smart Cars today for safer autonomous cars tomorrow

IoT in Smart Airports

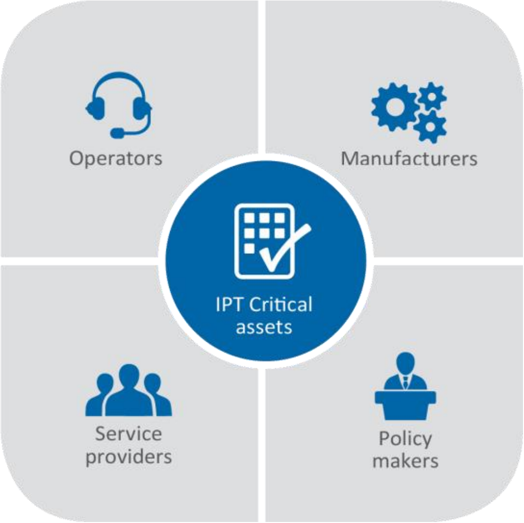
The objective of this study is to improve the security and resilience of airports and air traffic control to prevent disruptions that could have an impact on the service being delivered and on the passengers.



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

Securing Smart Airports



ENISA recommendations

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

Key recommendations (excerpt)

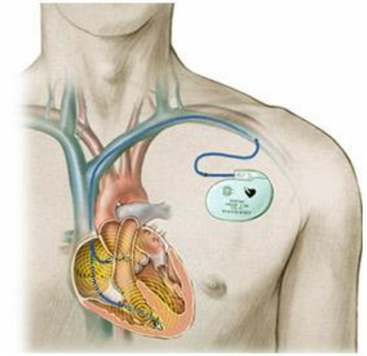
- Promote collaboration on cyber security across Europe
- Integrate security in business processes
- Develop products integrating security for safety

Cyber security for Transport requires *a global effort*

IoT in Hospitals and eHealth

Security concerns

- Protect patient confidentiality
- Improve security and resilience of hospitals information systems
- Protect connected critical assets with an impact on health



Hacking the Heart

ENISA proposes to:

- Identify common cyber security threats and challenges
- Present mitigation measures to address them
- Support pilots in hospitals across the EU

ENISA actions in 2016

ENISA sectorial guidance

- Understand threats and assets
- Highlight security good practices in specific sectors
  - Smart Hospitals
  - Smart Cars
  - Smart Airports
- Provide recommendations to enhance cyber security

Publications Out Soon

Security evaluation of IoT frameworks

- Assess security measures in IoT frameworks and APIs
- Understand common security aspects between sectors

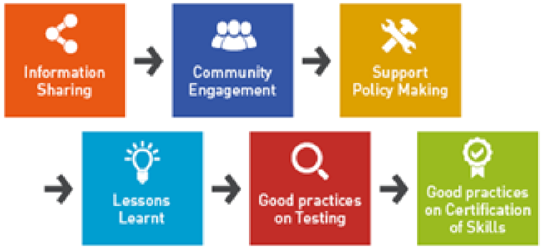
ENISA expert groups

- Engage with communities
- Sectorial groups (Smart Cars, Intelligent Public Transports, eHealth)

Collaborations with the European Commission

All stakeholders must collaborate to enhance IoT security

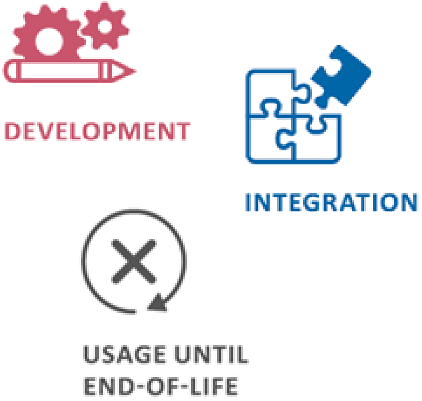
Recommendations to secure IoT



Information Sharing → Community Engagement → Support Policy Making → Lessons Learnt → Good practices on Testing → Good practices on Certification of Skills

Generic good practices

- Raise awareness of manufacturers and suppliers
- Define security management at organisational level
- Develop information exchange on threats and risks
- Promote a common cyber security framework
- Reuse existing good practices from other domains



DEVELOPMENT

INTEGRATION

USAGE UNTIL END-OF-LIFE

ENISA to provide guidance to secure the lifecycle of IoT

- Develop cross-sector baseline security measures
- Develop sectorial good practices
- Foster information exchange through ENISA Experts Groups

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

Conclusion

IoT security in general

- Security by default is a must
- IoT vendors must secure the entire lifecycle of products
- Harmonisation of minimum security features needed

> “ **Protect**
>
> **Cooperate**
>
> **Exchange** ”

ENISA efforts

- Focus on security for safety
- Engage and foster collaboration with manufacturers, developers, users
- Reuse IoT security good practices from other domains
- Secure the entire lifecycle of products and services

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu