The road to secure Smart Cars
ENISA approach

Dr. Cédric LÉVY-BENCHETON | Expert in Network and Information Security

TROOPERS16 | Heidelberg | 17 March 2016

Summary

Introduction

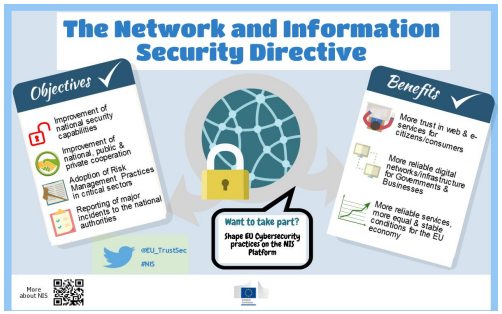
Positioning ENISA activities

Emerging Threat Environment

- Significant physical disasters affecting CIIs
- Complex networks and services
- Low quality of software and hardware
- Asymmetric threats allowing remote attacks to CII
- Increasing organised cybercrime and industrial espionage
- Lack of international agreements and regimes
- Lack of well functioning, international operational mechanism

EU Policy Context

ENISA II – new mandate ☑



The NIS Directive

EU's CIIP action plan ☑

eIDAs Directive – article 19 ☑

Telecom Package – Article 13a, Article 4 ☑

EU Cyber Security Strategy (COM) ☑

EU Cloud Computing Strategy and Partnership (COM) ☑

The NIS Directive

National Cyber Security Strategies

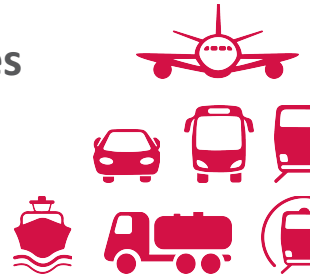
enisa

Cloud Computing Services

Online Marketplaces

Search Engines

Strategic Cooperation Network



Transport

Digital Service Providers

Operators of Essential Services

Incident Reporting

Security Requirements

Energy and Water

Healthcare

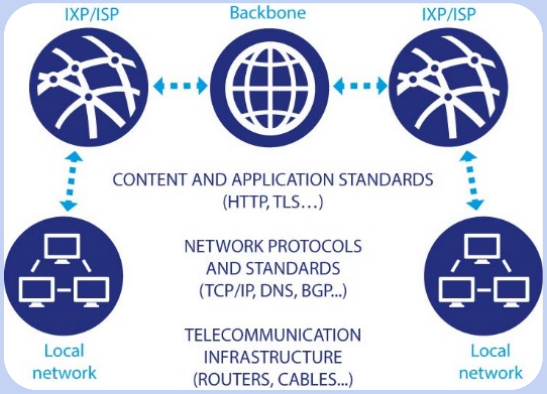
Banking and Financial market infrastructures

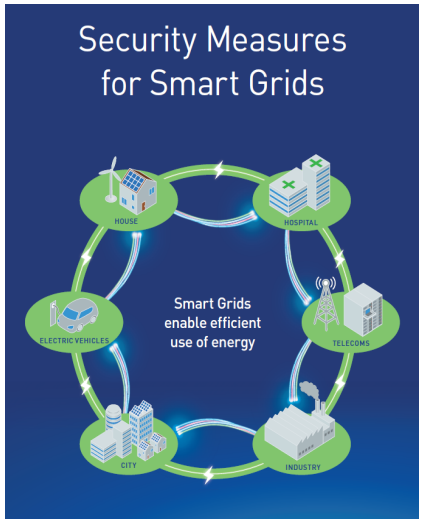
Digital Infrastructure

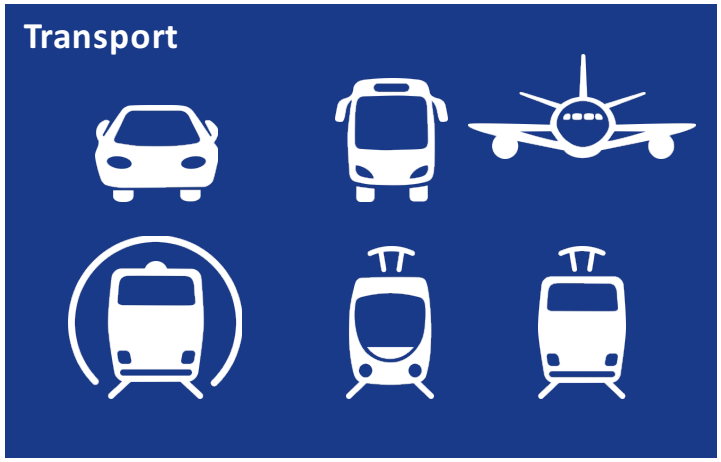
Tactical/Operational CSIRT Network

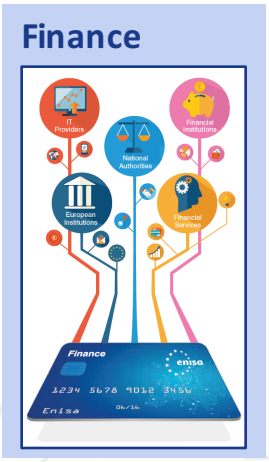
Secure Infrastructure and Services

Communication networks: Critical Information Infrastructure and Internet Infrastructure

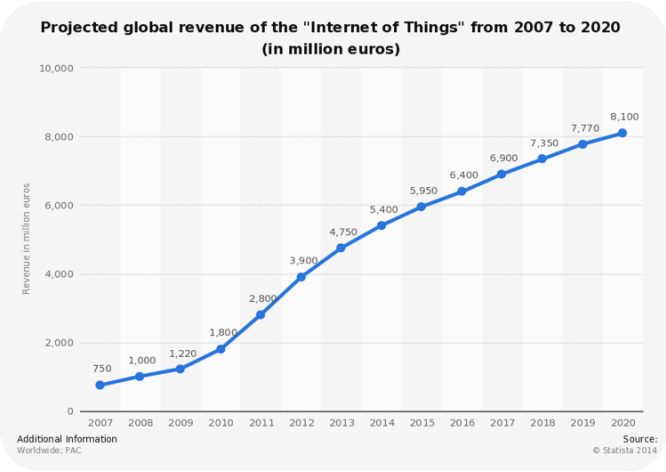








Everything becomes connected



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?)

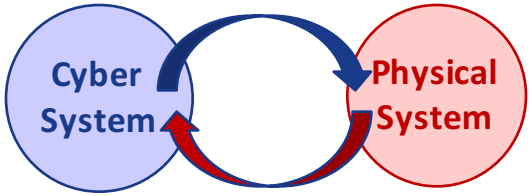
- Connectivity is needed, mobility is important
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities than non-IoT product, reasonable price
- Non-connected version is not available

Connected products are the new normal

Why IoT security matters?

No device is fully secured

- Reliance on third-party components, hardware and software
- Dependency to networks and external services
- Design of IoT/connected devices
- Vulnerabilities in protocols



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

IoT brings smartness and new security challenges

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

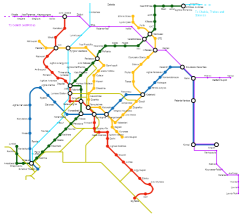
ENISA and IoT security

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 provide guidance to secure IoT against cyber threats

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

On the road to secure Smart Cars

Smart Cars integrate IoT in Cars

Smart Cars improve drivers and passengers experience

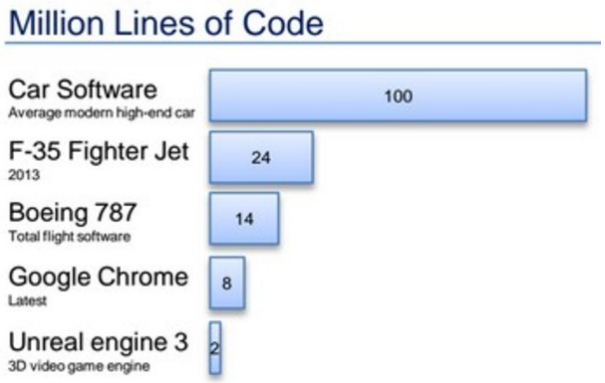
- Safety (collision avoidance, eCall)
- Convenience (keyless, assisted parking)
- Entertainment (On-board multimedia, Internet access)
- Economical advantage (adaptive insurance)

Some advantages of Smart Cars

- Statistics for drivers and third-parties
- Embedded Internet access
- Satisfaction of driving "the latest technology"

Smart Cars are leading the adoption of IoT

Challenges of Smart Cars



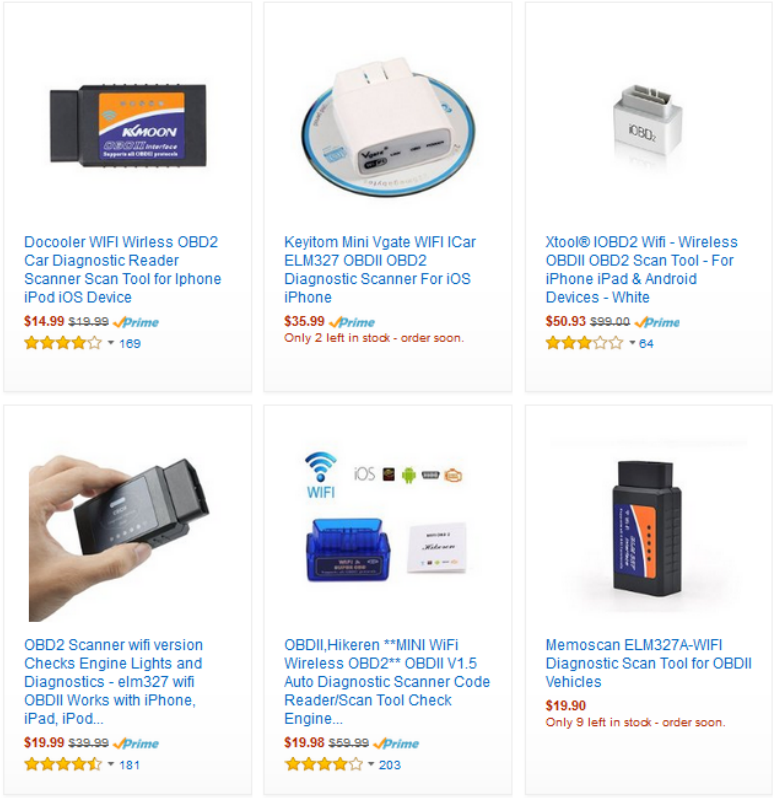
Technical challenges

- Reliance on third-party components, hardware and software: “over 100 M lines of code”
- Lack of basic security for cars (CAN Bus, ECU authentication)
- Patching a car is more difficult than it seems

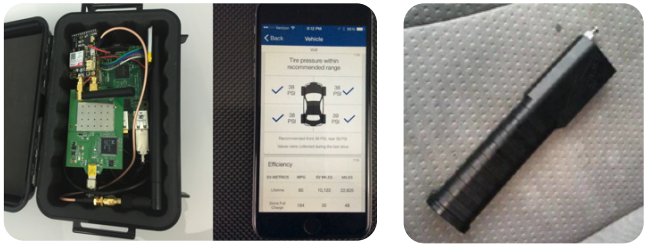
Safety challenges

- Liabilities are unclear
- Data exchange with external providers with no experience in car safety
- Integrity of messages which influence driving?

More challenges linked to Smart Cars



Low price of OBDII Wi-Fi scanners



Easy-to-open keyless cars

Israeli Soldiers Get Lost Using Waze App, and Clashes Follow
By DIAA HADID MARCH 1, 2016

Inaccurate Sat-Nav

OCT 9, 2015 @ 11:48 AM 5,031 VIEWS

Volvo Will Accept Liability For Its Self-Driving Cars

Unclear liabilities

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs

Wednesday, 24 February 2016

Unsecure API

Possible solutions

ENISA to highlight good practices

- Understand the threats and the critical assets
- Secure the entire life cycle of smart cars
- Security measures go beyond technical (organisation, policy)

Possible solutions from other IoT sectors

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

Secure Smart Cars to ensure the safety of citizens

Cyber Security initiatives in the EU

European Commission

- Collaborative ITS Deployment Platform (C-ITS)
- Alliance for IoT Innovation (AIOTI)

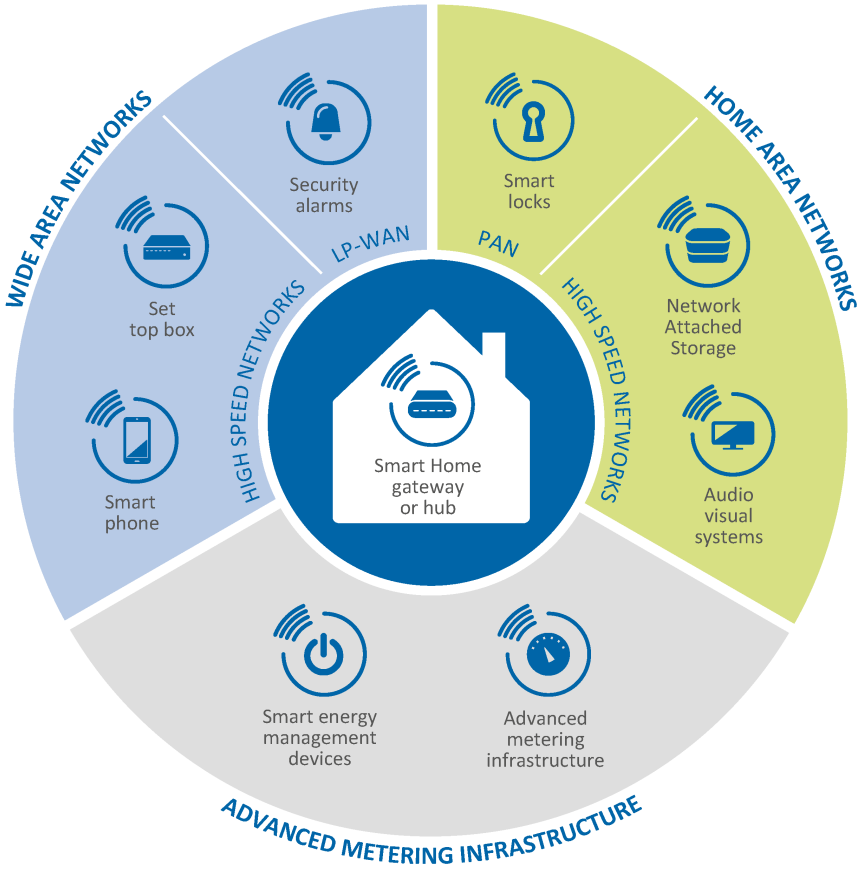
ENISA CaRSEC Expert Group

- Exchange on threats, challenges, solution
- Contribute and review ENISA study
- Participation is free and voluntary

Apply to ENISA CaRSEC: https://ec.europa.eu/eusurvey/CaRSEC
Terms of References available on ENISA website

Securing IoT in Smart Homes

What is a Smart Home?



Connected devices

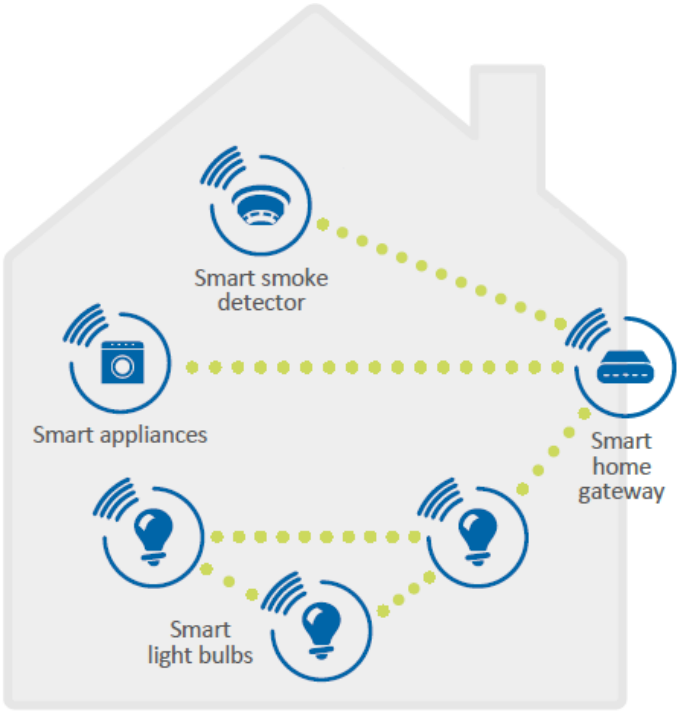
- Data acquisition and processing
- Actions on the environment

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…)

Challenges to the Smart Home



Challenges for products and services

- Manufacturers, retailers are not expert in security
- End-users are not security administrators
- Certification not needed by the industry
- Functionalities before security
- No incident reporting schemes

Challenges linked to the connectivity

- Data exchange with remote services, some not hosted in the EU
- Resilience in case of outage?
- Ubiquitous connectivity on multiple networks

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

Update on threats

Several baby monitors vulnerable to hacking, cybersecurity firm warns

The Associated Press Posted: Sep 02, 2015 1:53 PM ET | Last Updated: Sep 02, 2015 2:13 PM ET

WEDNESDAY, FEBRUARY 17, 2016

Remotely Disabling a Wireless Burglar Alarm

By Andrew Zonenberg @azonenberg

Reuse of Cryptographic Keys Exposes Millions of IoT Devices: Study

By Eduard Kovacs on November 25, 2015

Hello Barbie Doll Vulnerable to Hackers

By Robert Hackett @rhhackett DECEMBER 4, 2015, 8:43 PM EST

VTech hack: Data of 6.4M kids exposed

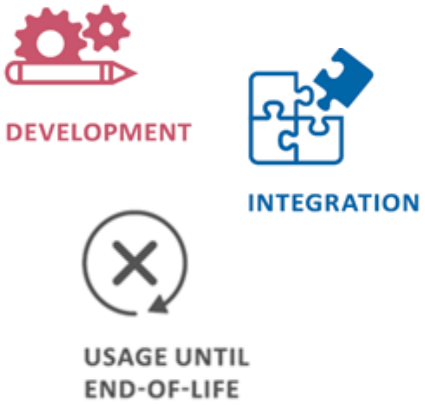
Wednesday, 2 Dec 2015 | 12:08 AM ET

Your kids are not safe

Securing Smart Homes

Good practices

- Secure the entire lifecycle of IoT devices and services
- Do not use in-house encryption!
- Rely on Smart Home architecture for security



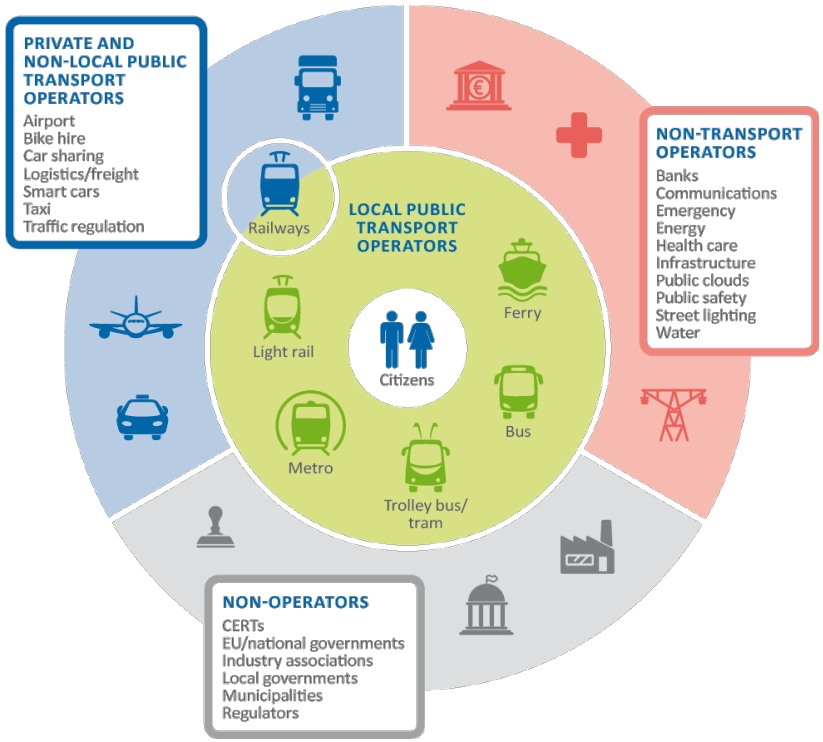
ENISA recommends all actors of Smart Homes to:

- Support security-driven business models
- Integrate cyber security in R&D projects
- Establish an evaluation framework for security

All stakeholders must cooperate to enhance IoT security in Smart Homes

Securing IoT in Intelligent Public Transport

Intelligent Public Transports



Improve the Quality of Life of citizens

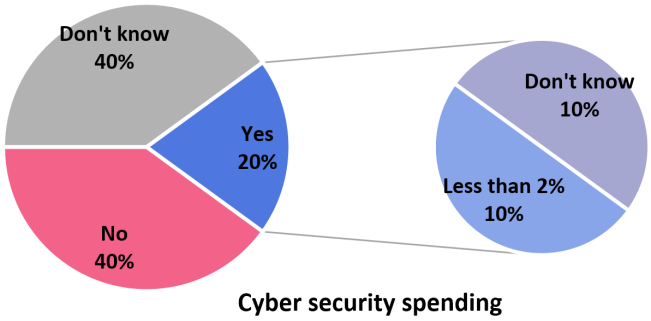
- Efficiency: real-time schedules, shared farecard
- Fun: on-board infotainment, public Wi-Fi
- Environment: reduced noise, pollution

Generate new business opportunities

- Quality of Service: traffic adaption
- Monitoring: pre-emptive maintenance
- Marketing: data exchange with other operators

Intelligent Public Transport is a key component in Smart Cities

Challenges towards a more secure IoT



Organisational challenges

- Awareness level is low
- Security is not well integrated in organisations
- Unwillingness to collaborate and exchange information on cyber security
- Low spending for cyber security

Technical challenges

- Safety does not integrate security
- Slow phasing out of legacy systems
- Lack of framework to assess IoT security

Cyber incident have an impact on the real world!

Good practices to secure Intelligent Public Transport

ENISA good practices

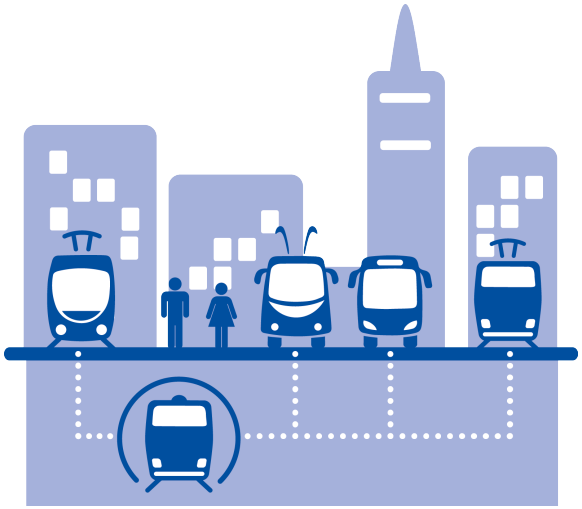
- Secure organisation, people, processes
- Secure third-party dependencies
- Applicable before, during or after an incident

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…)

ENISA TRANSSEC Expert Group



Objective: enhance security of Public Transport

- Exchange on threats, challenges, solution
- Contribute and review ENISA study
- Participation is free and voluntary

Group applications are open to:

- Operators and infrastructure owners
- Manufacturers or integrators
- Suppliers and developers of transport HW and/or SW
- Associations and not-for-profit organisations
- Relevant authorities, academia, standardisation bodies and policy makers

Apply to ENISA TRANSSEC: https://europa.eu/!TW93uf
Terms of References available on ENISA website

Conclusion

Good practices to secure IoT

For IoT manufacturers and end-users

- Express and validate security requirements
- Security “by design” goes beyond the design phase
- Do not redevelop security functions! Test your security!
- Keep up-to-date with the latest security news

Cyber security is not only technical

- Develop awareness and training on IoT threats and risks
- Assume that dependencies are/can be compromised
- Anticipate future regulation
- Make security a feature!

Critical sectors must become leader in IoT security

Possible steps to enhance security

A harmonised multi-sector approach

- Promote collaborations on cyber security across Europe and beyond
- Integrate security in business processes (trade-off risk/investment)
- Establish new approaches to risk management and trust
- Define minimum security requirements

Ensuring security of citizens

- Integration of security in research projects (H2020, industrial)
- Evaluation framework for IoT security (“5 stars” framework)
- EU regulation is coming (NIS Directive, GDPR, sector specific regulation)

IoT security is not an option!

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 on the road to secure Smart Cars

- 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

ENISA promotes a pragmatic approach of security

Thank you

PO Box 1309, 710 01 Heraklion, Greece

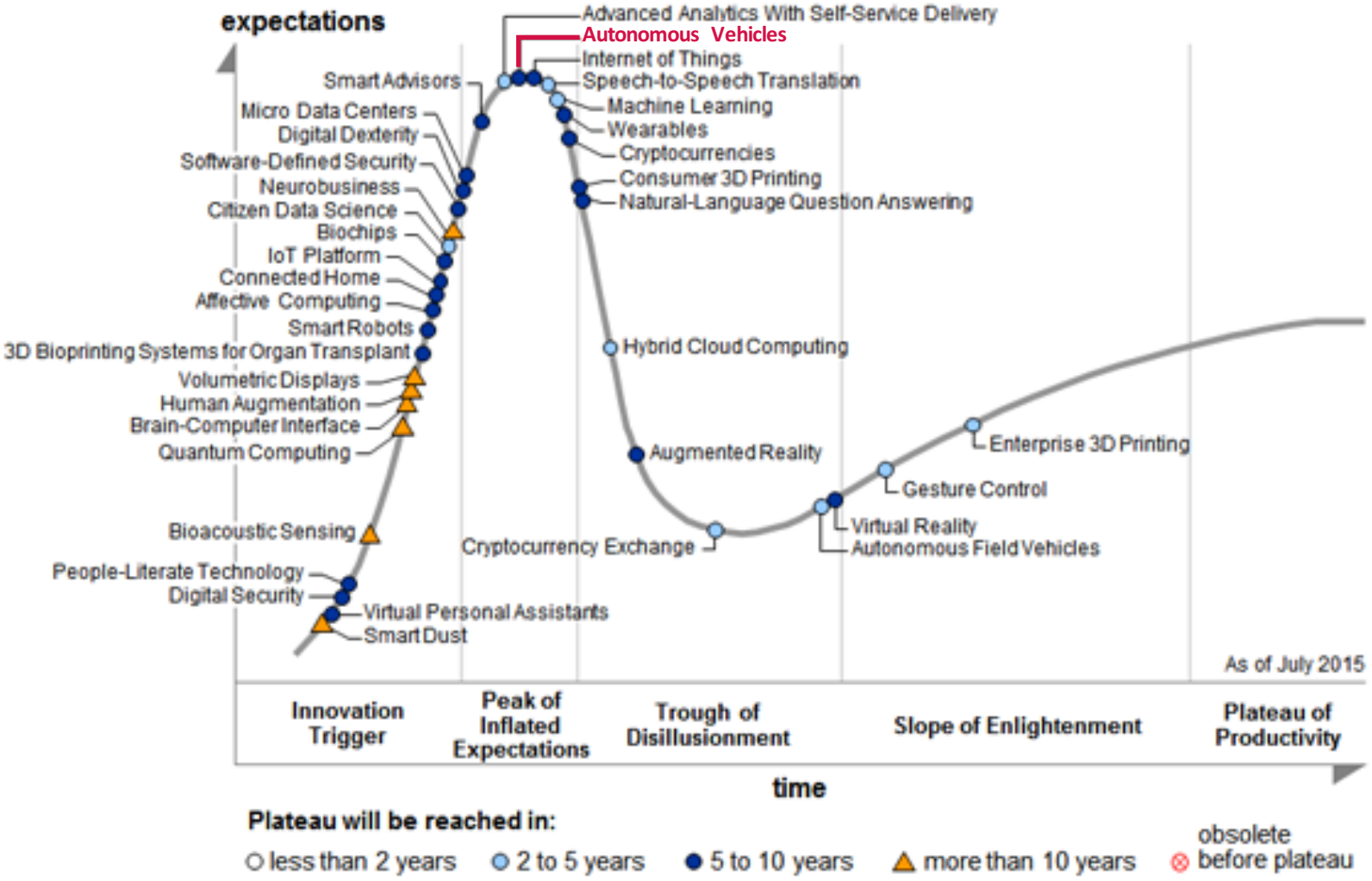
Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu

Backup slides

Prepare for secure autonomous vehicles



Secure critical assets in Intelligent Public Transport

Societal critical

- Elements affecting the quality of life of the citizens and their daily experience of transport
- Environment, safety and security, privacy…

- Sustainable urban mobility
- Passenger safety and security
- Data protection and privacy
- Sustainable environment

Example of assets: safety systems, radio communications, power distribution grid…

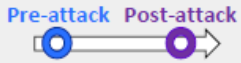
Business critical

- Elements contributing to business execution and sustainability
- Impact on revenue, service provision, operations, brand and image of organisation…

- Traffic and vehicle management
- Transportation safety and security
- Sales, fees and charges
- Resilient management structure
- Energy and environment

Example of assets: networking & communication components, payment systems…

Example: Application of good practices

GOOD PRACTICE	BUSINESS / SOCIETAL FUNCTIONS	THREAT GROUPS ADDRESSED	WHEN TO APPLY GOOD PRACTICE
Technical good practices			
Conduct security-focused risk assessments	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy/ Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Policies and standards			
Employ security by design	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Energy and environment / Sustainable environment* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*	
Define degraded modes of operation	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security / Passenger safety and security* • *Sales, fees & charge / Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Nefarious activities/abuse*	
Organisational, people and processes			
Monitor and record activity	• *Traffic & vehicle management / Sustainable urban mobility* • *Transportation safety and security/ Passenger safety and security* • *Sales, fees & charge /Data protection & privacy / Resilient management structure*	• *Unintentional damage* • *Physical & large-scale threats* • *Acts of nature/environmental incidents* • *Accidental errors/malfunctions/ failures* • *Disruptions/outages* • *Nefarious activities/abuse* • *Insider threats*