enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ITUEvents

ITU Regional Cybersecurity Forum for Europe and CIS

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

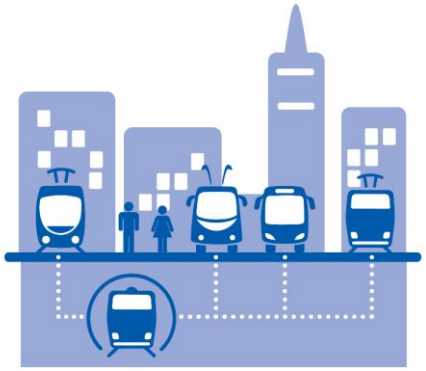
ENISA'S EFFORTS ON IOT CYBERSECURITY

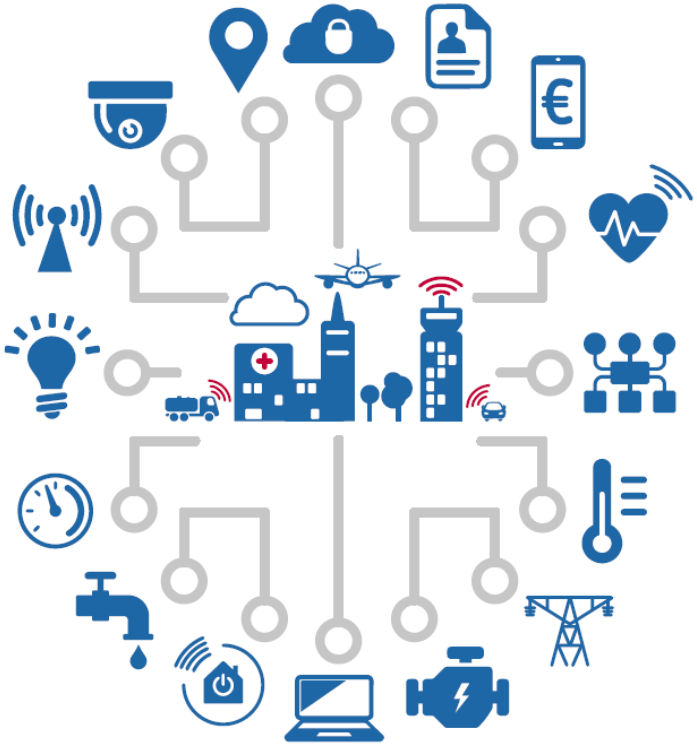
Rossen Naydenov
Network and Information Security Expert, ENISA

28 | 02 | 2020

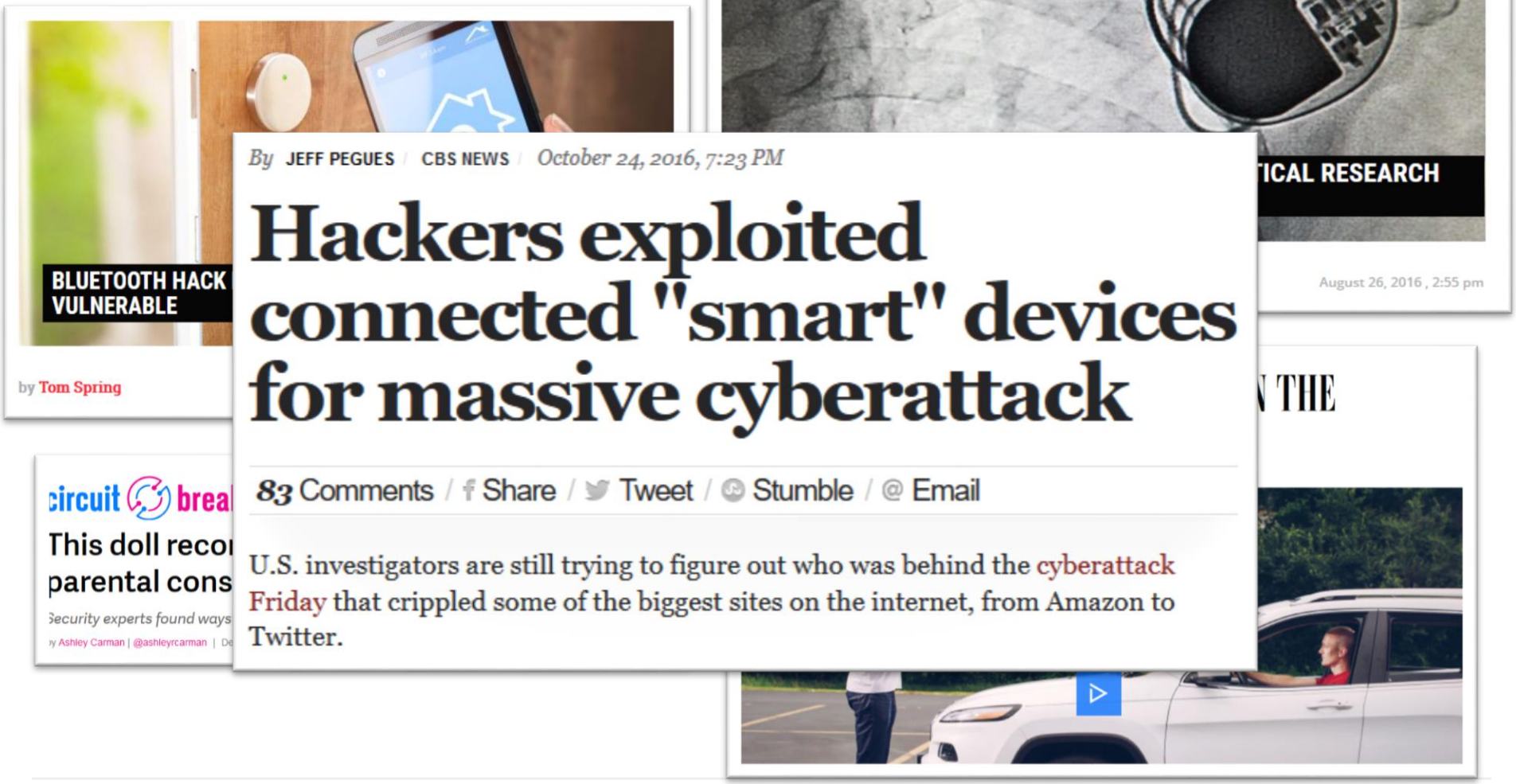
ENISA ACTIVITIES

IOT IS EVERYWHERE





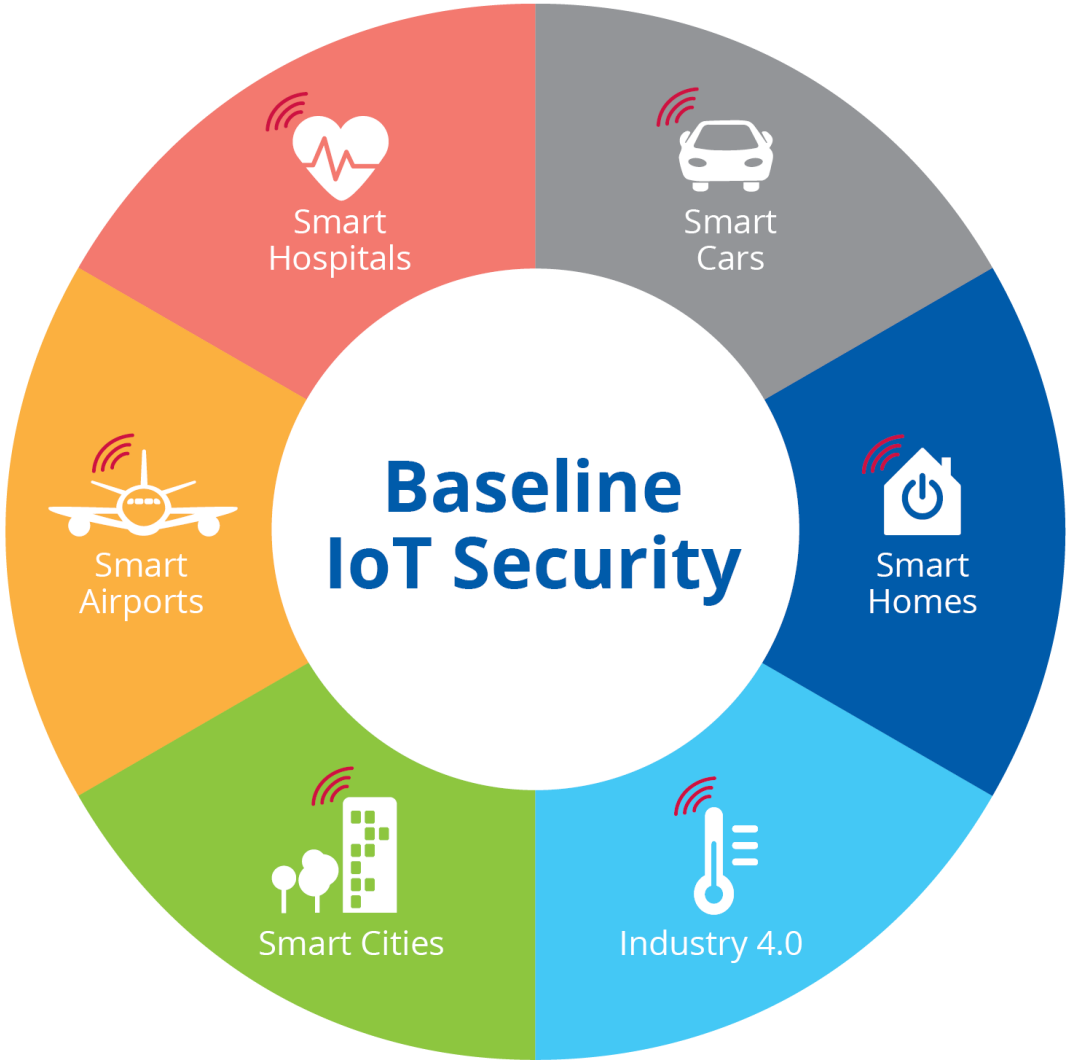
…AND IT HAS REAL-LIFE IMPLICATIONS



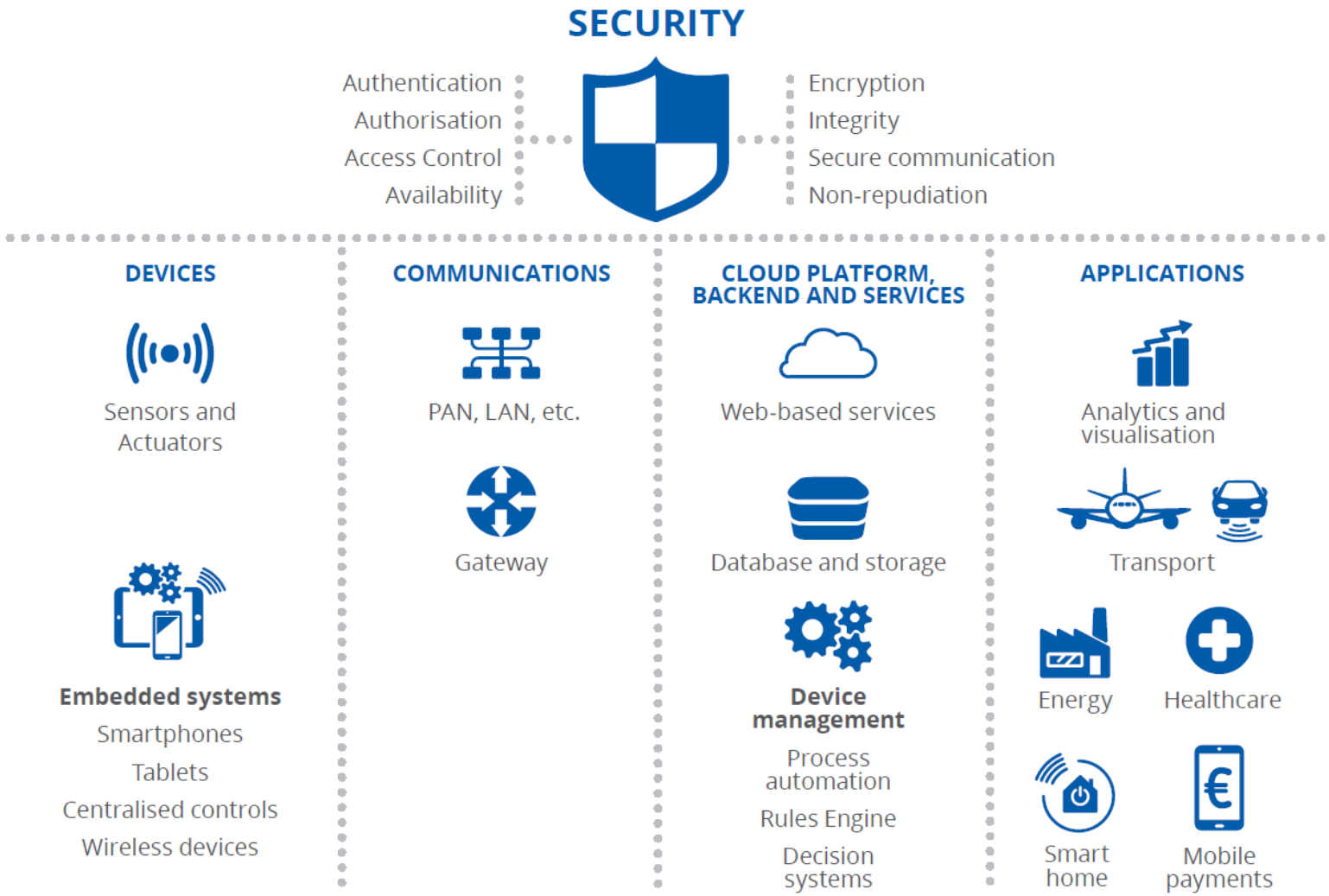
IOT SECURITY – MAIN CHALLENGES

- **Very large attack surface and widespread deployment**
- **Security for safety (especially for critical sectors)**
- **Interoperability, increased connectivity & cascading effects**
- **Security (by design) not a top priority**
- **Lack of expertise**
- **Applying security updates**
- **Lack of secure development practices**
- **Unclear liabilities**
- **Fragmentation of good practices and standards**

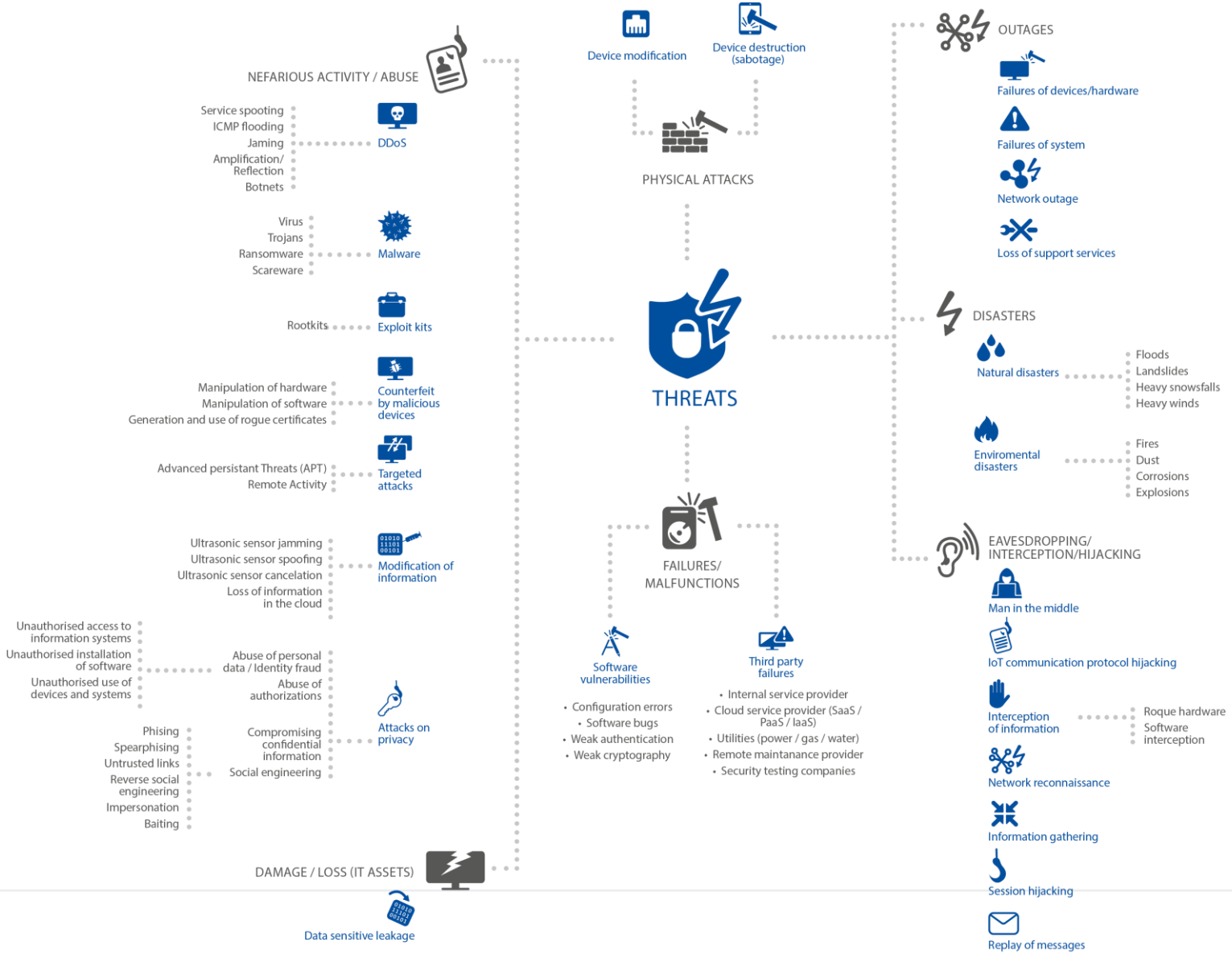
HOW DO WE SECURE IOT?



IOT HIGH-LEVEL REFERENCE MODEL



IOT THREAT TAXONOMY



BASELINE IOT SECURITY MEASURES

POLICIES

- SECURITY BY DESIGN
- PRIVACY BY DESIGN
- ASSET MANAGEMENT
- RISK AND THREAT IDENTIFICATION & ASSESSMENT

ORGANISATIONAL MEASURES

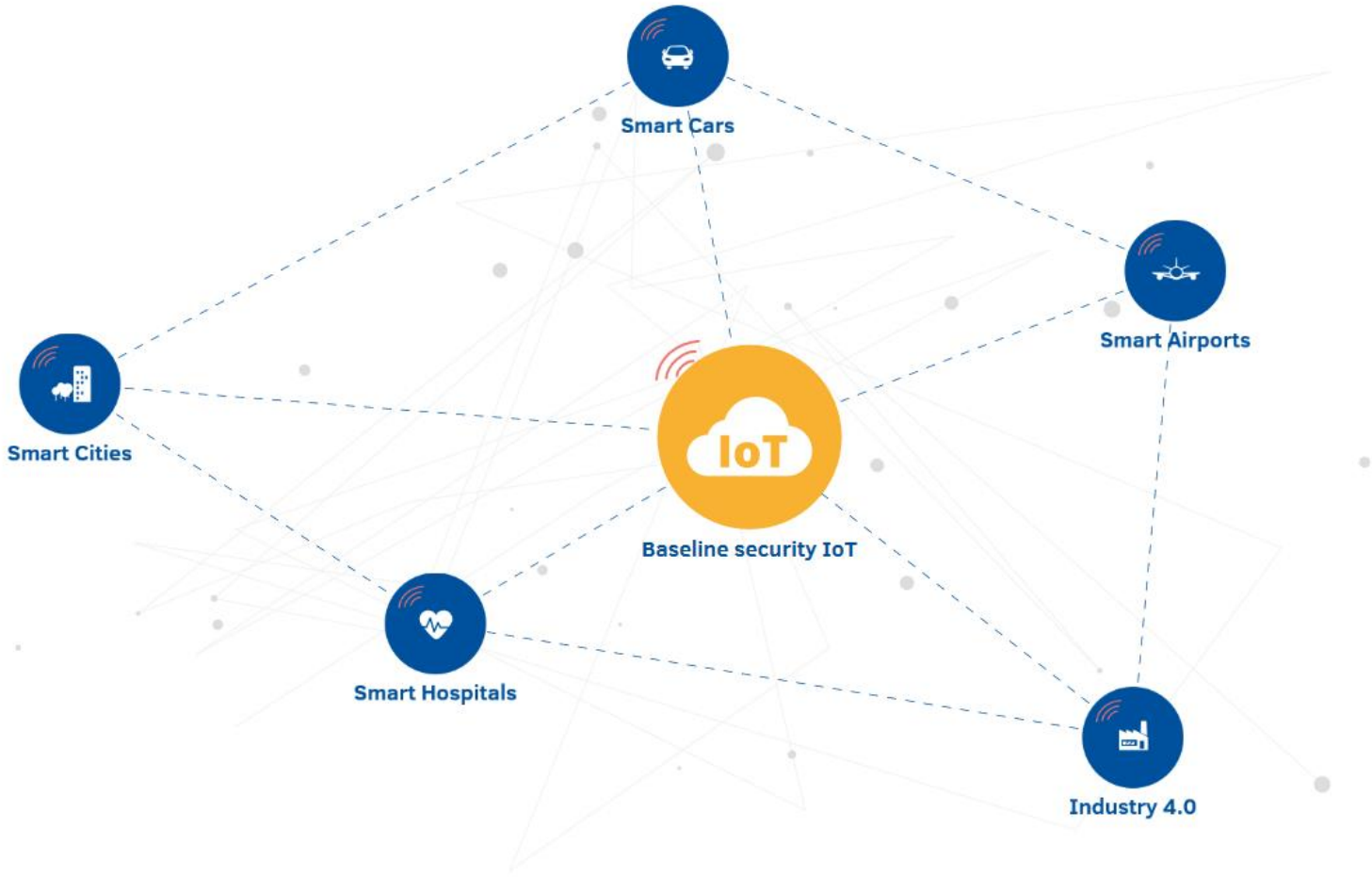
- END-OF-LIFE SUPPORT
- PROVEN SOLUTIONS
- MANAGEMENT OF SECURITY VULNERABILITIES AND/OR INCIDENTS
- HUMAN RESOURCES SECURITY TRAINING AND AWARENESS
- THIRD-PARTY RELATIONSHIPS

GOOD PRACTICES

TECHNICAL MEASURES

- HARDWARE SECURITY
- TRUST & INTEGRITY MANAGEMENT
- STRONG DEFAULT SECURITY & PRIVACY
- DATA PROTECTION & COMPLIANCE
- SYSTEM SAFETY & RELIABILITY
- SECURE SOFTWARE / FIRMWARE UPDATES
- AUTHENTICATION
- AUTHORIZATION
- ACCESS CONTROL - PHYSICAL & ENVIRONMENTAL SECURITY
- CRYPTOGRAPHY
- SECURE & TRUSTED COMMUNICATIONS
- SECURE INTERFACES & NETWORK SERVICES
- SECURE INPUT & OUTPUT HANDLING
- LOGGING
- MONITORING & AUDITING

IOT & SMART INFRASTRUCTURES TOOL



https://www.enisa.europa.eu/iot-tool

ENISA Good practices for IoT and Smart Infrastructures Tool

This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.

For further help on how to use the tool please consult this help guide.

Baseline security IoT | Smart Cars | Smart Hospitals | Smart Airports | Smart Cities | Industry 4.0 | back

Here you can find in a consolidated web format all the baseline security measures and good practices as they are listed in ENISA's report: Baseline security recommendations for IoT that was published in 2017.

You shall be able to find the Good practices you seek for, according to specific filters, such as Security Measures Category, Security Domains, Threat Groups or even specific Standards (see references column).

SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	THREAT GROUP
Logging Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection. [Technical measures] 15 relevant references. [Show]	■ Detection	■ Damage / Loss (IT Assets)
Access Control - Physical and Environmental security Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device. [Technical measures] 24 relevant references. [Show]	■ Physical and environmental security	■ Physical attacks ■ Nefarious Activity / Abuse
Secure Software / Firmware updates Backward compatibility of firmware updates. Automatic firmware updates should not change network	■ IT Security architecture	■ Outages

Filters

Security measure ⓘ −
Filter by measure
Select measure

Security measures category ⓘ +
Filter by category

Security domain ⓘ +
Filter by Security domain

Threat group ⓘ +
Filter by Threats

Reference ⓘ +
Filter by title, author

ENISA Good practices for IoT and Smart Infrastructures Tool

This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.

For further help on how to use the tool please consult this help guide.

Baseline security IoT | Smart Cars | Smart Hospitals | Smart Airports | Smart Cities | Industry 4.0 | back

Here you can find in a consolidated web format all the baseline security measures and good practices as they are listed in ENISA's report: Baseline security recommendations for IoT that was published in 2017.

You shall be able to find the Good practices you seek for, according to specific filters, such as Security Measures Category, Security Domains, Threat Groups or even specific Standards (see references column).

SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	THREAT GROUP
Logging Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection. [Technical measures] 15 relevant references. [Show]	■ Detection	■ Damage / Loss (IT Assets)
Access Control - Physical and Environmental security Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device. [Technical measures] 24 relevant references. [Show]	■ Physical and environmental security	■ Physical attacks ■ Nefarious Activity / Abuse
Secure Software / Firmware updates Backward compatibility of firmware updates. Automatic firmware updates should not change network	■ IT Security architecture	■ Outages

Filters

Security measure
Filter by measure
Select measure

Security measures category
Filter by category
Select category

- Organisational, People and Process measures
- Technical measures
- Policies

Filter by Threats

ENISA Good practices for IoT and Smart Infrastructures Tool

This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.

For further help on how to use the tool please consult this help guide.

Baseline security IoT | Smart Cars | Smart Hospitals | Smart Airports | Smart Cities | Industry 4.0 | back

Here you can find in a consolidated web format all the baseline security measures and good practices as they are listed in ENISA's report: Baseline security recommendations for IoT that was published in 2017.

You shall be able to find the Good practices you seek for, according to specific filters, such as Security Measures Category, Security Domains, Threat Groups or even specific Standards (see references column).

SECURITY MEASURES / GOOD PRACTICES

Access Control - Physical and Environmental security

Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

[Technical measures] 26 relevant references. [**Hide**]

SECURITY DOMAIN

- Physical and environmental security

THREAT GROUP

- Physical attacks
- Eavesdropping / Interception / Hijacking
- Failures / Malfunctions

ISO27001 #A9. Access Control, #A11. Physical and Environmental security — International Organization for Standardization (ISO)

NIST SP 800-30 — National Institute of Standards and Technology (NIST)

NIST SP 800-53 (Physical And Environmental Protection Control Family (PE), SA-18 Tamper Resistance And Detection, AC-1 Access Control Policy And Procedures) — National Institute of Standards and Technology (NIST)

NIST Framework for Improving Critical Infrastructure Cybersecurity — National Institute of Standards and Technology (NIST)

OWASP Access control — Open Web Application Security Project (OWASP)

OWASP I10. Internet of Things Top Ten — Open Web Application Security Project (OWASP)

European Commission - Advancing the Internet of Things in Europe — European Commission

IERC European Research Cluster on the Internet of Things — IERC European Research Cluster on the Internet of Things

FTC - Internet of Things: Privacy & Security in a Connected World — U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau

oneM2M - Standards for M2M and the Internet of Things — oneM2M

International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" — International Electrotechnical Commission (IEC)

Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products — Cloud Security Alliance (CSA)

Filters

Security measure (1) clear all

Filter by measure

× Access Control - Physical and Environmental security

Security measures category (1)

Filter by category clear all

× Technical measures

Security domain

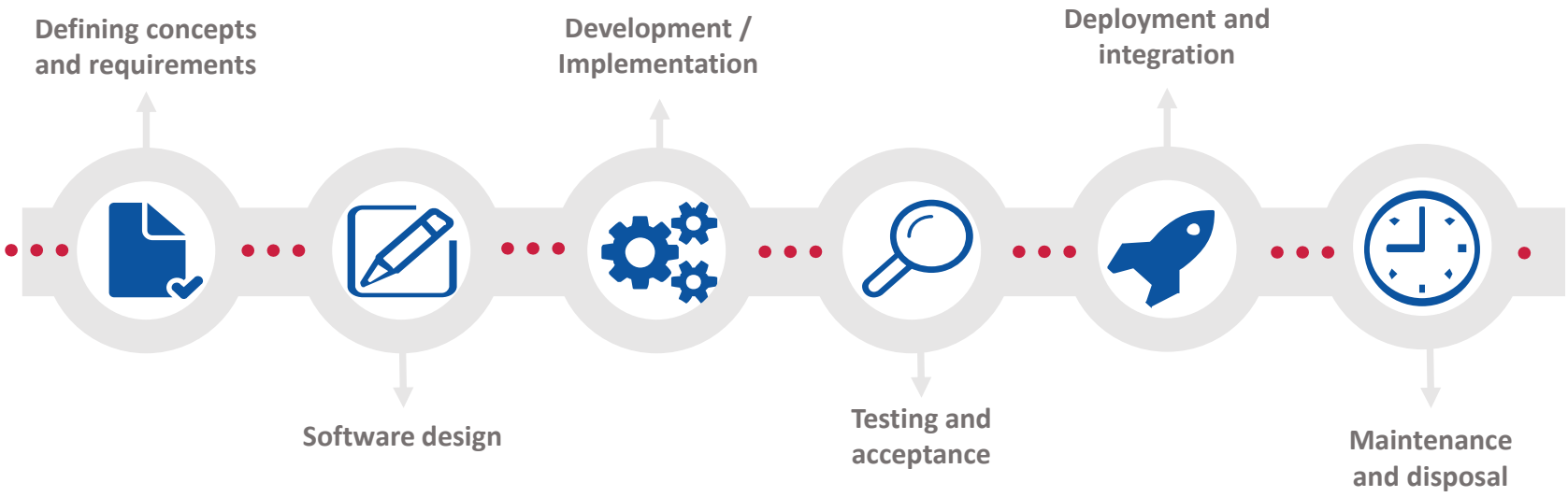
Filter by Security domain

Select Security domain

IOT SECURITY

LATEST DEVELOPMENTS

SECURE DEVELOPMENT GUIDELINES FOR IOT



SMART CARS SECURITY

UPCOMING IN IOT

- Supply chain security for IoT
- In Connected and Automated Mobility
  - Challenges in Connected and Automated Mobility
  - Web tool on Assets, Threats and Security Measures
  - Stakeholder mapping of the connected and automated mobility Area

HOW YOU CAN REACH US

Expert groups

- IoT Security
- Connected Mobility Security
- AI to be developed

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu