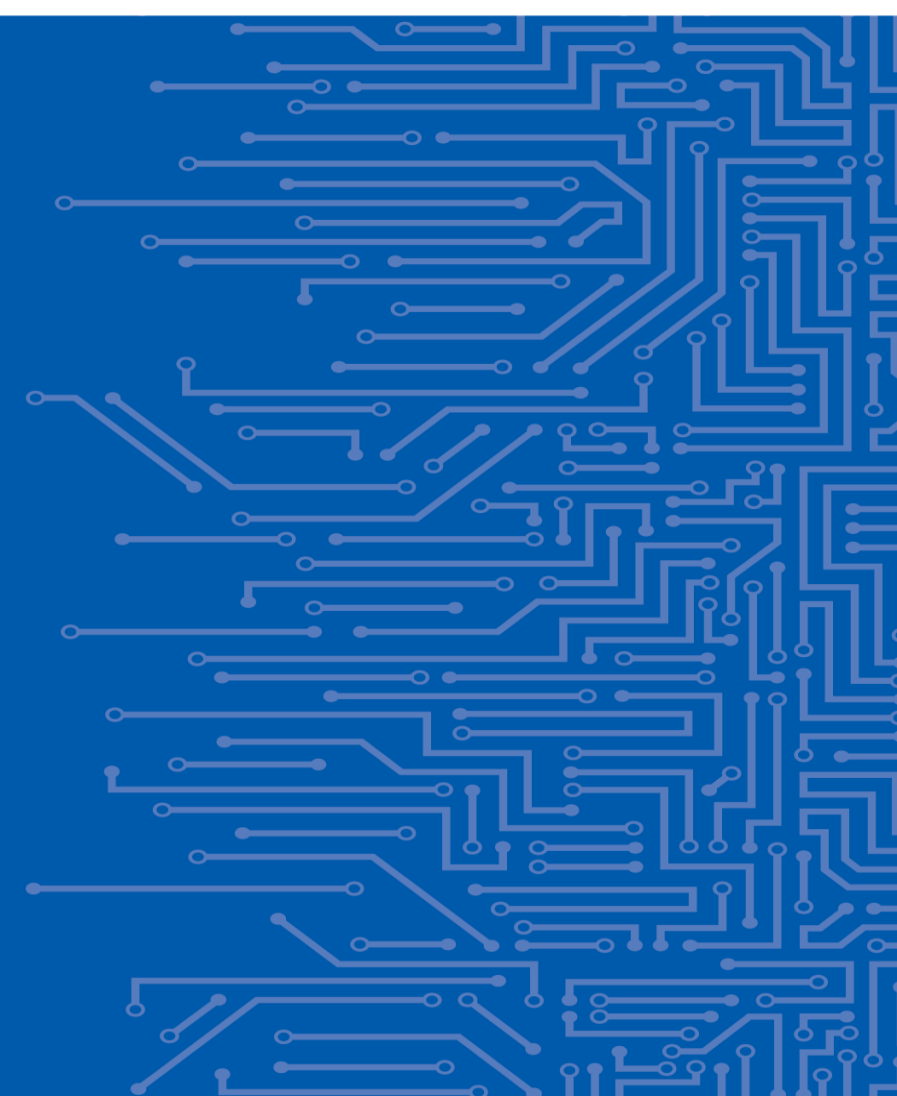
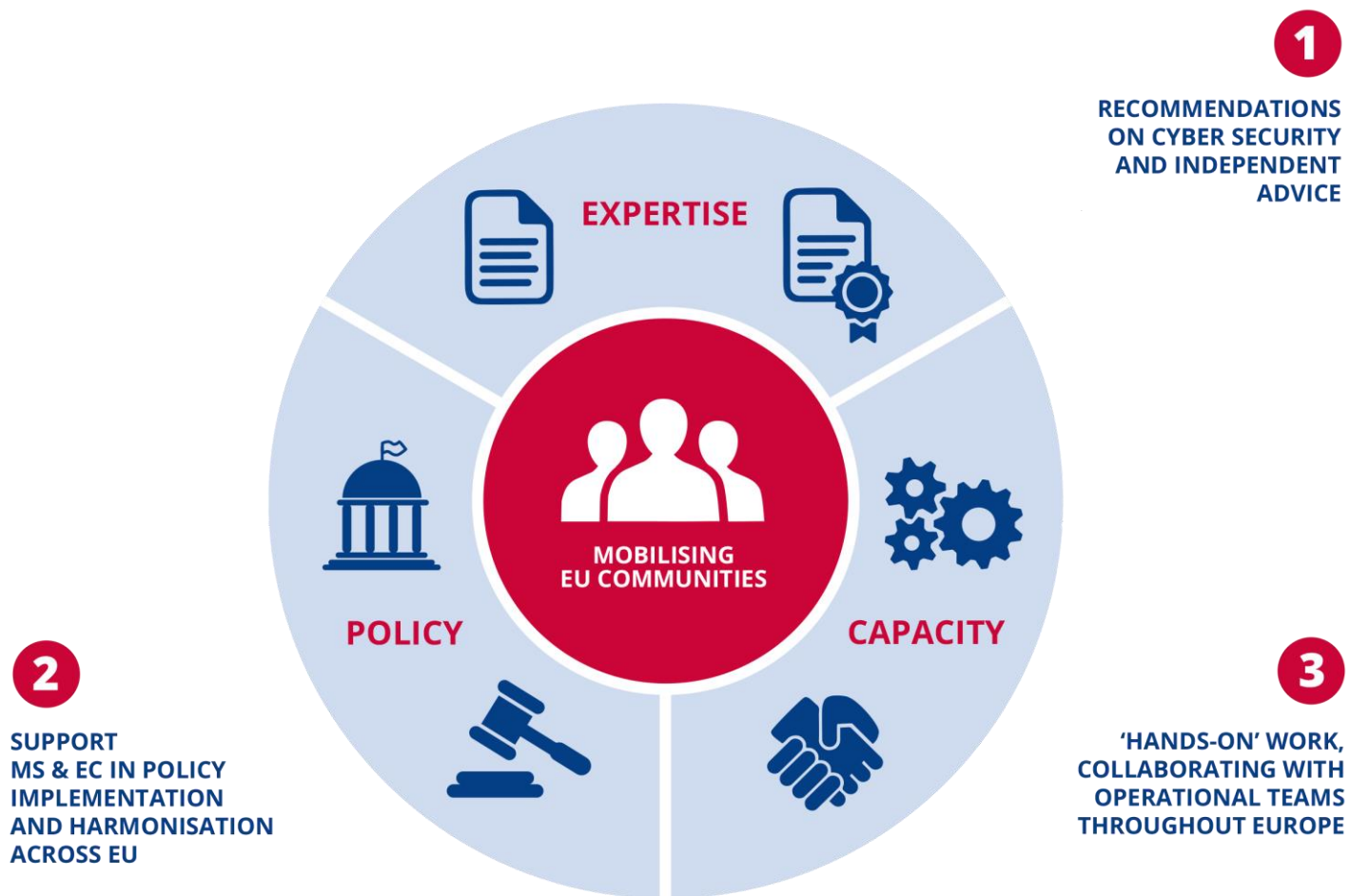


ENISA'S EFFORTS ON INDUSTRY 4.0 CYBERSECURITY

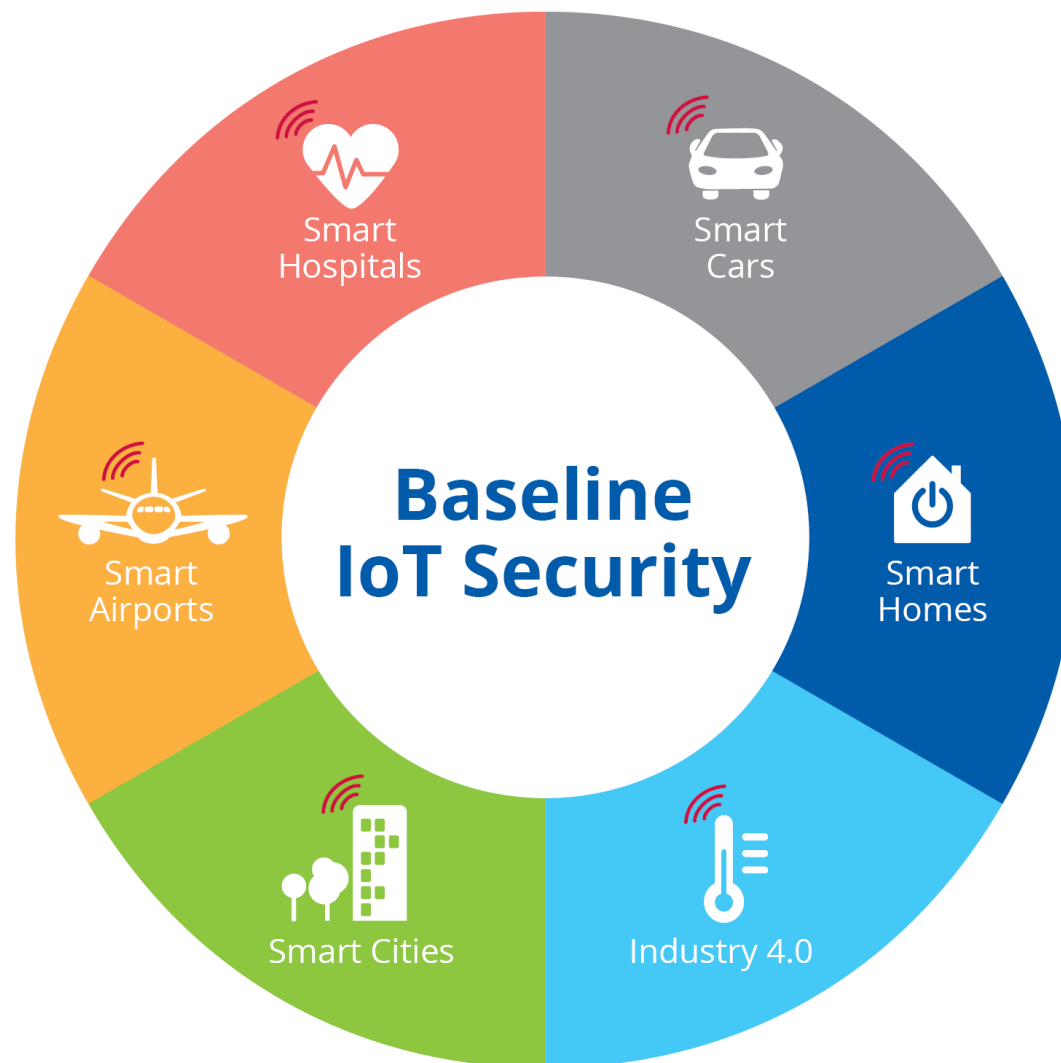
Dr. Apostolos Malatras
Network and Information Security Expert, ENISA



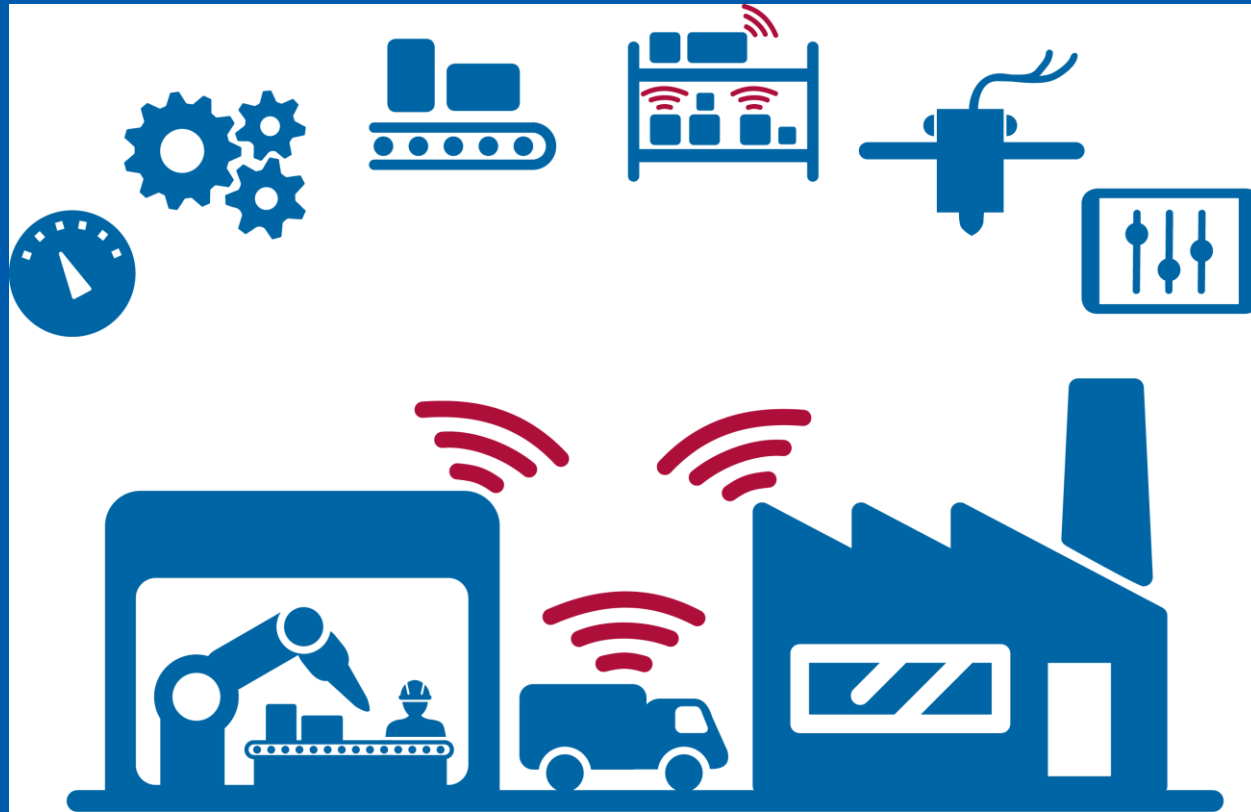
ENISA, EU AGENCY FOR CYBERSECURITY



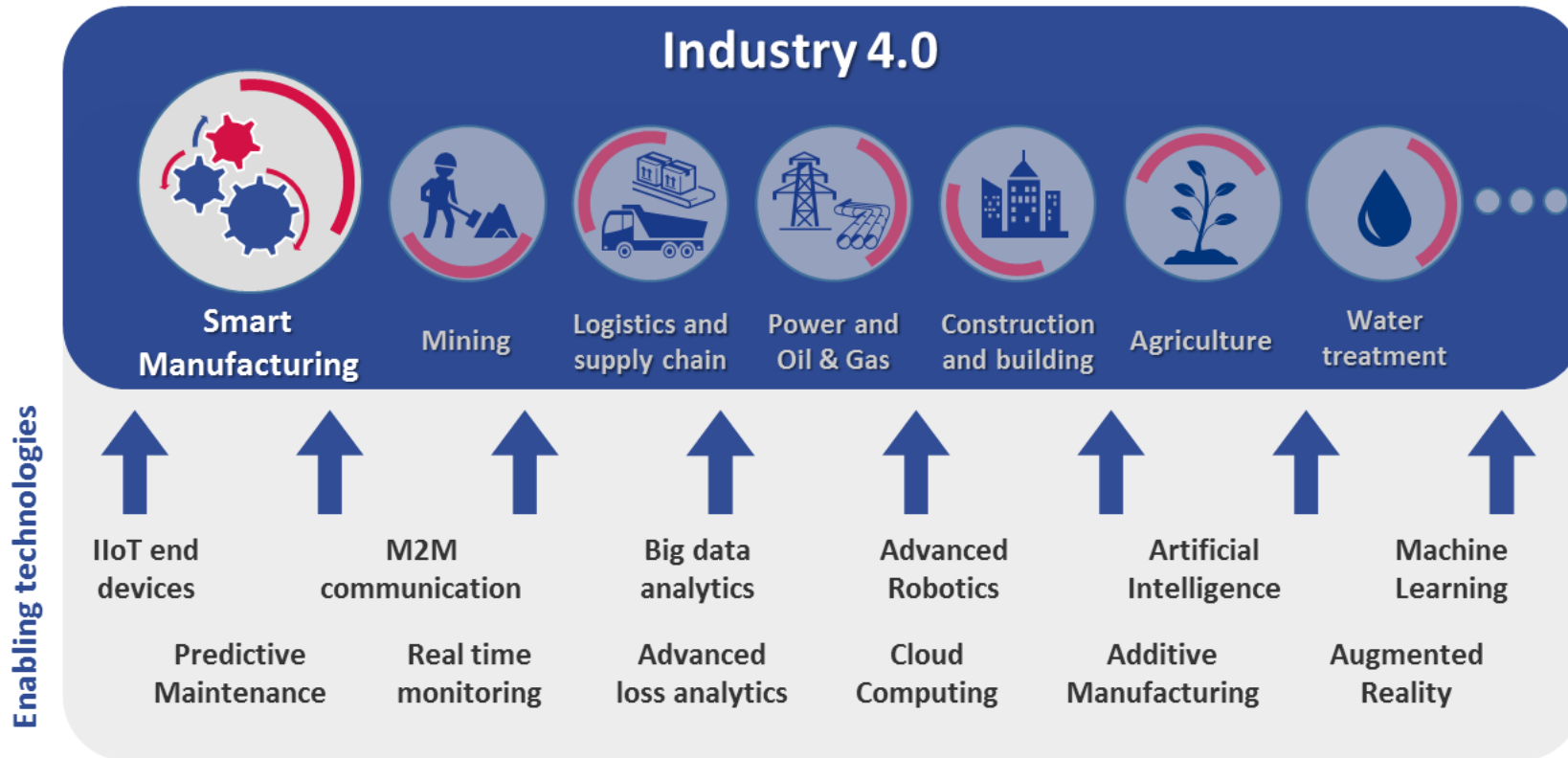
HOW DO WE SECURE IOT?



INDUSTRY 4.0



INDUSTRY 4.0 (SMART MANUFACTURING)

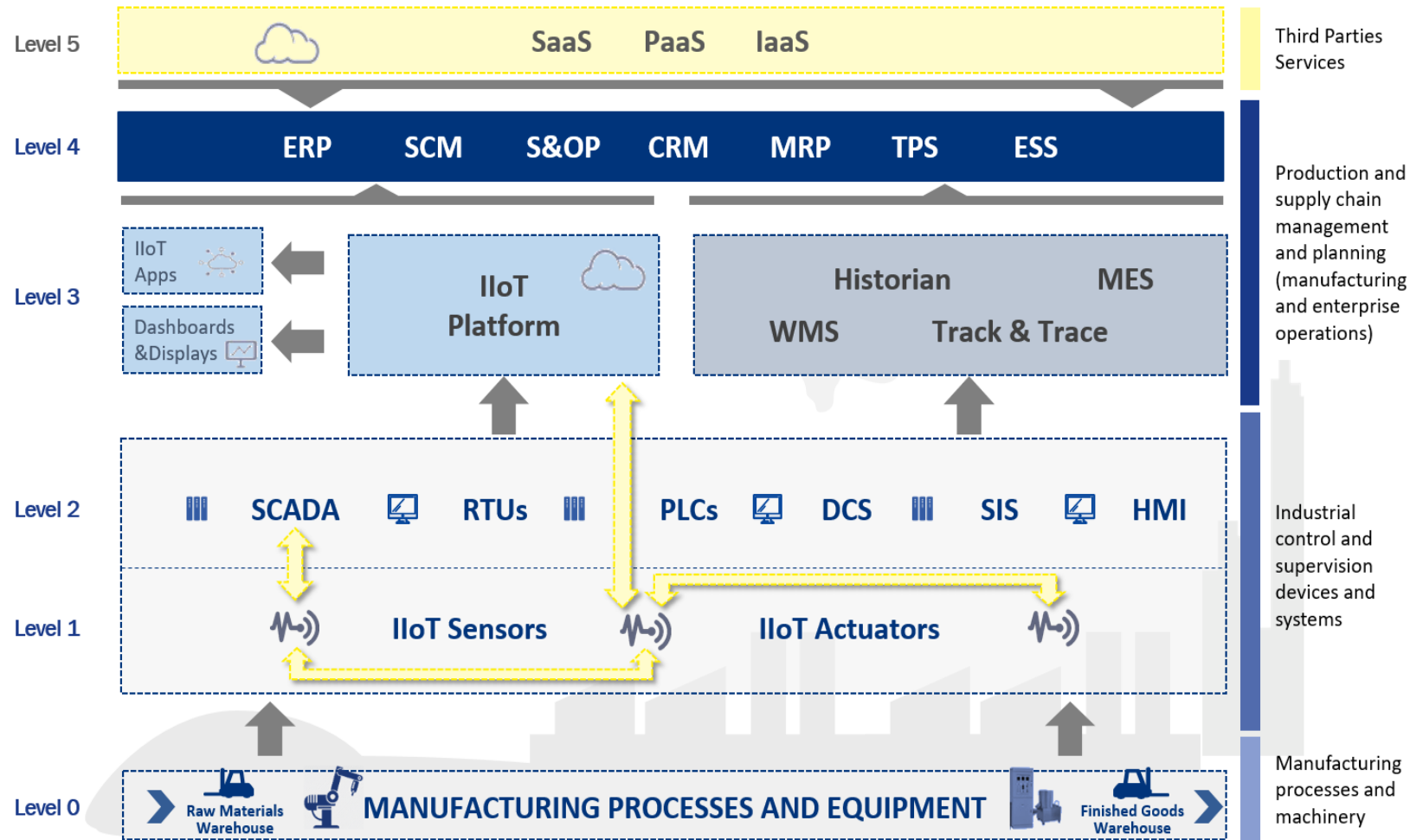




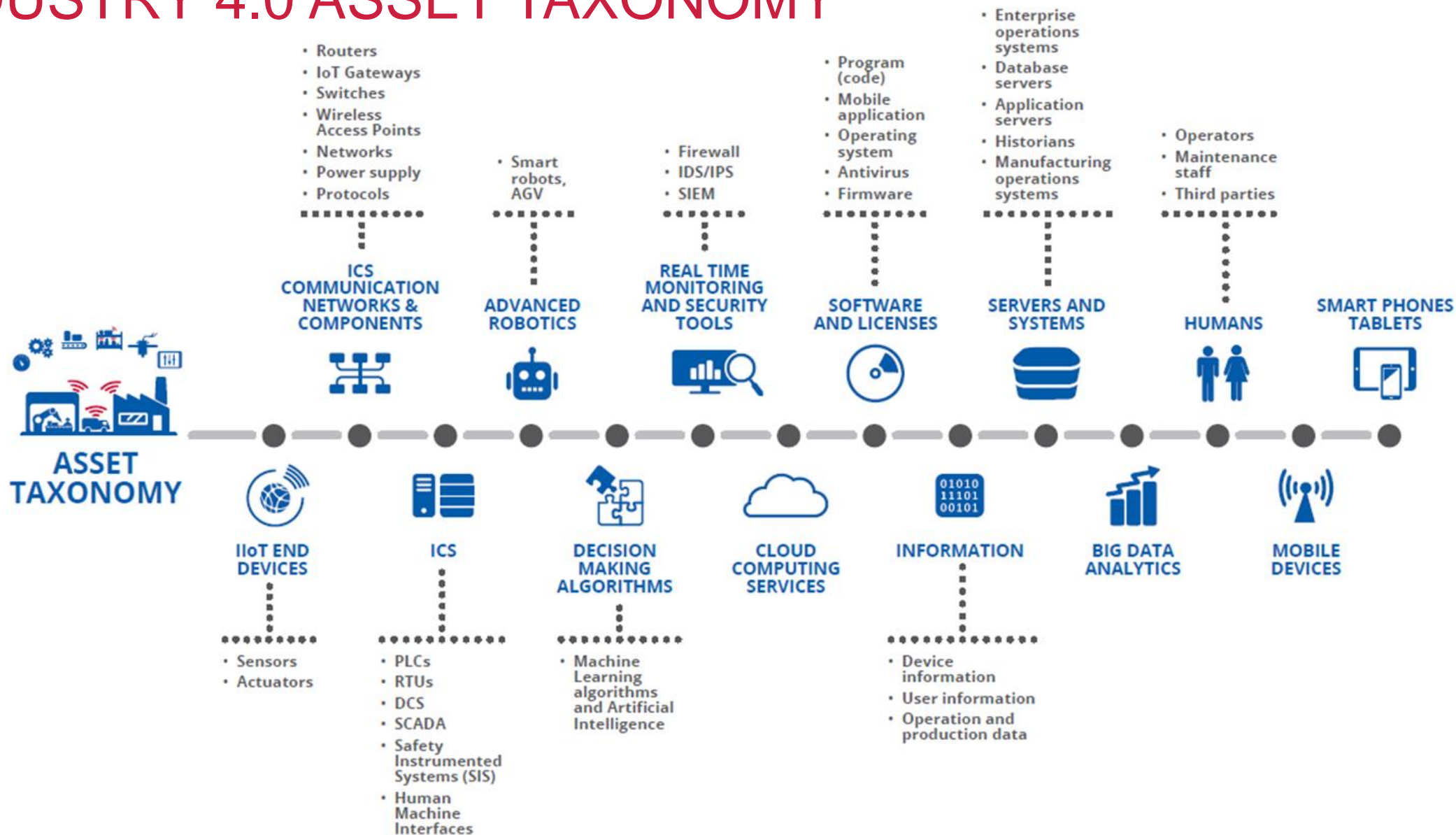
INDUSTRY 4.0 SECURITY CHALLENGES

- **Legacy industrial control systems**
- **Vulnerable components in IT/OT**
- **Insecure protocols**
- **Management of processes**
- **Increased connectivity**
- **IT/OT convergence**
- **Supply chain complexity**
- **Human factors**
- **Unused functionalities**
- **Safety aspects**
- **Security updates**
- **Secure product lifecycle**

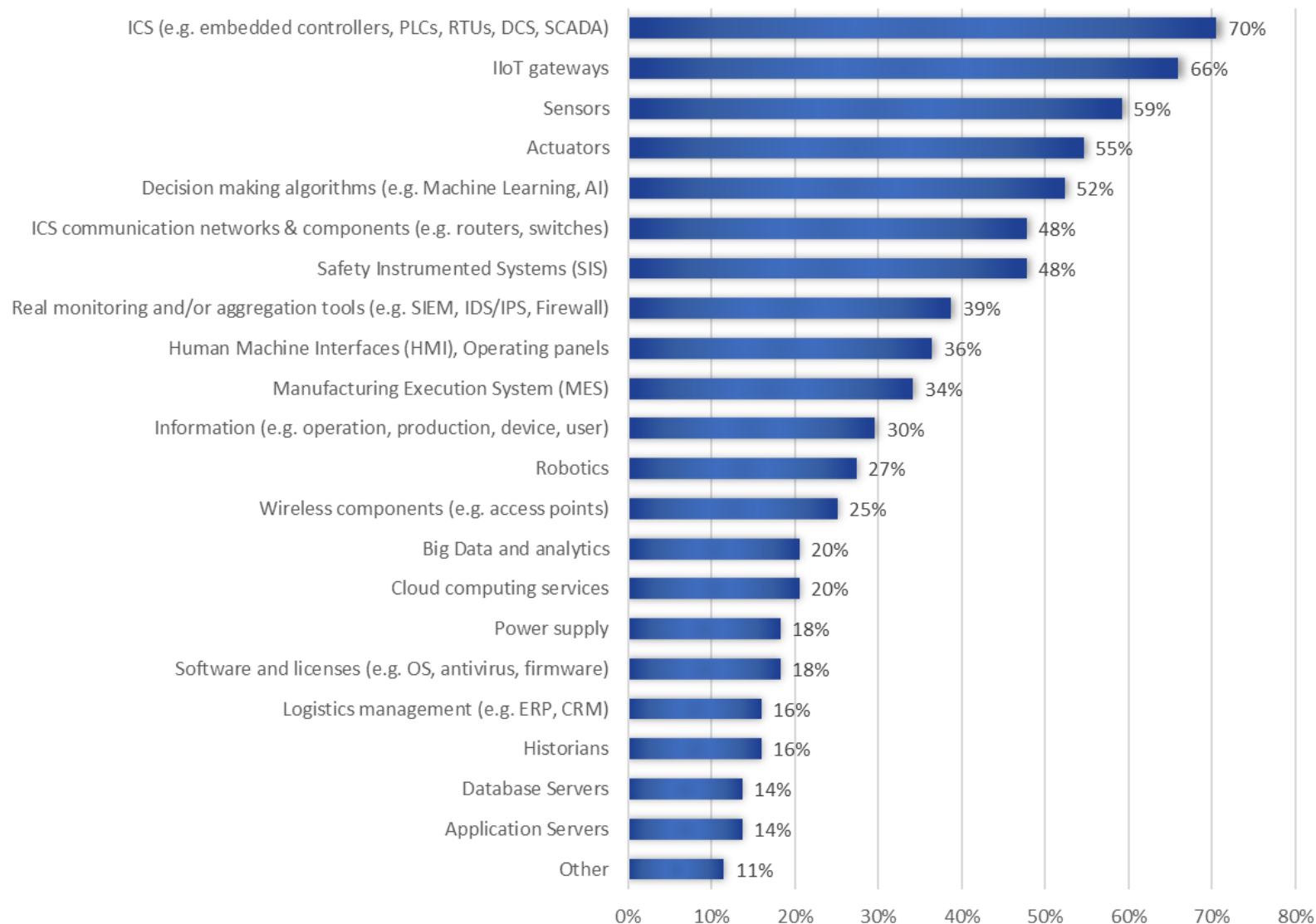
INDUSTRY 4.0 HIGH-LEVEL REFERENCE MODEL



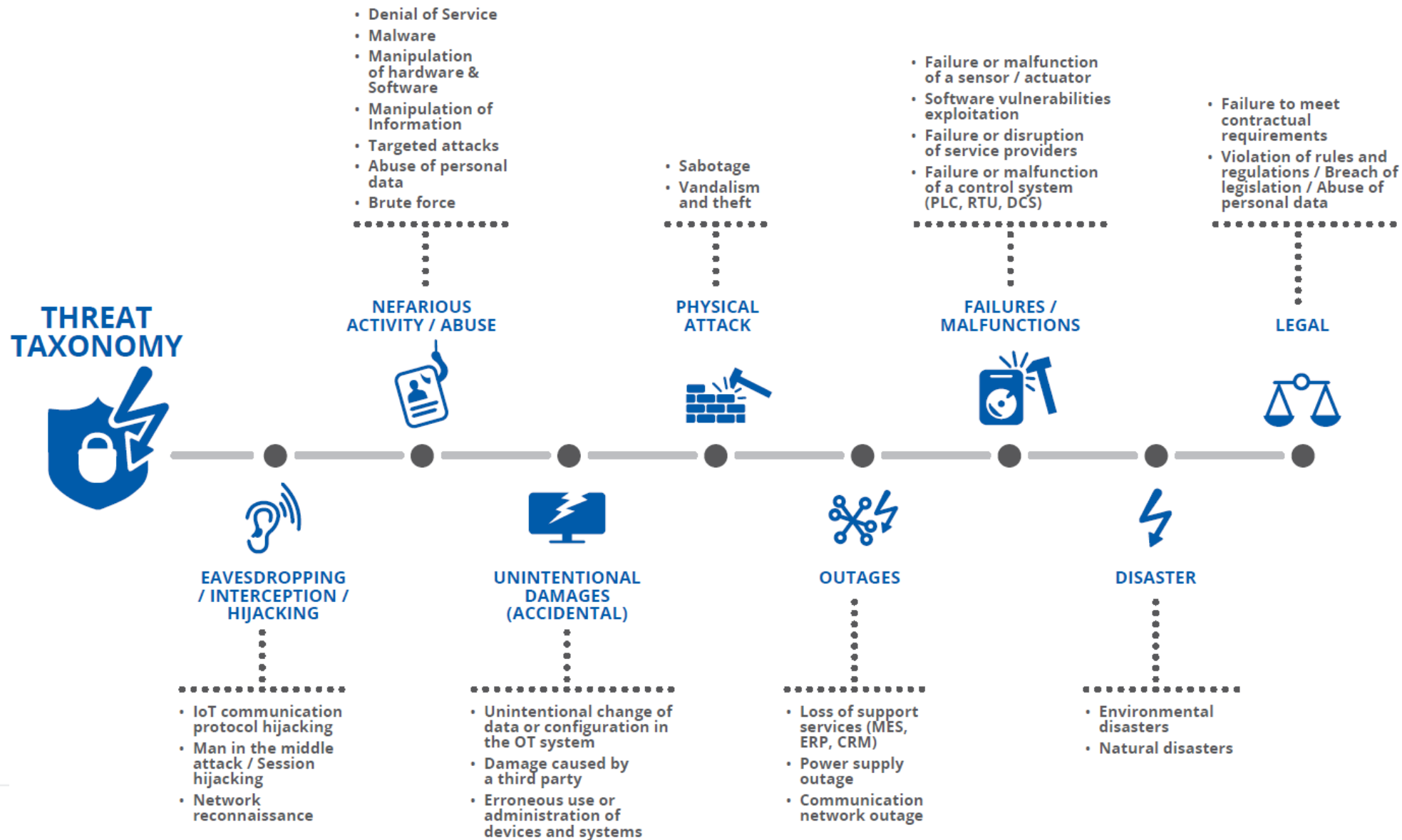
INDUSTRY 4.0 ASSET TAXONOMY



INDUSTRY 4.0 ASSET CRITICALITY



INDUSTRY 4.0 THREAT TAXONOMY



INDUSTRY 4.0 SECURITY MEASURES

POLICIES

SECURITY BY DESIGN
PRIVACY BY DESIGN
ASSET MANAGEMENT
RISK AND THREAT IMANAGEMENT



ORGANISATIONAL PRACTICES

ENDPOINTS LIFECYCLE
SECURITY ARCHITECTURE
INCIDENT HANDLING
VULNERABILITIES MANAGEMENT
TRAINING AND AWARENESS
THIRD-PARTY MANAGEMENT



GOOD PRACTICES



TECHNICAL PRACTICES

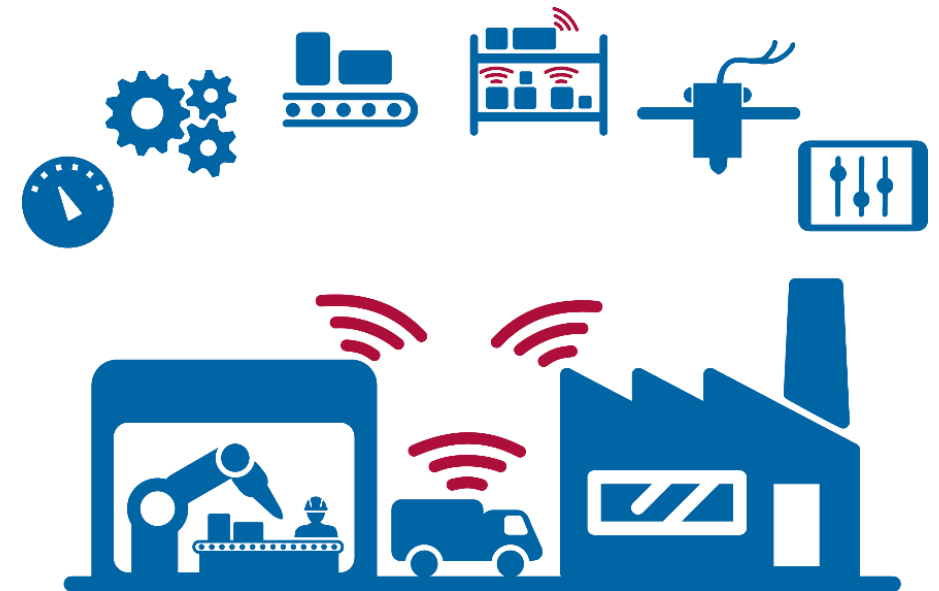
TRUST AND INTEGRITY MANAGEMENT
CLOUD SECURITY
BUSINESS CONTINUITY AND RECOVERY
MACHINE-TO-MACHINE SECURITY
DATA PROTECTION

SOFTWARE/FIRMWARE UPDATES
ACCESS CONTROL
NETWORKS, PROTOCOLS AND ENCRYPTION
MONITORING AND AUDITING
CONFIGURATION MANAGEMENT



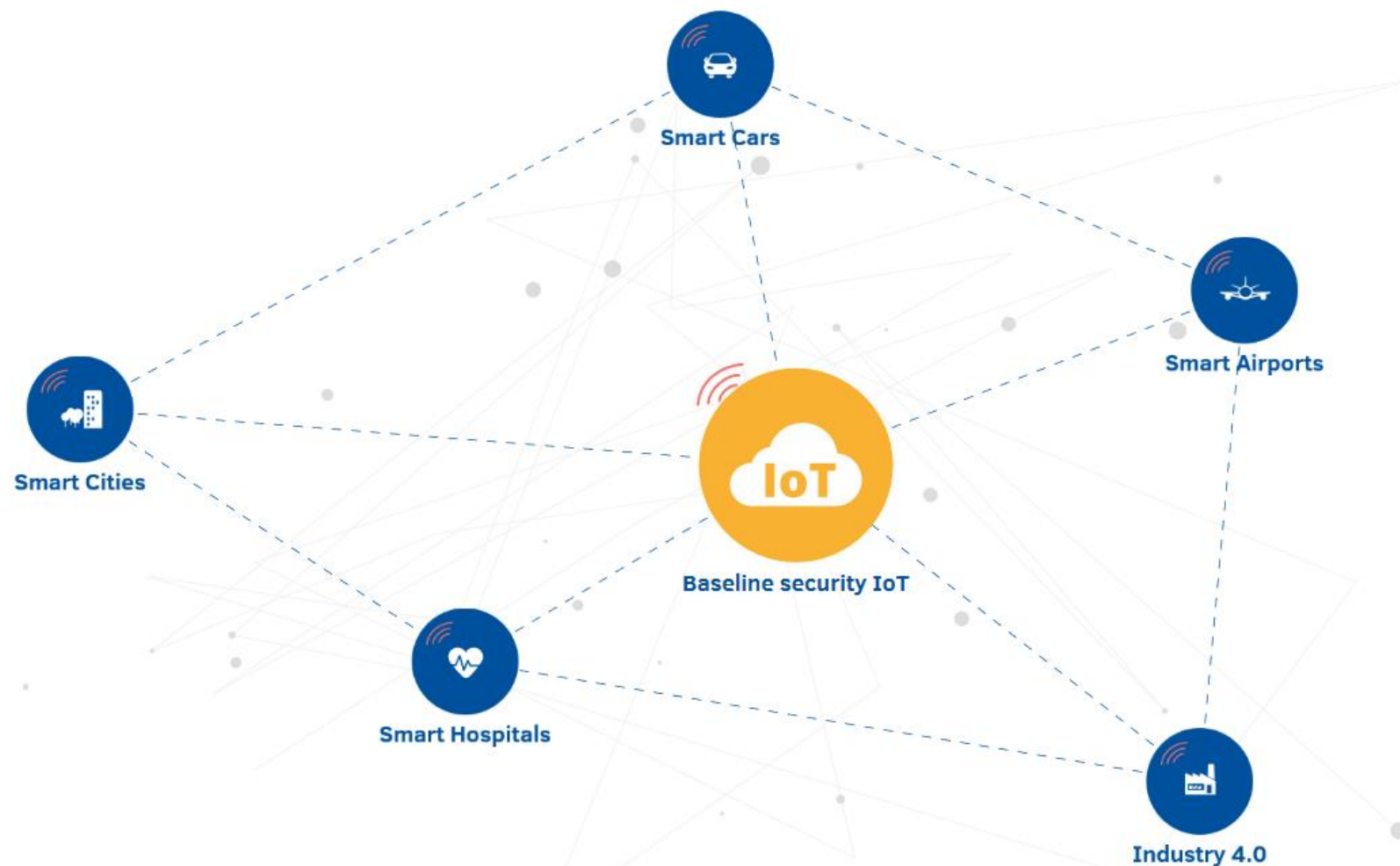
INDUSTRY 4.0 SECURITY RECOMMENDATIONS

- Convergence of IT/OT security
- Security and privacy by design
- Security of supply chain
- Clarify liability across Industry 4.0 supply chain
- Foster economic & administrative incentives for Industry 4.0 security
- Harmonization of Industry 4.0 standards
- Baseline for interoperability



<https://www.enisa.europa.eu/iot>

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

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](#)]

[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)


SECURITY DOMAIN

■ Physical and environmental security

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

THREAT GROUP

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 SECURE SOFTWARE DEVELOPMENT LIFECYCLE



Just published!

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

