

**TUVIT**

# 1<sup>ST</sup> CYBERSECURITY MARKET ANALYSIS CONFERENCE

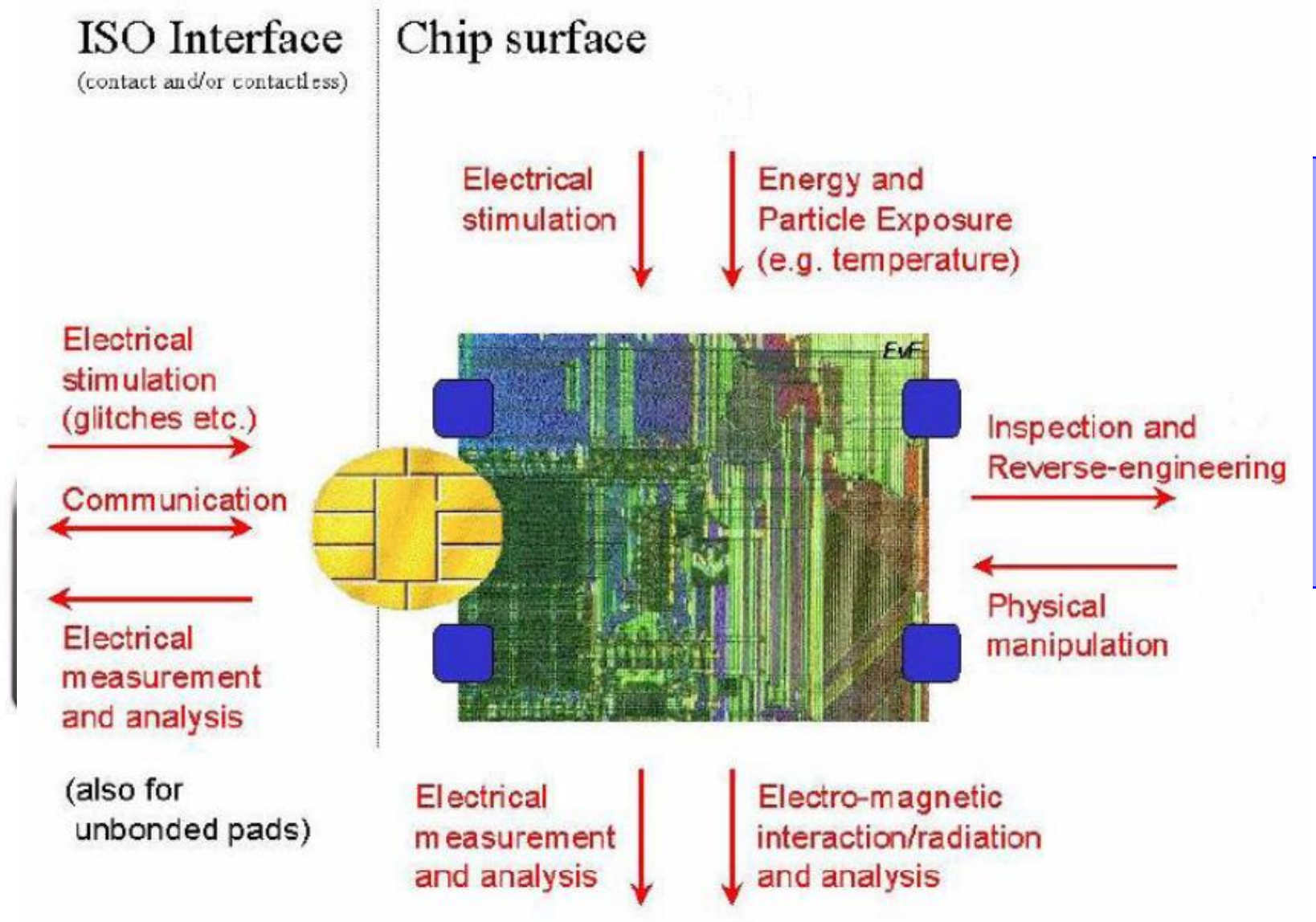
November 23<sup>rd</sup>-24<sup>th</sup>  
Thon Hotel EU,  
Brussels - Hybrid



**View of an IT Security testing lab**  
Brussels, Nov. 23rd, 2022



# Secure Elements



# Market Place Darknet

## Cybercrime Business



### Programs of Study

#### **Carding Diploma** - [Click here for description](#)

This diploma will teach you everything you need to know about credit card fraud and is designed around real world experiences.

After finishing this diploma you'll have the knowledge, skills, and the resources to commit credit card fraud.

#### **Cybercriminal Degree** - [Click here for degree course list](#)

The Cybercriminal degree covers advanced topics introducing you to Operational Security (OPSec), Wi-Fi hacking, Man-In-The-Middle (MiTM) attacks, creating malicious Word Documents, online scams, phishing, and includes how to hack an individual or business for profit or pirating.

This degree will prepare you for your career in cybercrime as an efficient and effective hacker.

#### **Future Courses** - [Click here for future courses yet to be released](#)

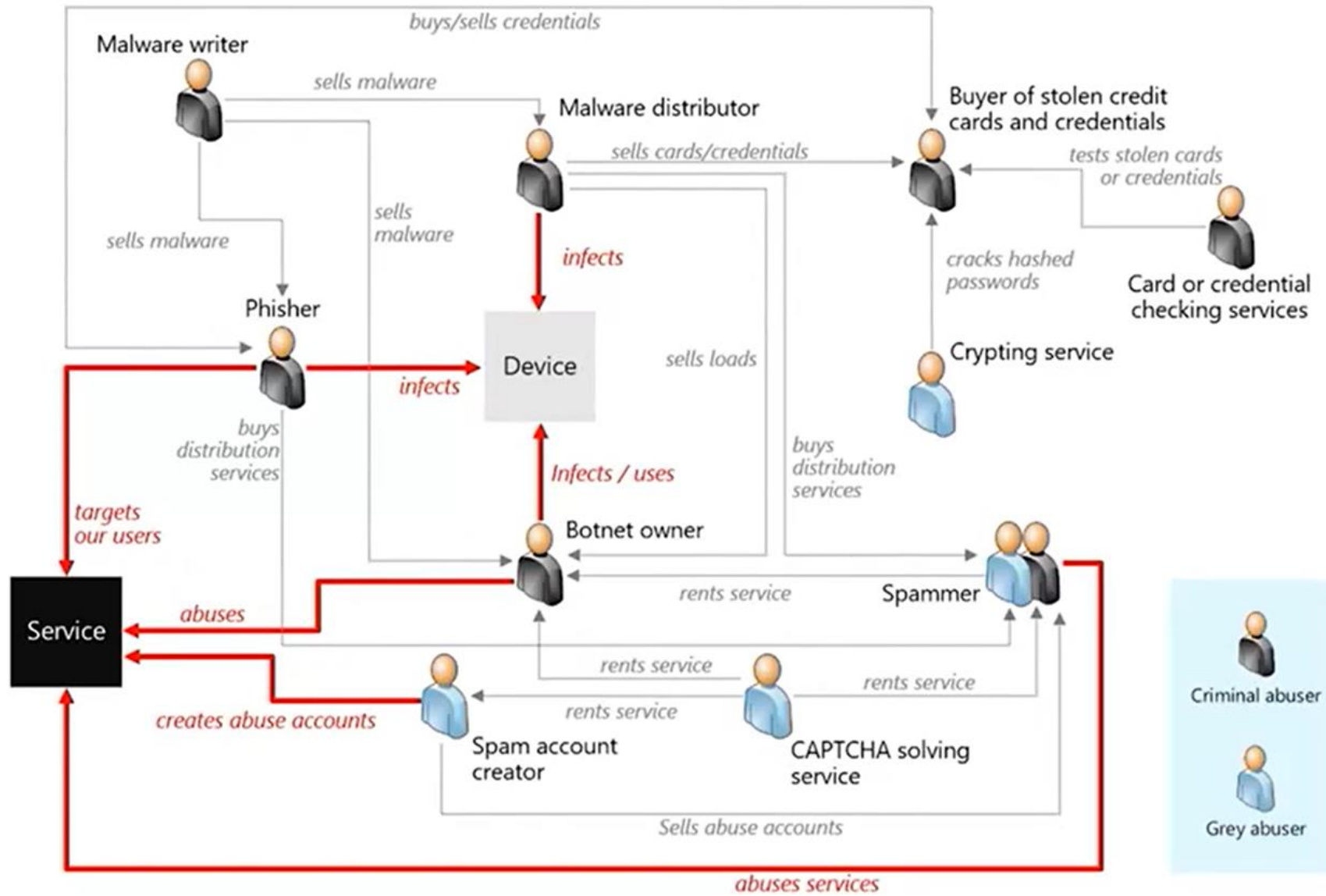
These future courses will enhance your cybercriminal skills giving you more of advantage as an attacker.

they demand ransom from you before they provide a decryption key for your locked system and e  
Ransomware typically spreads through phishing emails or by unknowingly visiting an infected wel

- 1 +

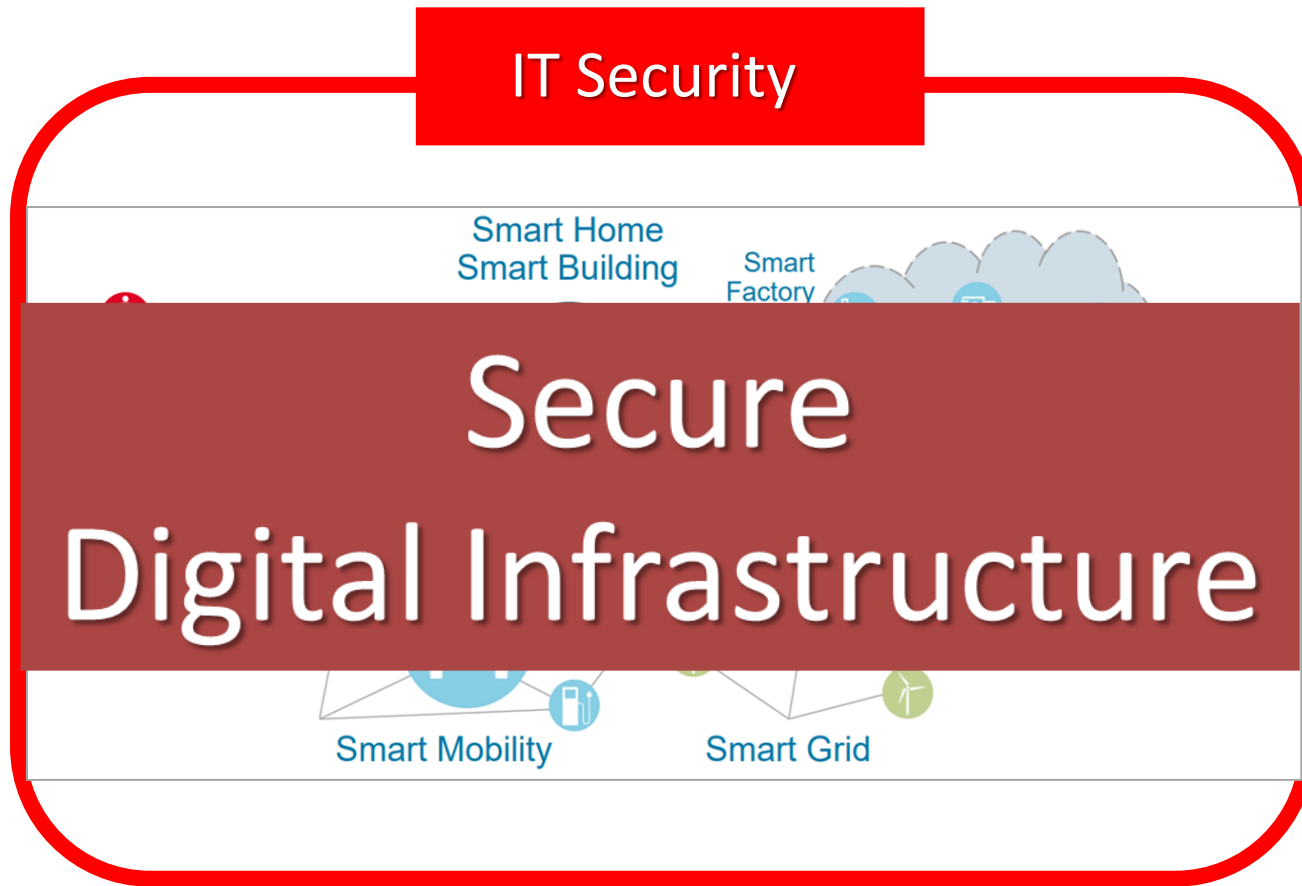
ADD TO CART

# Ecosystem of Fraud and Abuse



# No Safety without IT Security

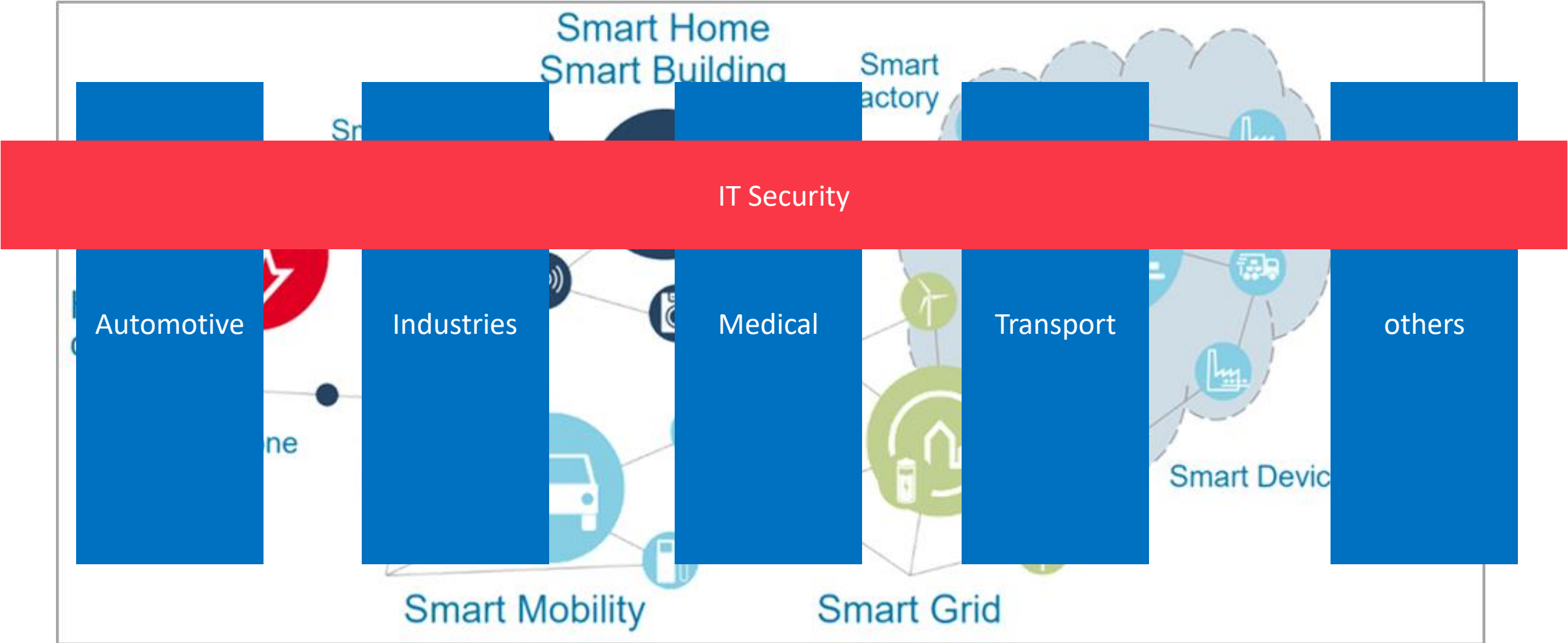
## IT Security is not an extension of Safety



IT Security is the essential prerequisite  
to achieve Safety  
in a digital connected world

Cybersecurity: Threads from  
Cyberspace  
IT Security: Cybersecurity and IT  
Infrastructure

# IT Security requirements are horizontal



# IT Security Core Elements for all Verticals

## Integration communication protocol unit



Application Unit  
Sensor  
Actor

Information Unit  
OS, Data Integrity  
Data Management

Management Unit  
Condition Display  
Software  
Decision Support

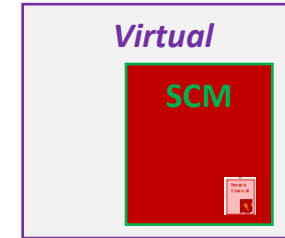
# Complexity → reduced by Modularization – Layer 1-4 core modules

Access Roles & Usage Policies

Secure Communication

Cryptographic Support

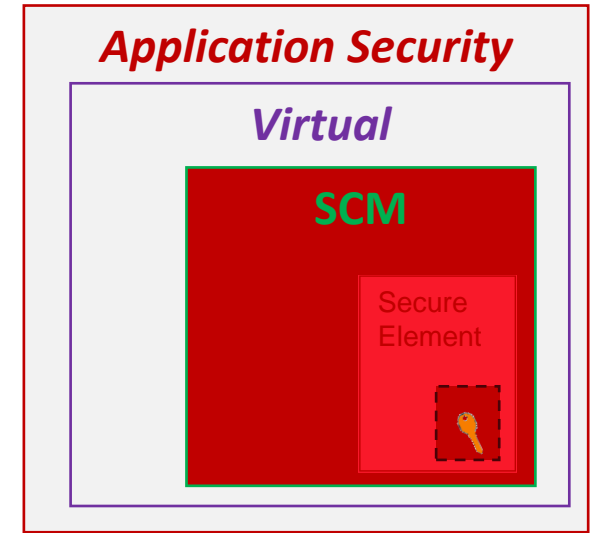
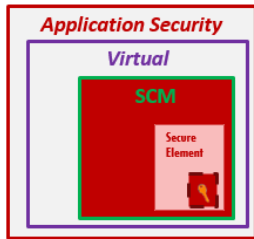
Secure Storage of Keys



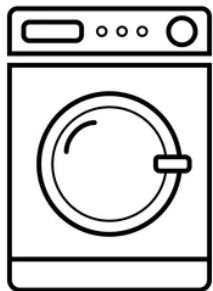


# Layer 5: Application Security

*substantial level*



IoT

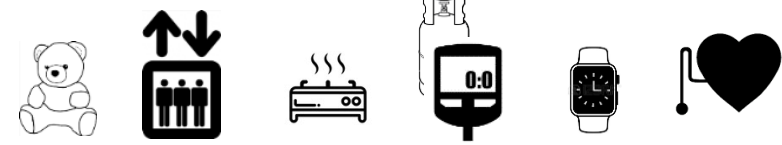


shutterstock.com · 1658051638

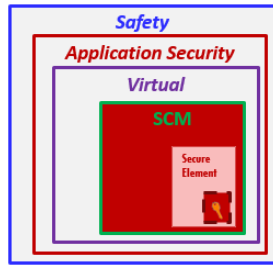
SmartHome



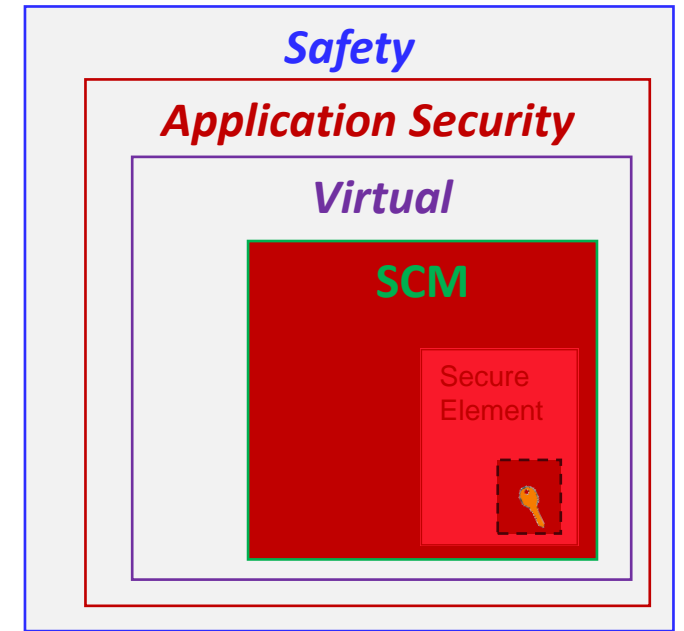
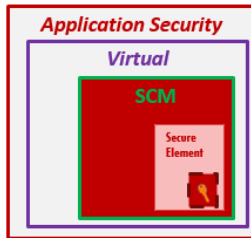
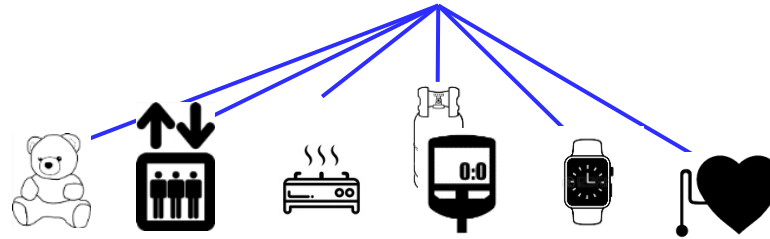
C-ITS



# Layer 6: Safety



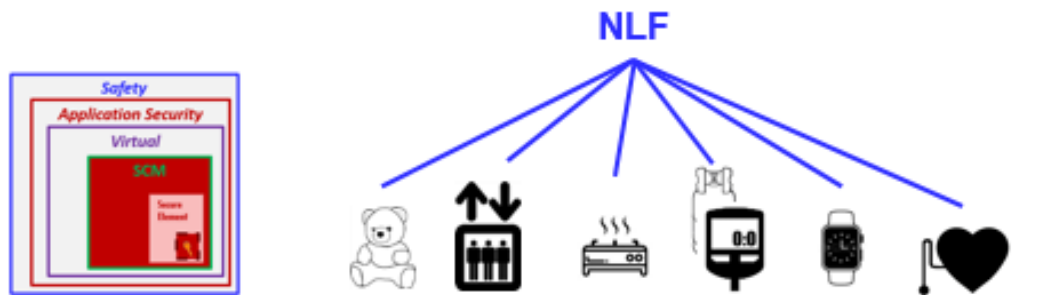
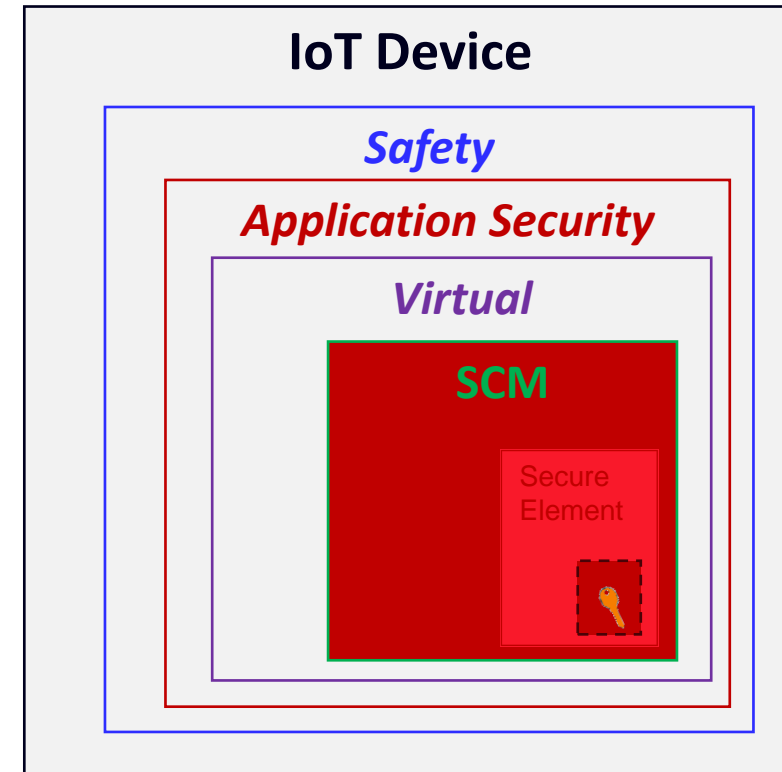
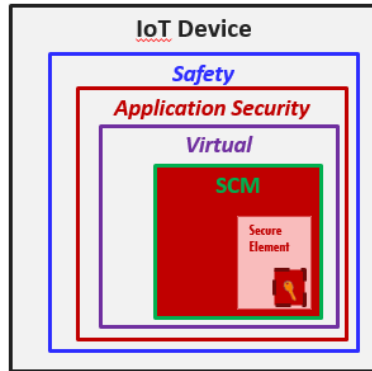
## New Legislative Framework



## Security4Safety (S4S)

In case the **IT Security** is fulfilled in layers 1-5, safety requirements could be checked by **Continuous Monitoring**

# Layer 7: Functionality (App)



# Cyber Resilience Act

- European Union is still lacking an all-encompassing approach to Cybersecurity
- Cybersecurity provisions in current legislation are limited to specific product groups, incomplete or only applicable on a voluntary basis (why was “Automotive” fully excluded from CRA???)
- Why has European legislator not made use of the existing Cybersecurity Act (CSA) framework by simply making its schemes, together with their associated assurance levels and conformity assessment procedures binding?
- Instead, the European legislator opted for a new horizontal policy framework that, similar to the CSA, does not only cover tangible digital products such as connected devices, but also non-tangible digital products such as software products embedded into connected devices.
- We very much appreciate that all products under the scope of the CRA will have to comply with the proposed cybersecurity requirements, irrespective of their risk level. Thus, all manufacturers will be obliged to take appropriate cybersecurity measures before placing their products on the market as well as during their products’ lifecycle.
- Apart from setting out ambitious cybersecurity requirements, it is crucial to ensure their consistent and effective compliance.

# Cyber Resilience Act

- The European legislator has rightly chosen a risk-based approach:  
The higher the risk level of a product, the more stringent the applicable conformity assessment procedures.
- However, the proposal falls short of implementing the risk-based approach consistently and coherently.

The Cyber Resilience Act (CRA) proposal is a starting point, but needs further strengthening on a number of issues

- a coherent and stringent implementation of the risk-based approach
- corresponding conformity assessment procedures.

# Cyber Resilience Act

## Central demands by the TÜV association

- 1. Stipulate an independent conformity assessment for all critical products
- 2. Expand the list of critical products to include, amongst others, consumer products
- 3. Require the application of harmonized standards to non-critical products for a presumption of conformity
- 4. Ensure coherence with conformity assessment procedures in sectoral product legislation
- 5. Ensure coherence with cybersecurity provisions of sectoral product legislation