CYBERSECURITY IN DE PRAKTIJK

Technische risico's en productveiligheid

Techlink
Linking technicians

wpp
warmtepomp platform

PV-Vlaanderen
fotovoltaïsche zonne-energie

CYBERSECURITY IN DE PRAKTIJK

Technische risico's en productveiligheid

1. Trusted Cybersecure Connected Products in Energy Transition – Ludwig De Locht (Sirris)
2. Technical risks and product security – Vincent Haerinck (Toreon)

Techlink
Linking technicians

wpp
warmtepomp platform

PV-Vlaanderen
fotovoltaïsche zonne-energie

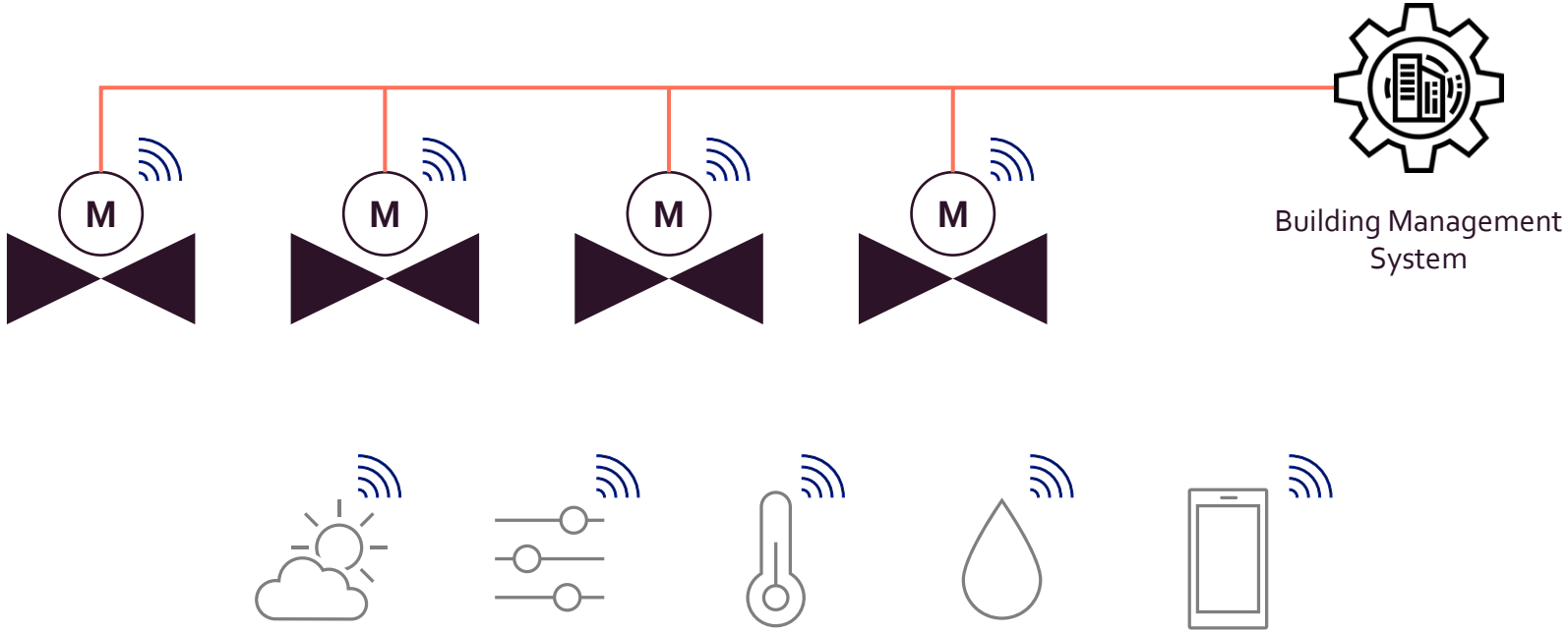
The innovation companion of the technology industry

Trusted Cybersecure Connected Products in Energy Transition

Ludwig De Locht – Program Manager Digital Security

innovation forward

When Everything Connects, Security Gets Harder



CRA – a new regulatory reality

Objective:	Scope:	Who is affected?
• Ensure digital and connected products on the EU market have a baseline level of cybersecurity throughout their lifecycle.	• Applies to *hardware and software products with digital elements* (e.g., IoT devices, embedded systems, applications, cloud-based components). • +data processing solutions	• Manufacturers of connected products • Importers and distributors • Software developers and vendors • System integrators

https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Requirements

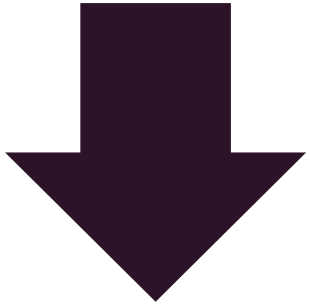
- **Security-by-design and by-default** in product development
- **Vulnerability handling**: monitoring, disclosure, and patching processes
- **Cyber risk assessment** and mitigation plans
- **Compliance documentation** (technical file, EU declaration of conformity)
- **CE marking** including cybersecurity compliance
- **Conformity assessment procedures**, which vary by product risk level

Start CRA Compliance with Your Digital Product Risk Assessment

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

Annex I – Section 1



YOU IDENTIFY YOUR RISK ASSESSMENT

3-step risk assessment framework

Identify What Needs Protection

What systems, assets, data cause major damage if hacked?

Assess the Biggest Threats

- What are the most likely cyber threats (phishing, ransomware, 3rd party)?
- Use a low-medium-high rating

Act Mitigate & Monitor

- Simple cost-effective security actions (backup, MFA, training)

Trusted Cybersecure Connected Products in Energy Transition

COOCK+: Practical Support for Your Company

Project Objectives:

- ✓ Help **SMEs in the energy transition** sector comply with the **EU Cyber Resilience Act (CRA)**.
- ✓ Support SMEs in **designing, acquiring, configuring, and testing** connected securely.
- ✓ Provide **clear, actionable guidelines** and tools tailored to SMEs with **limited R&D capacity**.

CRA – Why Act Now

2027 is closer than it seems

- Build security into products from the start
- Formalize vulnerability handling and disclosure
- Document risk assessments to demonstrate compliance
- Gain visibility into third-party components (SBOM)

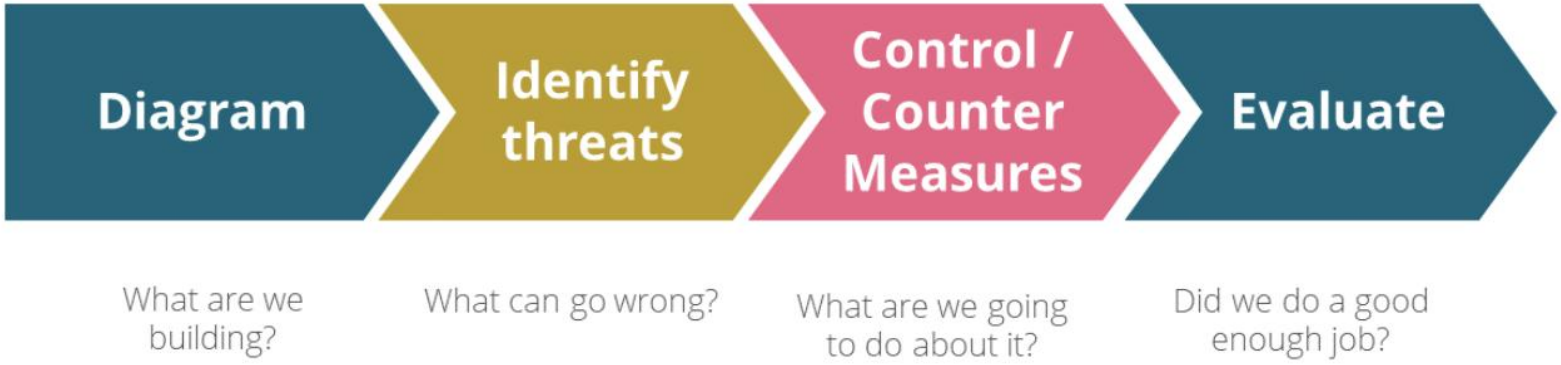
Making Risk-Based Security Actionable with Threat Modelling

Define the system and what stakeholders expect

Apply proven attack scenarios to exposed system entry points

Evaluate the risk of each scenario

Select effective defences and mitigations



Ludwig
De Locht

PROGRAM MANAGER DIGITAL SECURITY

0474 / 96.44.89

ludwig.delocht@sirris.be

TOREON

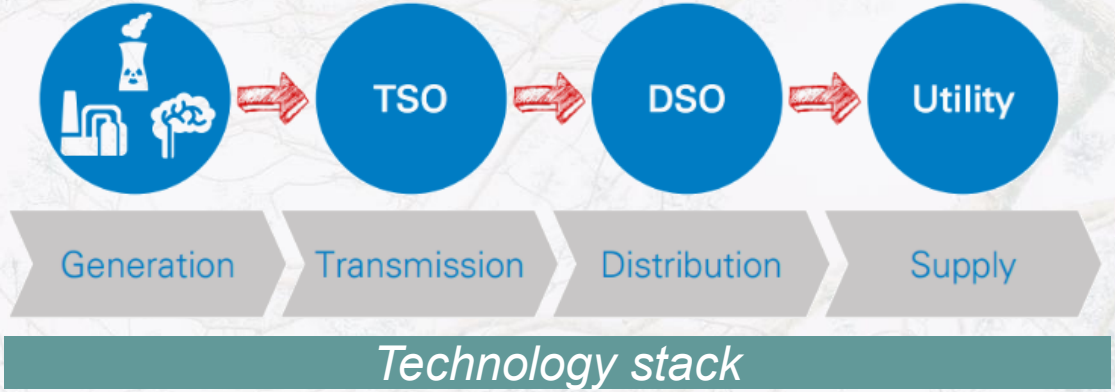
Cyber security in practice

Technical risks and product security

#whoami

- 10y+ Cyber security
- 10y+ Energy

SCAN ME




vrt nws
DeMorgen.
LEVEN
MENINGEN
POLITIEK
Dossier Zonnepanelen
Achtergrond Black-out
EURACTIV
Ukraine Defence The Capitals Politics Economy | Newsletters Videos Events Jobs Advocacy Lab Public Projects
Energy, Environment & Transport
Advocacy Lab Content
EU's energy transition resilience needs action, gas infrastructure funding
Europe needs low-carbon hydrogen, but there's also a push to develop renewable gases and to incentivise the

Product security

Not cutting it up in separate parts

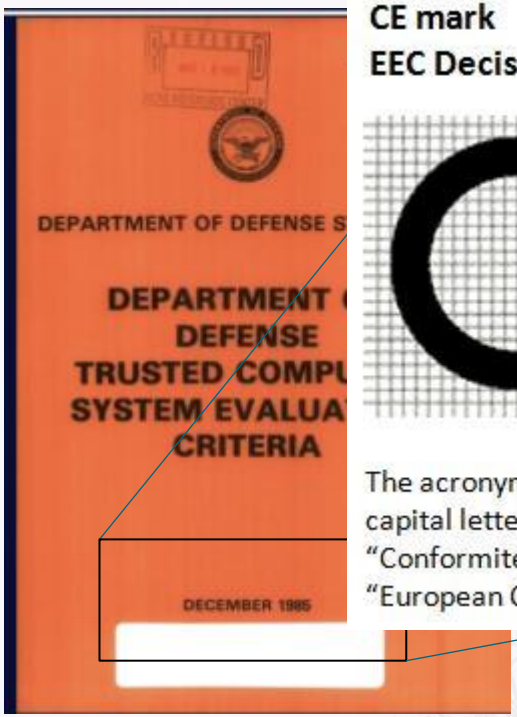
Product security is a **holistic** approach to **building, delivering, and maintaining** secure products (hardware, software, devices) across their **entire lifecycle**, from design to end-of-life, by embedding security into every stage to protect against cyber threats, tampering, and data breaches, ensuring **resilience** and **trust**.

Getting hit and getting back up again

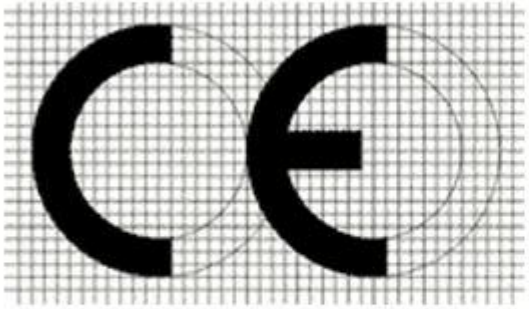
What is a product? ☺

- An article or substance that is manufactured or refined for sale *from Oxford Languages*

Is it new?



CE mark
EEC Decision 93/465/EEC



The CE mark was officially published in the EEC Decision 93/465/EEC, date 22 July 1993.

The conditions pertaining to the usage of the CE mark are stated in the annex of the EEC Decision 93/465/EEC.

The acronym "CE" is composed of the capital letters of a French expression "Conformité Européenne", translated as "European Conformity".

Do I need product security?

Product Security

Supply Chain Security

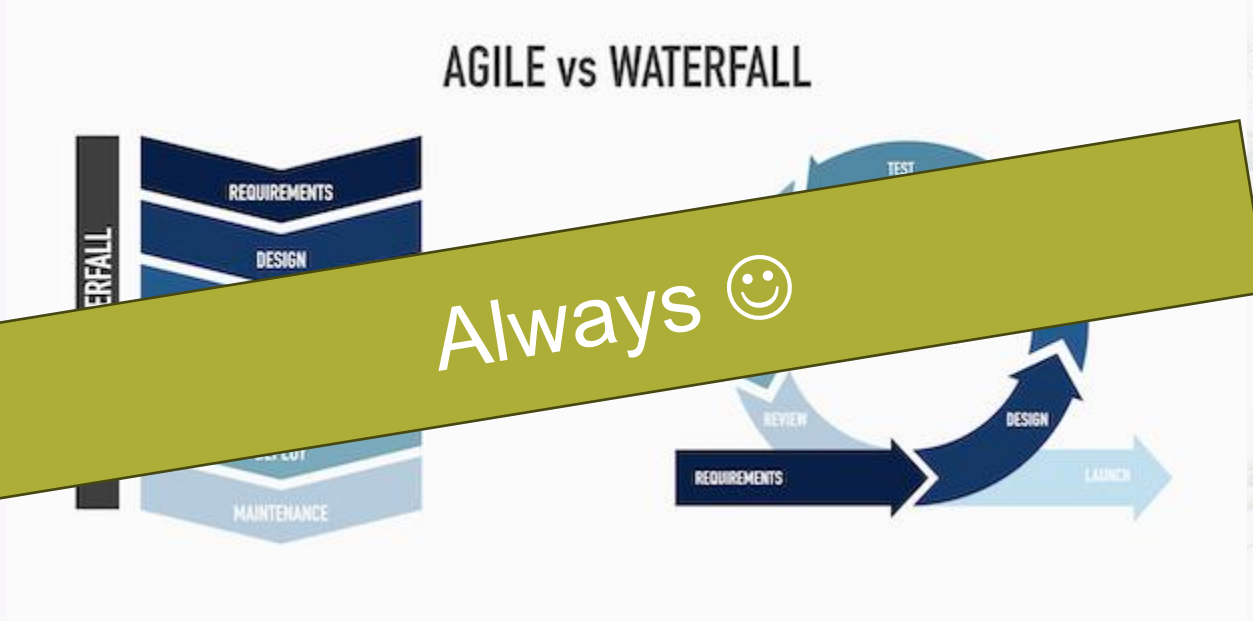
Do I need product security?

CRA

NIS2

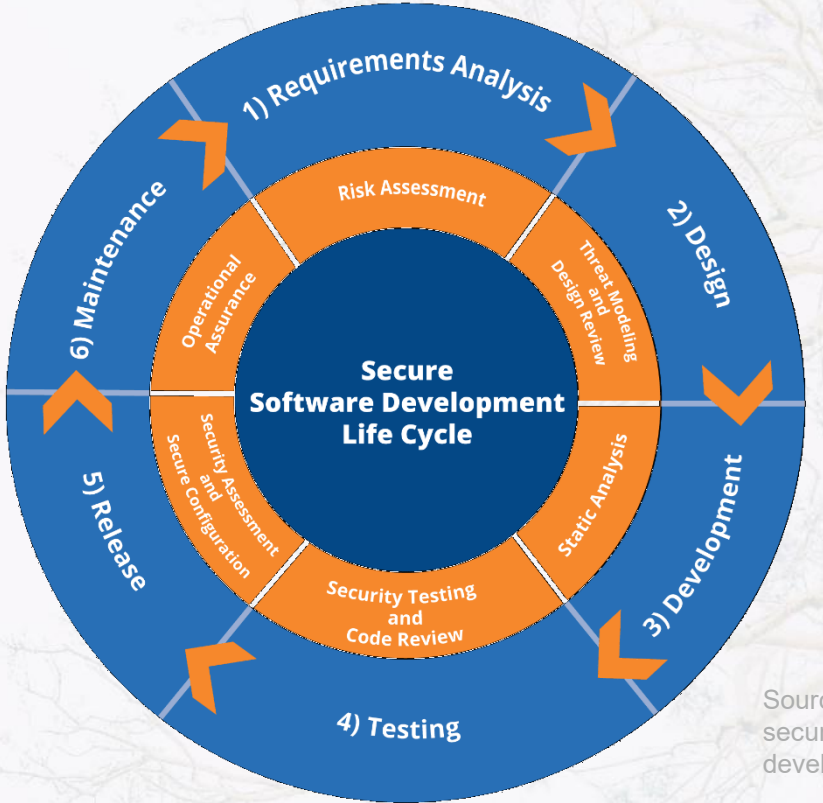
When do I need to apply product security?

Software/System Development Lifecycle (SDLC)



Source: https://www.easyagile.com/blog/software-development-methodologies

Secure SDLC (SSDLC)



Source: https://www.digitalmaelstrom.net/it-security-services/secure-software-development-lifecycle-ssdlc/

How do you know a product is secure?

Producer	• Design • Document • Test / Certify
Consumer	• Require • Test/Assess • Assure/Insure

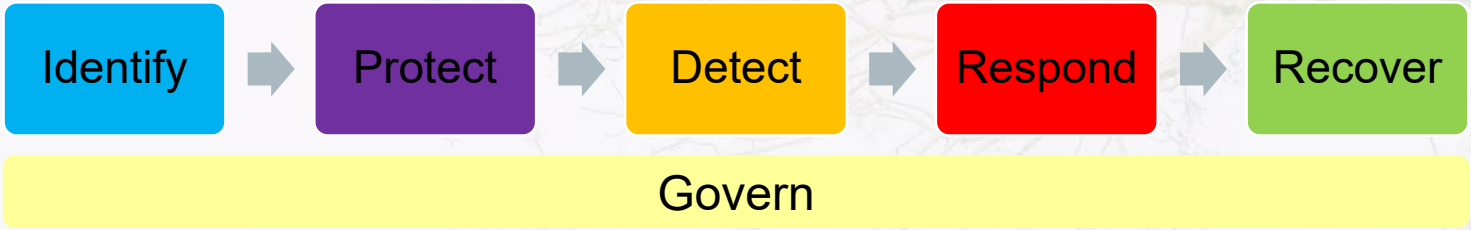
What can I do to secure products?

What can I do: basic judgement

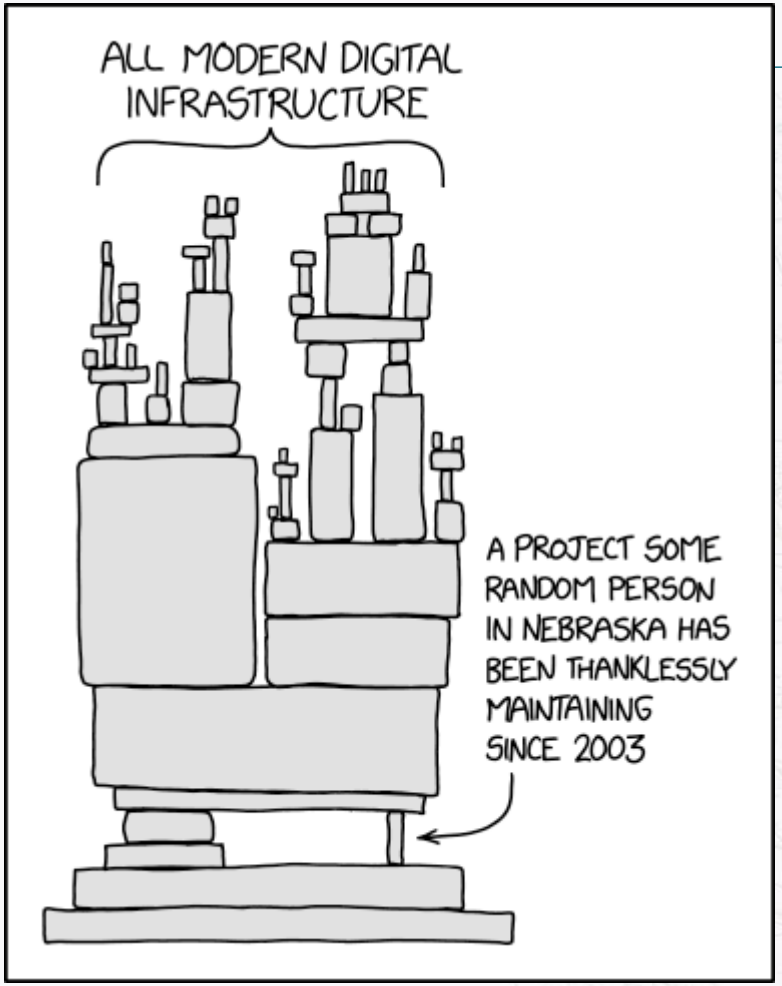
What should I do: best practice

What must I do: CRA if applicable, otherwise use risk-based approach

What can I do?



Identify



Source: https://xkcd.com/2347/

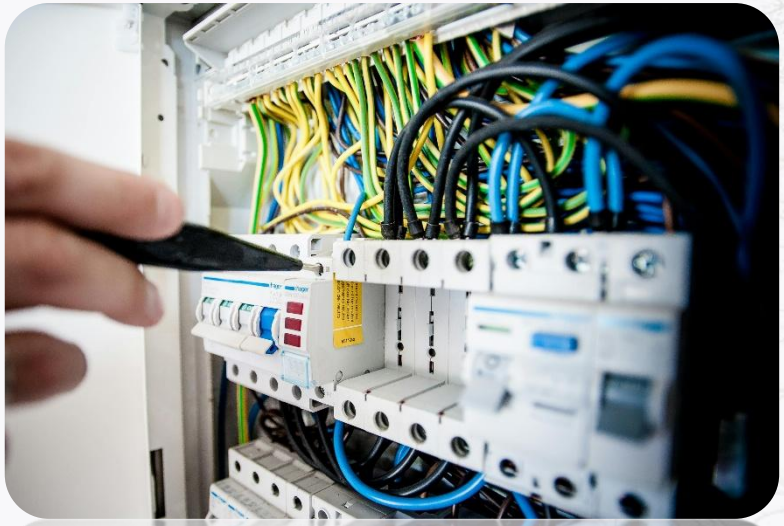
SBOM

- Know the components you create and integrate (with)
- See Log4j/React/…

Suppliers

- Document and prioritise
- Do they offer services/products you can easily replace?
- Are they monopolists?
- How “risky” are they?
- Do they have attestations/certifications?

Operating environment

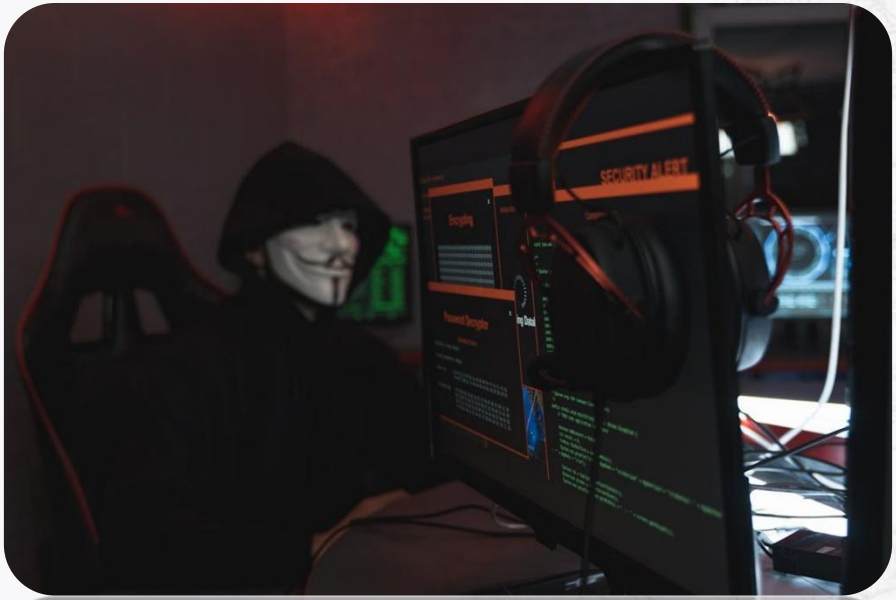


- Plant vs residential
- Deployment size vs scale
- Isolated vs connected

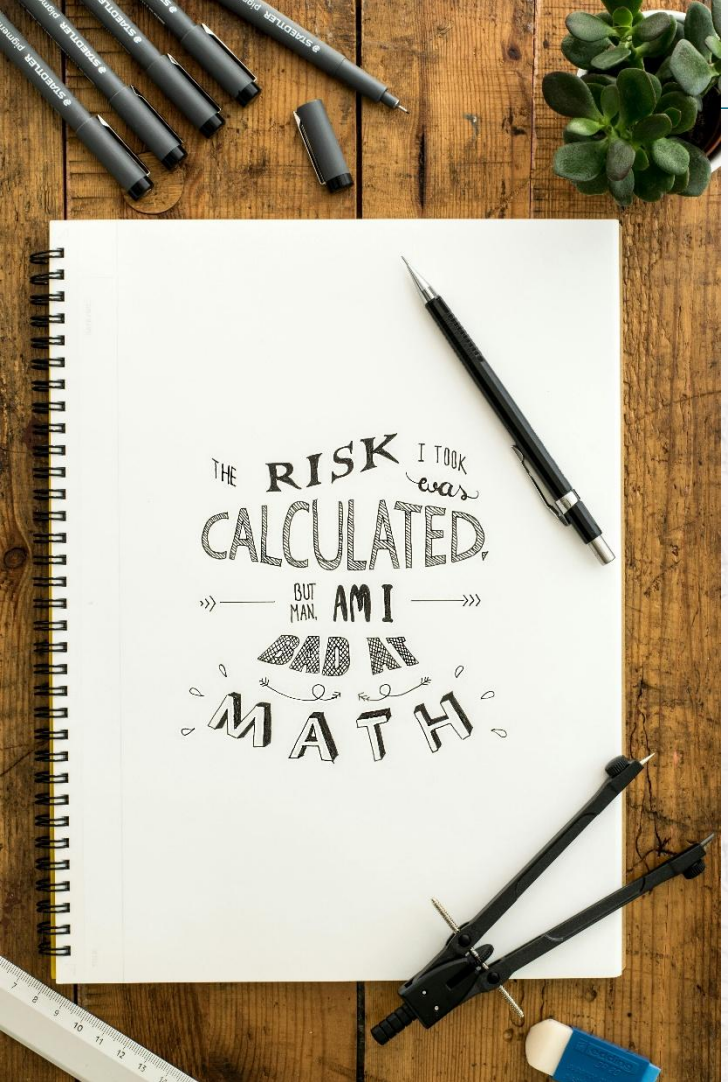
Document data flows

- Expected communications
  - Call home, monitoring, …
- Non-standard communications
  - Built-in but unused

Vulnerability identification



- Threat intel
  - E.g. Cyber Threat Research & Intelligence Sharing | CCB Safeonweb
- Disclosure management
- Vulnerability analysis



Analyse risk

- Perform threat model or risk analysis
- Define security requirements and drivers
- Analyse vulnerabilities in code, product, …

Protect

Access management

- Authenticate users – preferably strongly and securely
  - **Force** unique password
- Authenticate other components
  - Use secret non-embedded keys!
- Least privilege
  - No “Admin” account for everyone
  - Define roles – user, installer, monitor, …

Awareness

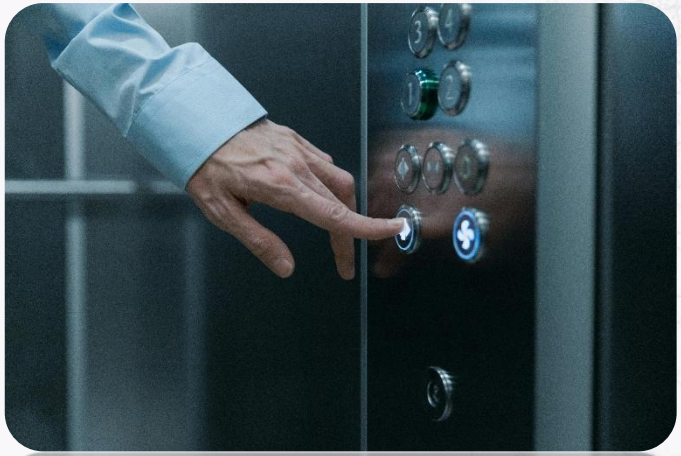
- Educate users, personnel, suppliers, …

Data protection

- At rest
- In motion
- In use

- Safeguards like back-ups
- Sensitive data: secrets, …

Secure operation



- Configuration management
- Software and hardware maintenance
- Usage monitoring/logging
- Detection of unauthorised software
- Resilient operation

Home Assistant

Default unique password
HTTPS by default
Minimal ports open
Easy guide to set up

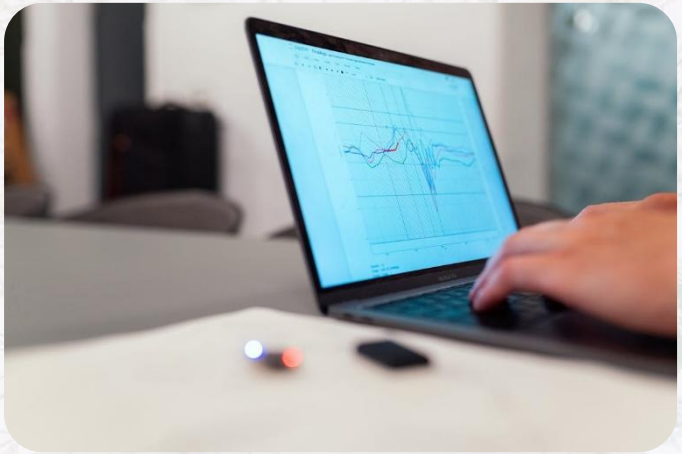
openHAB
empowering the smart home

Default passwordless
HTTP by default
Minimal ports open
Difficult setting up

Detect

Monitoring

- Physical environment
- Networks and services
- Hardware and software parameters
- Usage and activity: internal and external
- Correlation from multiple sources
- Incident generation



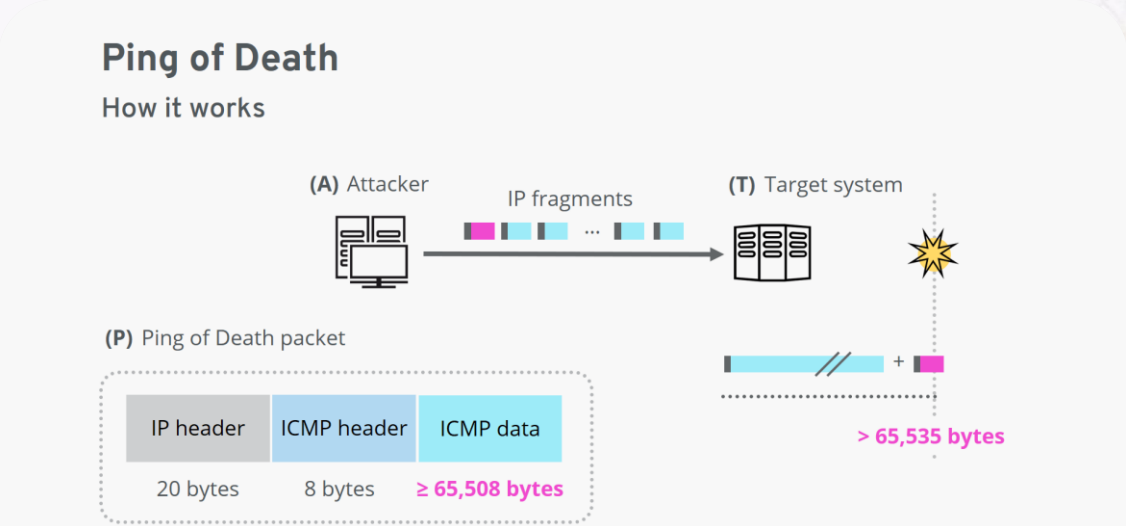
Faults in hardware hacking

Lennert Wouters reveals one of the first security breakdowns of Starlink's user terminals

COSIC researcher Lennert Wouters managed to hack into a Starlink satellite dish. It only cost him $25 worth of parts to create a tool that allows custom code to run on the satellite dishes. His homemade printed circuit board (PCB) launched a fault injection attack to bypass the security protocol. This way, the researcher managed to get into locked parts of the system.

Source: Lennert Wouters reveals one of the first security breakdowns of Starlink's user terminals - COSIC

Network-based attacks



Source: https://www.ionos.com/digitalguide/fileadmin/DigitalGuide/Schaubilder/how-a-ping-of-death-works.png

Respond

Plan

- Incident response process and actions
  - Fail-secure, fail-closed or fail-open?
- Incident criteria definition
- Containment of incidents

Analysis inputs

- Incident data and metadata collection
- Stakeholder engagement

Recover

Secure restoration

- Integrity verification during recovery
  - Secure boot/secure load/…
- Recovery actions definition
  - Altered startup cycle/self-checks/..

Govern

Stakeholder analysis

- Internal and external
- Roles and responsibilities
- Objectives
- Communication lines

Risk management

- Supply chain
- Customers, employees, developers, partners
- Risk appetite and tolerance
- Due diligence
- Risk and response register
- Threat modeling

What must I do?

- Check laws and regulations

Effect of EU Regulations

Where can I find help and guidance?

1. OWASP SAMM (Software Assurance Maturity Model) – Prescriptive standard – High level
2. Eclipse Open Regulatory Compliance WG – Open Source focused
3. IEC62443-4-1 and 4-2
4. ETSI TS 102 165-1
5. NIST SSDF
6. …

CRA

CRA – Recap

Adopted in 2024

No transposition needed (EU regulation)

Full activation 11/12/2027

Product security now part of CE-label

Shared responsibility

Mandatory reporting for vulnerabilities and incidents

Reference: https://ccb.belgium.be/regulation/cra

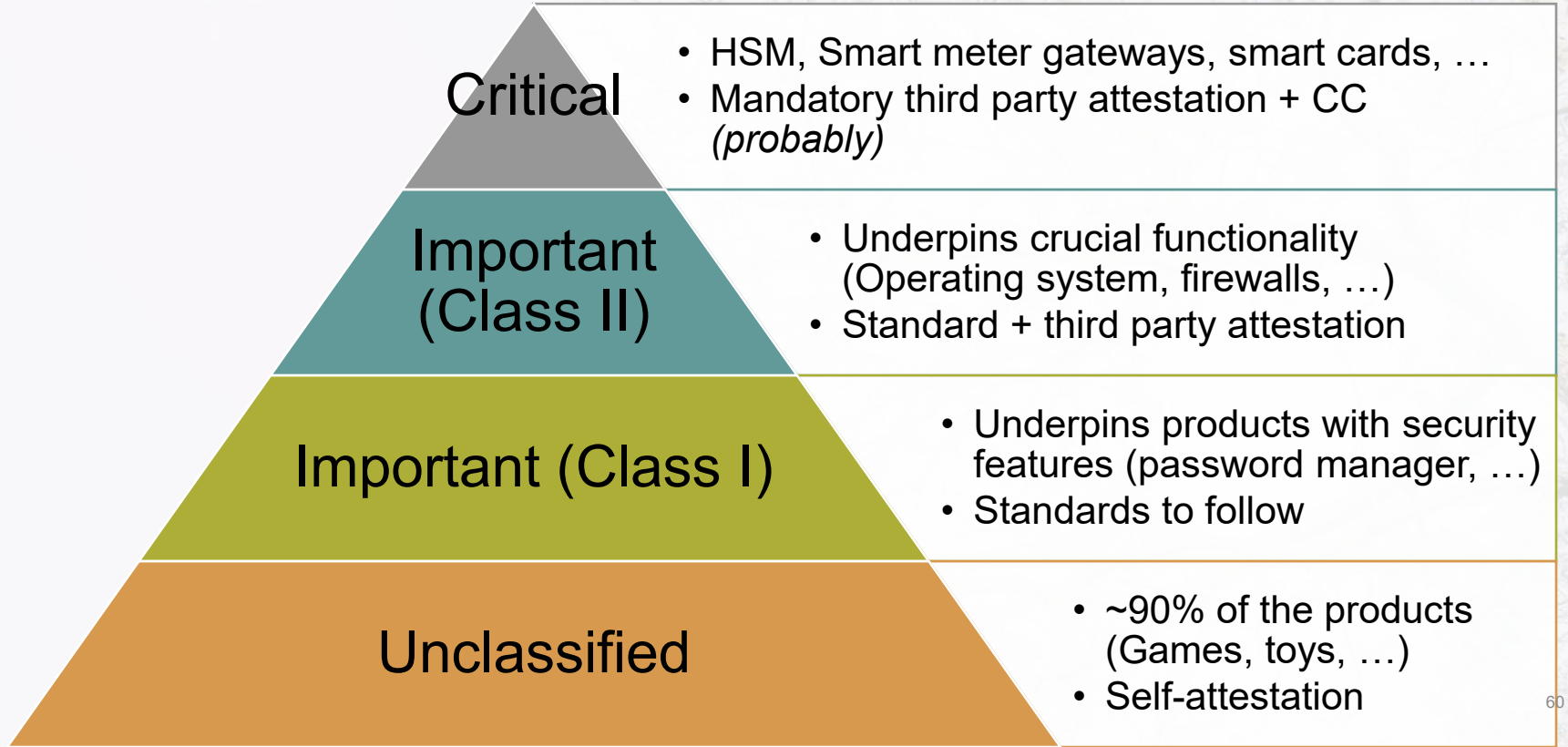
CRA - Scope

"Product with digital elements" *(≈connected products)* ***being placed on the market***

NOT in scope
✗ SaaS and web platforms and managed services (covered by NIS2)
✗ Built-in software on device for basic functions like fridge firmware (≈not connected)
✗ Cars, medical devices, aviation, shipping, rail freight (temporary under CRA until law is published), defense, … (specific laws)
✗ Non-commercially open source, e.g. libraries etc (voluntary)

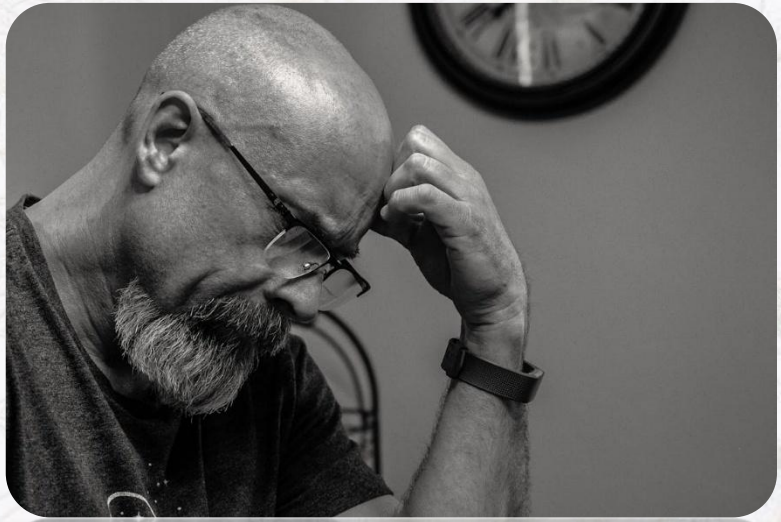
In scope
✓ e.g. smart TVs, soundbars, …
✓ e.g. digital carrier devices with software (e.g. OS, software applications, .)
✓ Web browser
✓ Mobile apps on your phone
✓ Smart devices like camera's, but also the platforms that process their data
✓ Integrating open source into your product = treating it as your own code/supplier

Categories

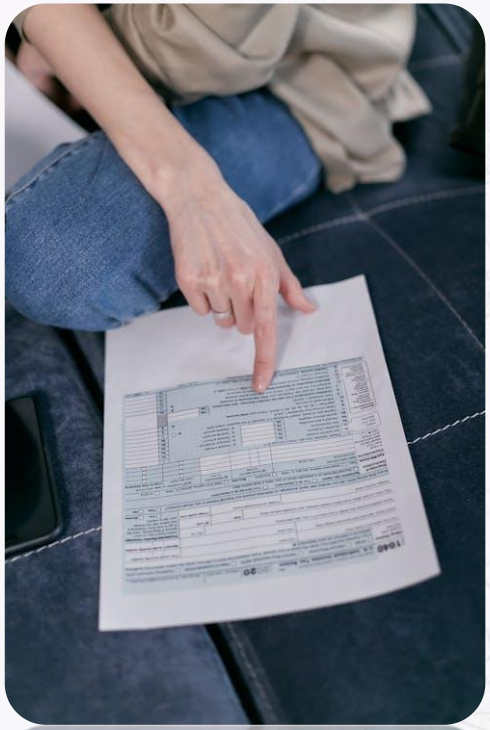

Critical
• HSM, Smart meter gateways, smart cards, …
• Mandatory third party attestation + CC *(probably)*
Important (Class II)
• Underpins crucial functionality (Operating system, firewalls, …)
• Standard + third party attestation
Important (Class I)
• Underpins products with security features (password manager, …)
• Standards to follow
Unclassified
• ~90% of the products (Games, toys, …)
• Self-attestation

Anticipate future laws and regulations

- Check “common sense”
  - Document secure configuration and conformity
  - Secure out of the box
  - Implement basic security features (MFA, …)
  - Risk based decision-making
  - Make product adaptive throughout lifespan
  - Check vulnerability periodically



How to use secure products?



- RTFM if available
- Use your best judgement
- Keep in mind
  - Secure products <> Secure organisation
  - Use <> Intended use


PARAMECIUM

Thank you!