CRA

Cyber Resilience Act

cybersecurity@avl.com

Agenda

1 **CRA in a Nutshell**

2 **Affected Products and Categories**

3 **What and When – Requirements and Timeline**

4 **How AVL Supports You**

What Does AVL Stand For?

Building resilience through technology, process, and experience.

Core Tech

- Embedded systems
- Software platforms
- Functional safety

Cybersecurity Expertise

- Secure embedded software development
- End-to-end secure development lifecycle
- Vulnerability management & testing

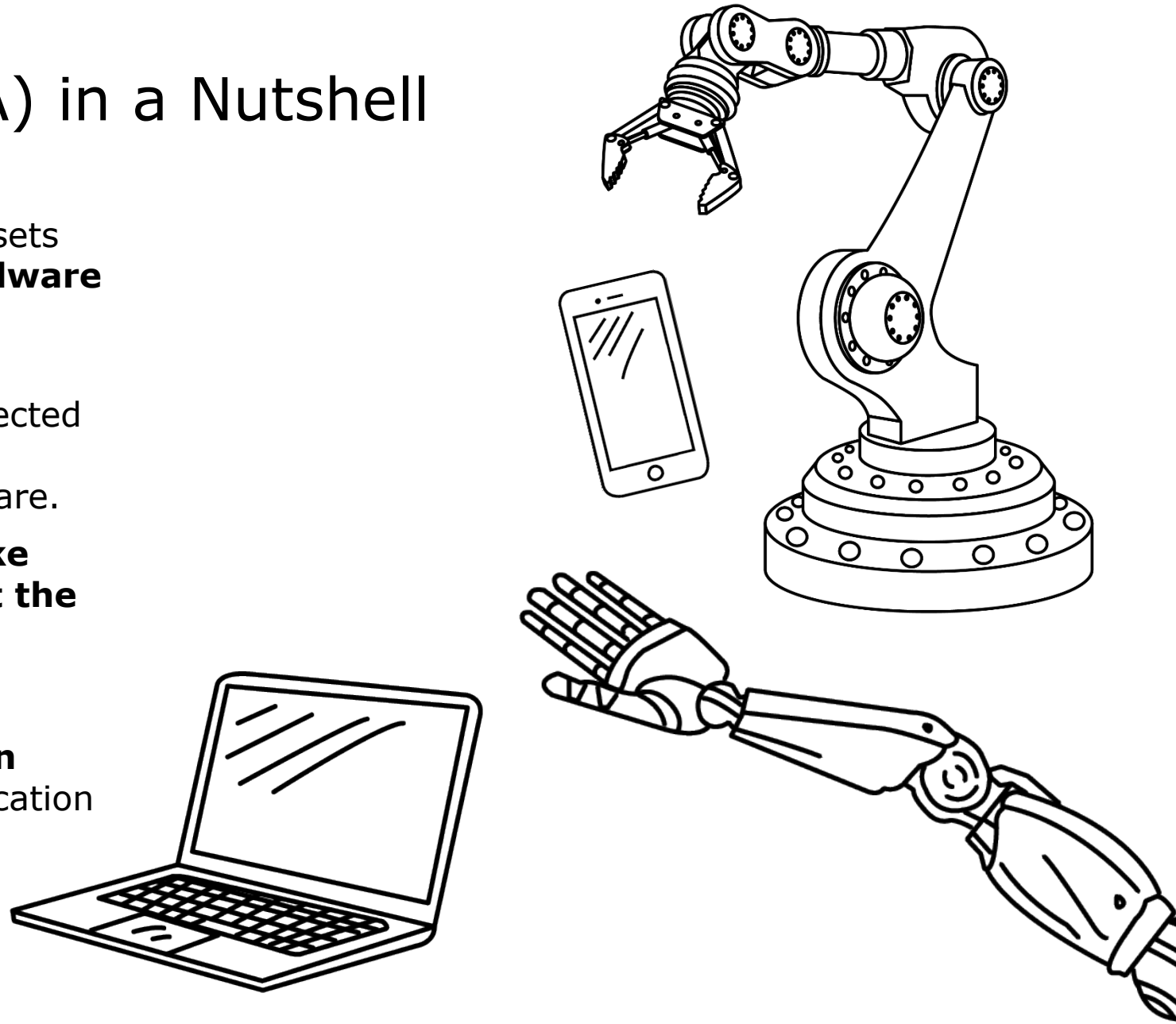
Proven Experience

- Compliance & certification
- Integration of system and cybersecurity know-how
- Established process frameworks

Cyber Resilience Act (CRA) in a Nutshell

- The European Cyber Resilience Act (CRA) sets **cybersecurity requirements** for all **hardware and software products with digital elements** placed on the EU market.
- It applies to any product that can be connected to a device or network – including both connected hardware and standalone software.
- The CRA ensures that **manufacturers take cybersecurity into account throughout the entire product life cycle**, from design to maintenance.

  It also introduces a **common certification framework** for information and communication technology (ICT) products, services, and processes.



Cyber Resilience Act (CRA) in a Nutshell

- **Excluded Products Due to Existing Cybersecurity Regulations:**
  - Vehicles (UNECE R155, ISO/SAE 21434)
  - Civil Aviation (EU 2018/1139)
  - Medical Devices (EU 2017/745, EU 2017/746)
  - Marine Equipment
  - Products Related to National Security (e.g., military)
  - Non-Commercial Open-Source Products

Headline

CATEGORY	DEFAULT "UNCLASSIFIED"	IMPORTANT "CLASS I"	IMPORTANT "CLASS II"	CRITICAL PRODUCTS
Examples	Smart home devices, Printers, Media Player SW	Password Managers, Identity Management Systems, Browsers, Routers, OS, VPN	Hypervisors, Firewalls, IDS/IPS Tamper-resistant micro-processors	Smart meter gateways, smartcards or similar devices, secure elements, HSM
Conformance	Self Assessment	Harmonized standards ensuring CRA principles are met	Third Party Assessment	EUCC European Common Criteria Assessment

CRA Requirements Overview (1)

01 **EU Declaration of Conformity** – stating the conformity of digital products with the essential requirements.

02 **Technical Documentation** – encompassing all necessary evidence to demonstrate compliance. This includes the outcomes of technical security processes.

03 **Information and Instructions to the User** – product users need to be informed about cybersecurity.

CRA Requirements Overview (2)

Assessment of the cybersecurity risks associated with the product

(1) **Product-related** essential requirements (Annex I, Part I)
(2) **Vulnerability handling** essential requirements (Annex I, Part II)
(3) **Technical docu**, including information and instructions for use (Annex II + VII)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Part II)

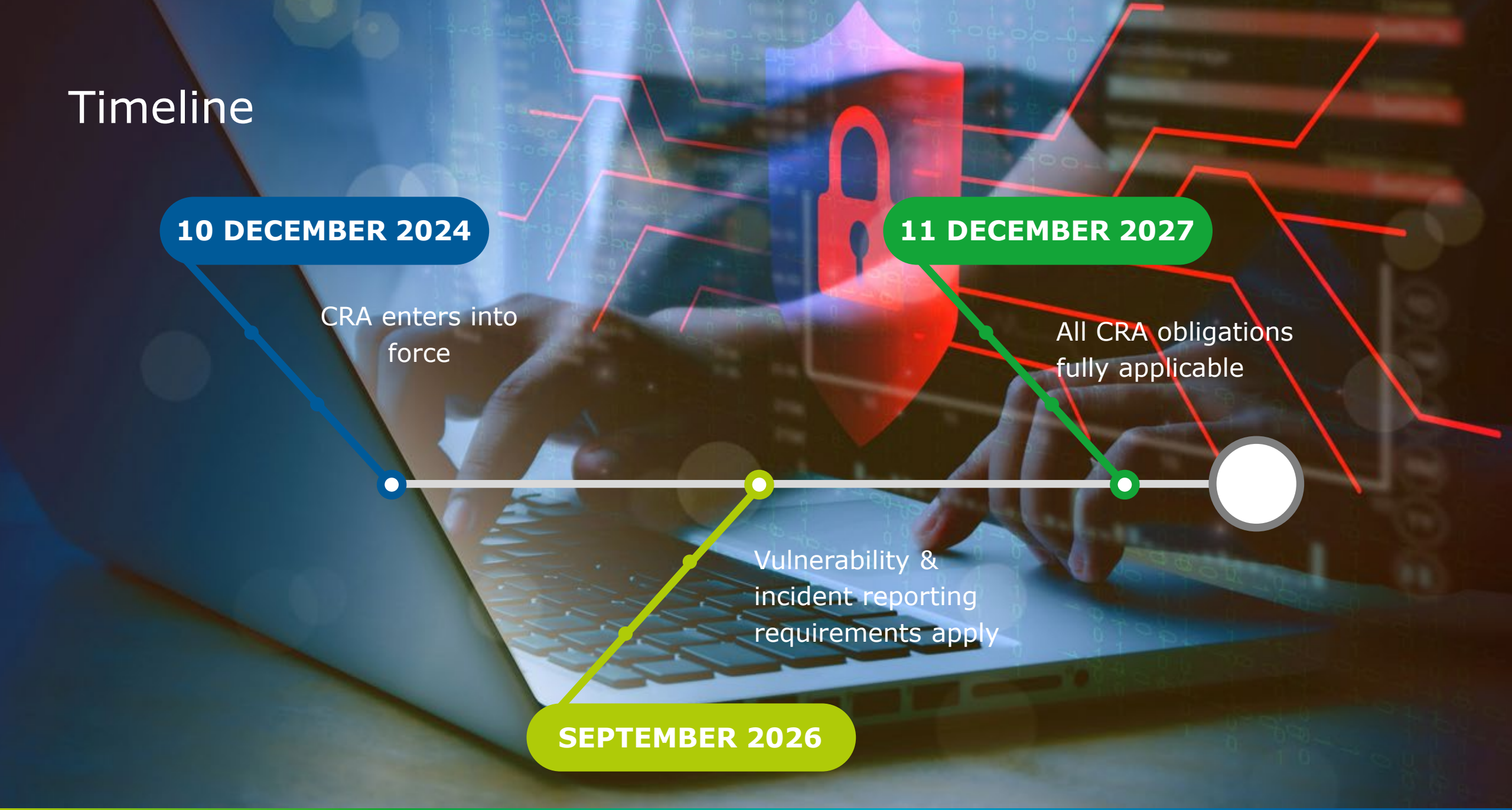
Design, development and production phase

Maintenance phase (‚expected use time')

(1) Obligation to **report** any actively exploited vulnerability and severe incident to the CSIRT and ENISA
(2) Obligation to **inform** the impacted users
(3) Obligation to **deliver free of charge security-updates**

Adapted from the European Commission

Timeline


10 DECEMBER 2024
CRA enters into force
SEPTEMBER 2026
Vulnerability & incident reporting requirements apply
11 DECEMBER 2027
All CRA obligations fully applicable

How AVL Supports You

Consulting

- Product Security Management
- Trainings & Workshops
- Gap Analysis / Compliance Check
- Risk & Self-Assessment Support
- CRA Implementation Guidance
- Security Standards (ISO 27001, TISAX, ISO/SAE 21434, NIS-2)

Secure Development

- DevSecOps Toolchain Integration
- Process Consulting
- Embedded Software for Secure Devices
- Cloud / Backend Digitalization
- IoT & OT Hardware Development
- Industrial Software Engineering

AVL CRA Starter Package – Quick Entry into CRA Compliance

Adaptable to your needs

What's Included:

- 4h Training & Workshop
- On-site introduction to CRA requirements
- Discussion on company/product impact
- Planning next steps and gap analysis

Gap Analysis & Compliance Check:

- Assessment via interviews, document review, product inspection
- Report with gaps, risk ratings & recommendations
- Presentation of results

Thank you

www.avl.com