ARM KNOWLEDGE LAB: DESIGNING THE FUTURE

DAY 1

CRA – Introduction and Overview

Daniel Bartz, EBV Elektronik

Arm Knowledge Lab:
Three short and compact sessions

Day 1

Secure by Design – From Threats to Trusted Devices

Day 2

AI at the Edge – Building Smarter Embedded Systems

Day 3

Safety-Critical Systems – Engineering Reliability

Find more presentations from our Arm Knowledge Lab:
https://www2.hitex.com/arm-knowledge-lab-2026-download

EBV Elektronik
I An Avnet Company I

Technology. Passion. EBV.

Cyber Resilience Act
Introduction and Overview

16.06.2026

Daniel Bartz, Technology FAE

EU Cyber Security Regulation

NIS2
Critical IT services

- IT infrastructure
- Server
- Network

RED
Internet connected Radio equipment

- Internet connected radio equipment
- Connected toys
- Childcare and monitoring
- Wearables

CRA
All connected devices, internet or otherwise

- Connected devices
- Sub-Components
- Software components
- Finished Products

enisa
European Network and Information Security Agency

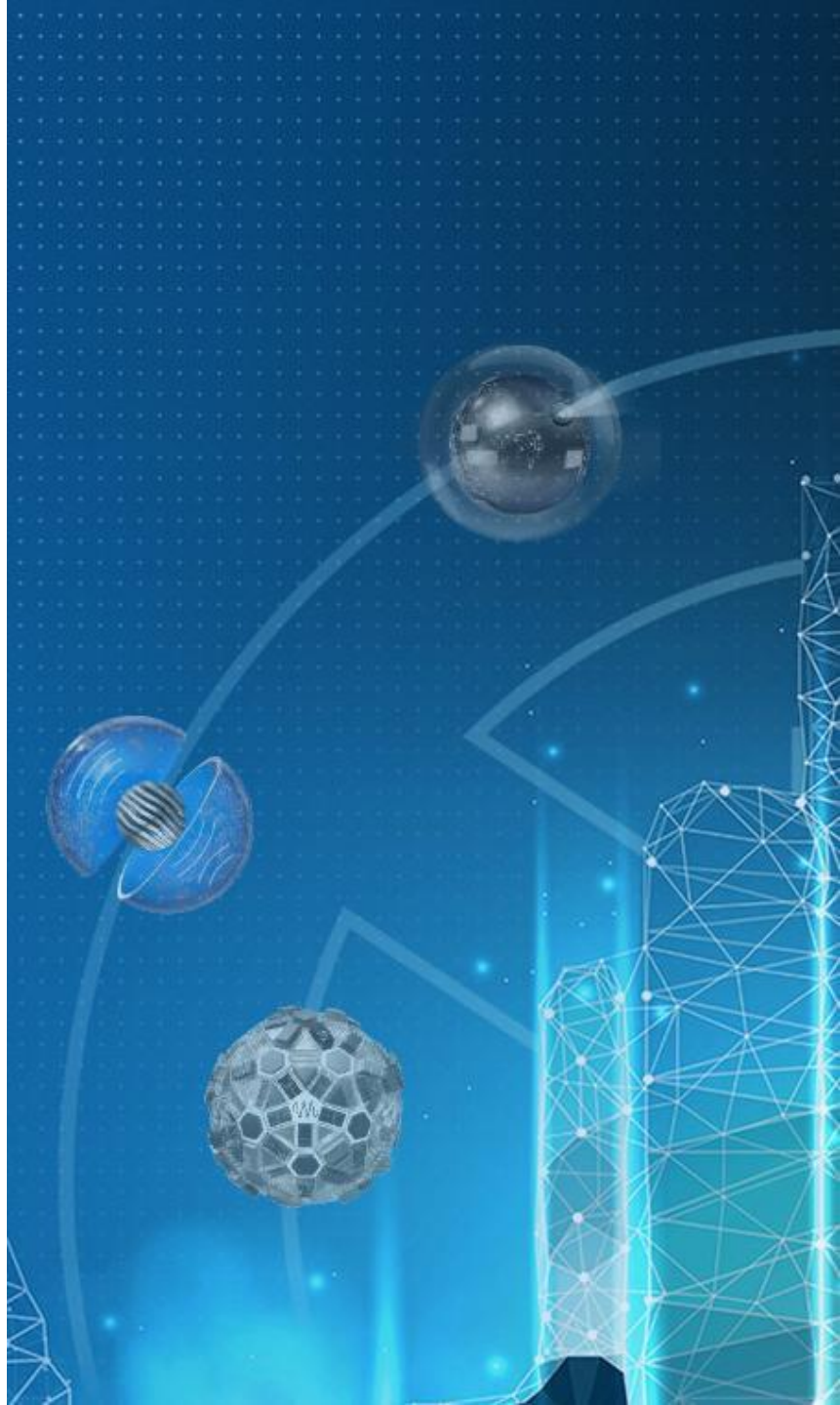
EBV Elektronik
An Avnet Company

Time left until CRA is mandatory

544

DAYS

until the applicability of the EU Cyber Resilience Act



Development Process

The proposed Regulation will apply to

all products with digital elements

whose intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

But it does <u>not</u> apply to products (with digital elements) within the scope of …

Regulation (EU) 2017/745 – medical devices for human use and accessories for such devices

Regulation (EU) 2017/746 – in vitro diagnostic medical devices for human use and accessories for such devices

Regulation (EU) 2018/1139 – high uniform level of civil aviation safety

Regulation (EU) 2019/2144 – Automotive Type Approval General Safety Requirements

Regulation (EU) 2014/90/EU - Marine Equipment Directive (MED)

CRA Requirements (Annex I)

Essential Security Requirements

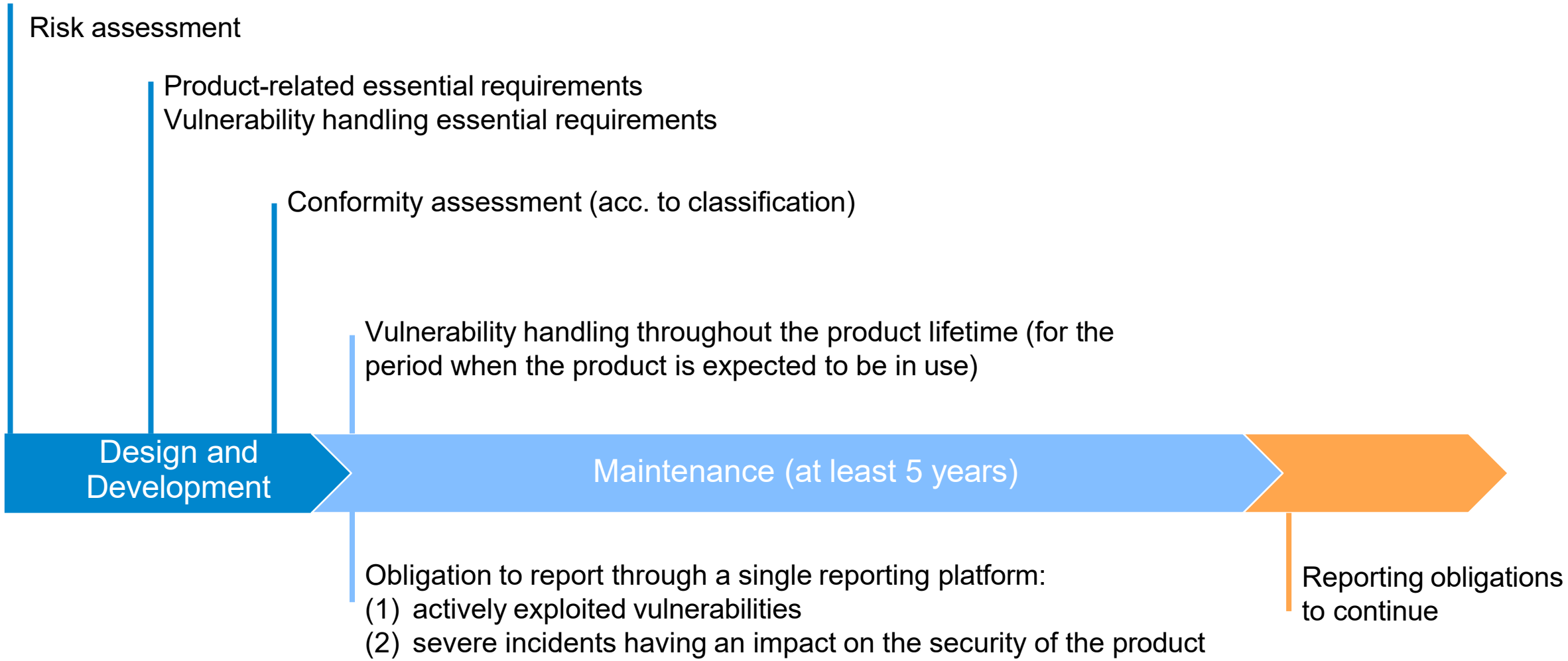
- No known, practically exploitable vulnerabilities. (2a)
- Security by design and by default. (1, 2b)
- Vulnerability management (2c)
- Access control (2d)
- Confidentiality and integrity of data in transit and at rest. (2e,2f)
- Availability of core functionality (2h)
- Minimization of data processing, attack surface and impact on other systems. (2g,l,j,k)
- Monitoring of security process (2l)
- Data portability (2m)

Exact requirements based on risk assessment

Vulnerability Handling Requirements

- Identify and document vulnerabilities
- Address and remediate vulnerabilities without delay. Provide security updates.
- Apply effective and regular tests and reviews.
- Share and publicly disclose information about fixed vulnerabilities.
- Policy on coordinated vulnerability disclosure.
- Share information about potential vulnerabilities in products with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities
- Provide for mechanisms to securely distribute updates.
- Ensure that security updates are available without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken

Obligations of Manufacturer



EBV Elektronik
An Avnet Company

Technology. Passion. EBV.

Product Classification

CRA Product Classification

Default	Important Product Class 1	Important Product Class 2	Critical Product
Self Assessment	Self-assessment only if against Harmonized Standard(s) (Module A)	3rd party - EU-Type examination and internal production control (Module B+C) ***(product assessment)*** 3rd party - Full quality assurance (Module H) ***(process assessment)***	3rd party - European cybersecurity certification scheme EUCC ***(product and process assessment)***
All other	• Identity management, access management, authentication and access control readers, including biometric readers • Products with digital elements with the function of VPN • Security information and event management (SIEM) systems • Public key infrastructure and digital certificate issuance software • Physical and virtual network interfaces • Routers, modem, switches. • Microprocessors with security-related functionalities • Microcontrollers with security-related functionalities • ASIC and FPGA with security-related functionalities • Smart home general purpose virtual assistants • Smart home products with security functionalities (lock, camera, etc.) • Internet connected toys that have social interactive features or location tracking features • Personal wearable products to be worn or placed on a human body that have a health monitoring or personal wearable products that are intended for the use by and for children. • …	• Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments • Firewalls, intrusion detection and/or prevention systems • Tamper-resistant microprocessors • Tamper-resistant microcontrollers	• Hardware Devices with Security Boxes • Smart meter gateways and other devices for advanced security purposes, including for secure crypto processing • Smartcards, secure elements

CRA Standards

30.08.2026

Horizontal Standards

30.10.2026

Vertical Standards

CEN Cenelec JTC 13
Cybersecurity and Data Protection WG6/WG9

EN 40000-1-1
Vocabulary

EN 40000-1-2
Principles of Cybersecurity

EN 40000-1-3
Vulnerability handling

EN 40000-1-4
Generic security requirements

Cenelec TC 47
Semiconductors and Trusted Chips

Cenelec TC 65
Industrial process measurement, control and automation

ETSI Technical Committee on Cyber Security

EN 304 617 Browser	**EN 304 636** Firewall	**EN 304 642** Network function telecom	**EN 304 631** Smart home assistants	**EN 304 625** Virtual Network Interfaces
EN 304 618 Password Manager	**EN 304 622** SIEM Systems	**EN 304 626** Operating Systems	**EN 304 633** Internet connected toys	**EN 304 621** Network Management Systems
EN 304 619 Anti Virus	**EN 304 623** Boot Manager	**EN 304 627** Router, Modem, Switch	**EN 304 634** Personal wearable	
EN 304 620 VPN	**EN 304 624** PKI	**EN 304 632** Smart home security	**EN 304 635** Virtualization	

Horizontal Standards

EN 40000-1-1: Vocabulary

EN 40000-1-2: Principles for cyber resilience
- CRA Annex I, Part 1, Requirement 1
- **Process** standards to ensure that products are developed and maintained with a risk based approach, covering any security risk.
- Implementation is covered via process documentation.

EN 40000-1-3: Vulnerability handling
- CRA Annex I, Part 2
- **Process** standard, to ensure the product is maintained in a secure state, using a risk based approach.
- Implementation is demonstrated via process documentation and action on the market, like updates, customer notifications, etc. .

EN 40000-1-4: Generic security requirements
- CRA Annex I, Part 1, Requirements 2 a-m
- **Product** standard, addressing a specific set of security requirements by mapping security objectives to a catalog of possible security controls.
- Implementation is demonstrated via the product and its technical documentation.

Vertical Standard Drafts available

docbox.etsi.org / CYBER / EUSR / Open

	sort by name/desc	sort by date/desc	sort by size/desc
☐	EN_304-617_V0.1.1_2026-04-04_Browsers_Early-draft.pdf	2026-04-17 17:17	1192,2 KB
☐	EN_304-619_V0.0.26_2026-04_Antivirus-Antimalware_Mature-draft.pdf	2026-04-30 20:00	2705 KB
☐	EN_304-620_V0.1.9_2026-04-27_Virtual-Private-Networks_Mature-draft.pdf	2026-04-30 16:37	1682,1 KB
☐	EN_304-621_V0.1.3_2026-04-20_Network-Management-Systems_Mature-draft.pdf	2026-04-21 10:21	2274 KB
☐	EN_304-623_V0.1.1_2026-05-04_Boot_Managers_Mature-draft.pdf	2026-05-04 8:02	2637,1 KB
☐	EN_304-625_V0.0.14_2026-04-17_Network-Interfaces_Mature-draft.pdf	2026-04-17 16:54	1715,4 KB
☐	EN_304-626_V0.2.0_2026-04-23_Operating-Systems_Mature-draft.pdf	2026-04-30 19:46	1644,3 KB
☐	EN_304-631_V0.2.1.4_2026-04-17_Smart-home-virtual-assistants_Mature-draft.pdf	2026-04-17 15:39	2136,1 KB
☐	EN_304-632_V0.2.1.4_2026-04-17_Smart-home-security-products_Mature-draft.pdf	2026-04-17 15:47	2141,5 KB
☐	EN_304-633_V0.2.3.3_2026-04-17_Internet-connected-toys_Mature-Draft.pdf	2026-04-17 15:54	2131,2 KB
☐	EN_304-634_V0.2.6_2026-04-17_Personal-wearables_Mature-draft.pdf	2026-04-30 19:07	2046,6 KB
☐	EN_304-635_V0.0.15_2026-04-20_Virtualization-Container_Mature-draft.pdf	2026-04-21 10:10	2843,8 KB
☐	EN_304-636_V0.1.0_2026-04-22_Firewalls_Mature-draft.pdf	2026-04-30 20:11	1529,8 KB
☐	ETSI Commenting Format for Open Consultation_v8.xlsx	2026-02-05 16:06	41,6 KB
☐	ETSI_CYBER-EUSR_Commenting_instructions_open consultations_17-04-2026.pdf	2026-04-17 15:03	150,9 KB
☐	OC1_ETSI_CYBER-EUSR_Comments_Resolutions_Public Version.xlsx	2026-01-15 14:25	58 KB
☐	OC2_ETSI_CYBER-EUSR_Comments-Resolutions_Public-Version_NOT-FINAL_Mar-23.xlsx	2026-03-23 15:50	58,6 KB
☐	OC3_ETSI_CYBER-EUSR_Comments-Resolutions_Public-Version_NOT-FINAL_Mar-23.xlsx	2026-03-23 16:12	57,7 KB

18 items.

https://docbox.etsi.org/CYBER/EUSR/Open

Important Process Steps

Product Security Incident Response Team (PSIRT)

Manufacturers must establish a dedicated team to handle and manage all vulnerability management actions, a PSIRT.

Tasks of the PSIRT

- Receive vulnerability reports
- Validate and triage them quickly
- Coordinate engineering and deliver fixes fast
- Communicate advisories transparently and safely
- Track and document lifecycle end-to-end

The ability to notify authorities about actively exploited vulnerabilities must be established by

11.09.2026

Cybersecurity Risk Assessments

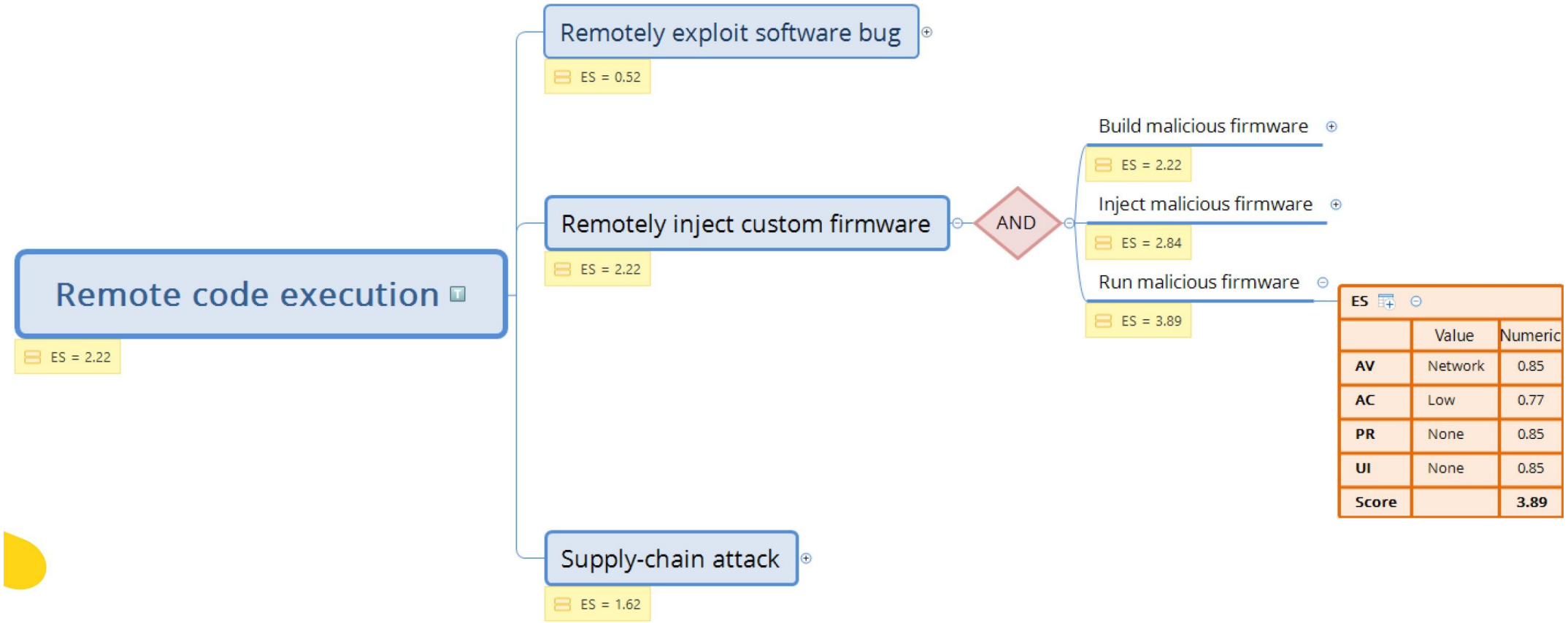
Design	Implementation	Robustness	External modifications
Missing authentication	Weak input validation	Bruteforce attacks	Physical modification (FIB)
Test mode	Runtime errors	Side-channel attacks	Fault injection (glitch, laser, EM)
Insecure update / key provisioning	Too many interfaces	Reverse engineering	Flash dump
…	…	…	…

Unrealistic to hope dealing with all unexpected behaviors.
We need to adopt a threat-driven approach.

Article 13.2, 13.3

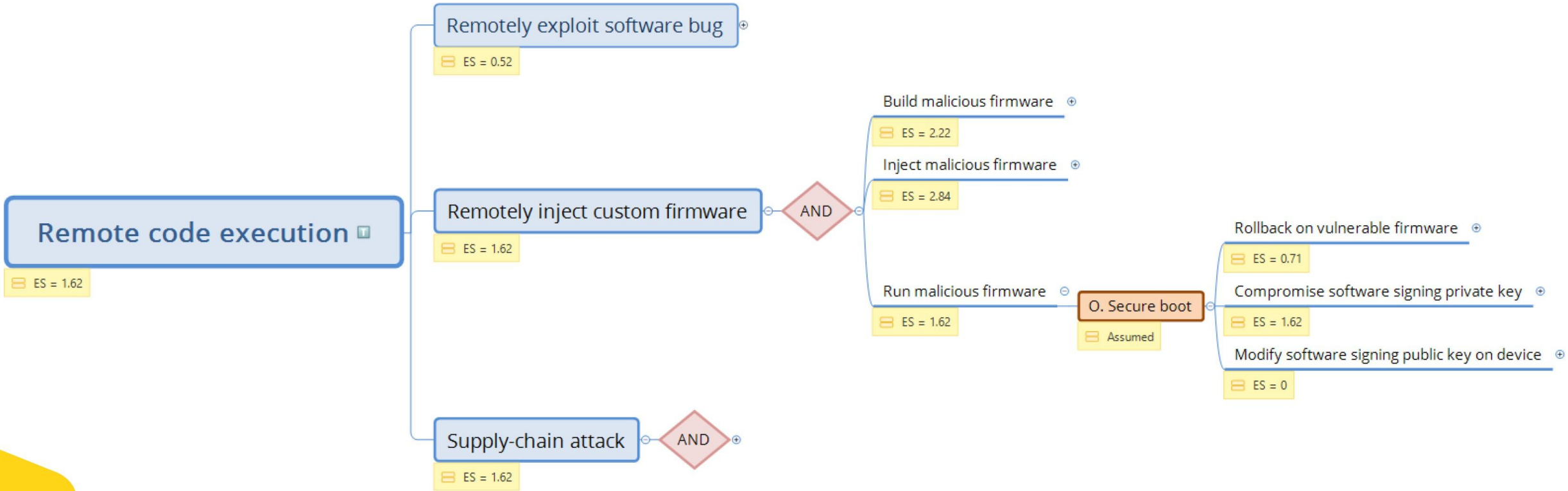
Cybersecurity Risk Assessments

Attack Tree using Common Vulnerability Scoring System (CVSSv3)



Cybersecurity Risk Assessments

Attack Tree using Common Vulnerability Scoring System (CVSSv3)



SBOM – Software Bill of Material

- Improve decision making
- SBOM typically generated during build or via source scanning
- Integrated with **vulnerability management** & asset inventory
- Supports **incident response** & faster patch decision-making
- Shared with authorities and customers (opt.) in machine-readable formats
- Streamline security audits & certifications

Current Standards & Ecosystem

- SPDX (ISO/IEC 5962) – compliance & licensing focus
- CycloneDX (OWASP) – security & supply-chain metadata (fast adoption)

https://spdx.dev/

https://cyclonedx.org/

SBOM – Best Practices

Using the SBOM to track CVE

Detect + automatic assessment

Detect applicable CVE using the SBOM and reference CVE databases

Optimized with an accurate filtering + leverages previous assessment

CVE SCAN automation

Manual assessment

Evaluate the impact of the CVE

Is the exploit possible on the product? What are the risks?

Cybersecurity Expert

No risk

CVE acceptable or not exploitable

No action
Continue monitoring

Fix available

Apply

Apply and fix the CVE

Fix exists in another version

Port and apply

Port the patch
Apply and fix the CVE

No fix

Understand the risk

Communicate the risk
Suggest mitigation plan
Monitoring fix availability

Dedicated Engineering Team

EBV Elektronik
An Avnet Company

Technology. Passion. EBV.

Guidance to Customer

BSI TR-03183 Cyber Resilience Requirements

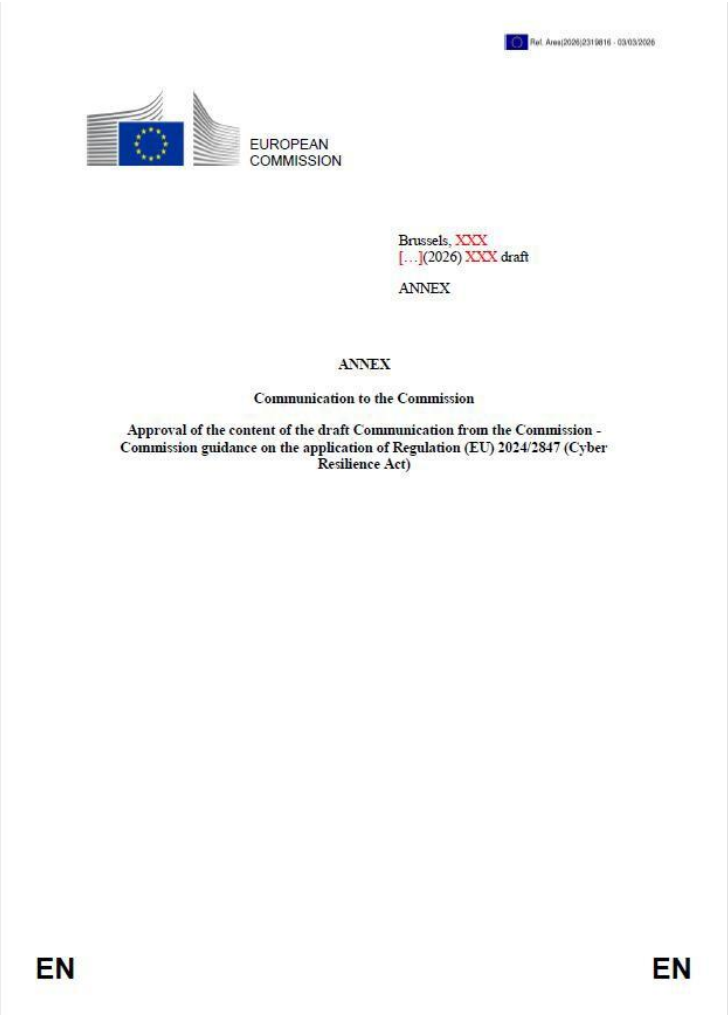
To prepare manufacturers for the CRA introduction, the German IT security agency BSI developed technical guidelines to achieve CRA compliance.

- Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 1: General requirements Version 0.10.0
- Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.1.0
- Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 3: Vulnerability Reports and Notifications Version 1.0.0

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/dok/TR-03183

Draft Commission guidance on the Cyber Resilience Act



EUROPEAN COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEX

ANNEX

Communication to the Commission

Approval of the content of the draft Communication from the Commission - Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act)

EN EN

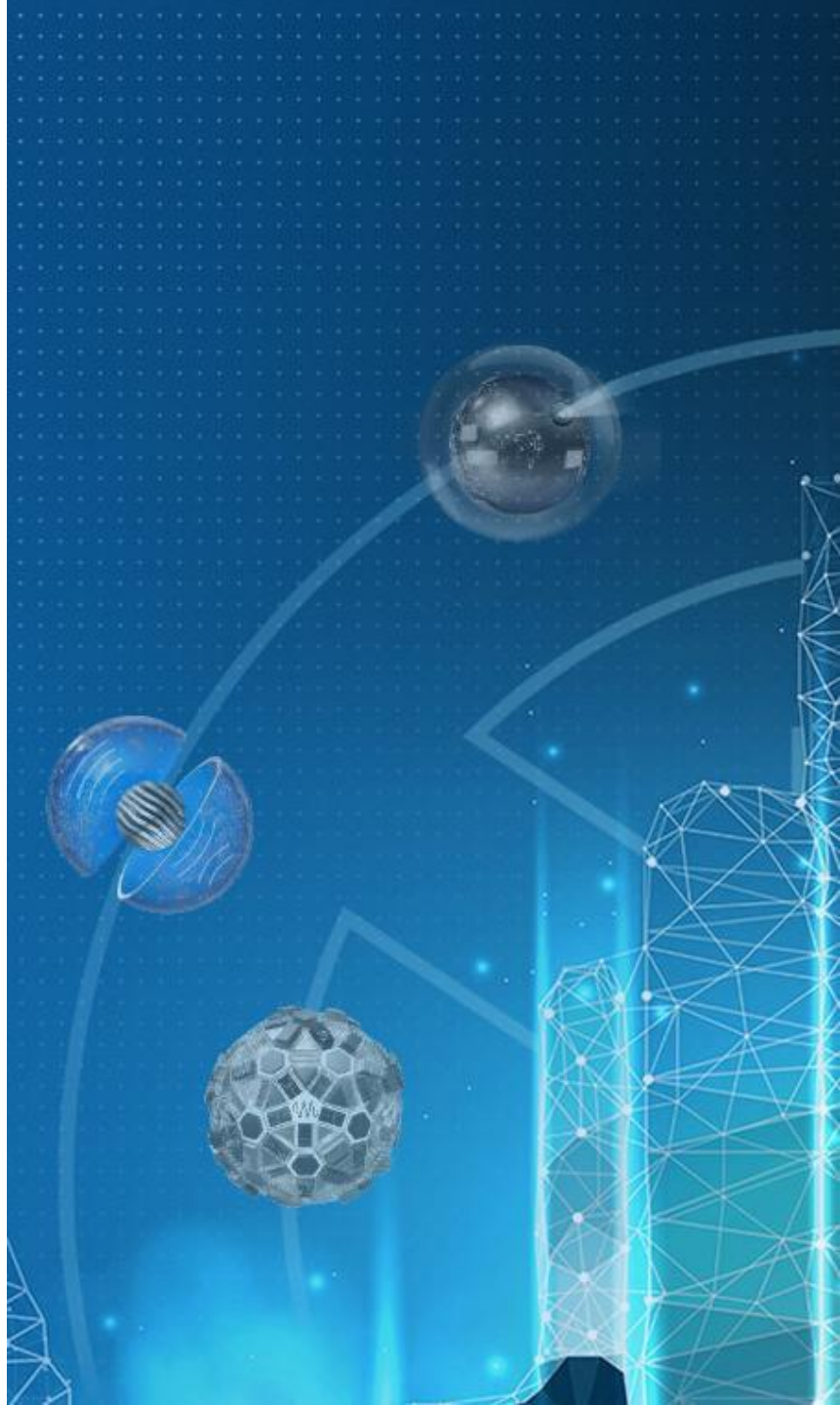
The European Commission is preparing a Communication that will provide guidance on how to apply the Cyber Resilience Act (CRA) in practice. The guidance will help manufacturers, developers, and other stakeholders understand their obligations under the Regulation and ensure a consistent approach across the EU. It will clarify how key provisions of the CRA should be interpreted and implemented.

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en

EBV Elektronik
An Avnet Company

Conclusion

- Conduct cybersecurity risk assessments
- Ensure products meet essential cybersecurity requirements
- Implement vulnerability handling processes
- Draw up technical documentation
- Generate a Software Bill of Materials (SBOM)



TECHNOLOGY.

PASSION.

EBV.

Hitex offerings …

Ask alexander.hess@hitex.de – he looks forward to receiving your inquiries regarding Hitex offerings, including:

- Arm encryption libraries
- Security stack for Hardware Security Modules
- Support for your ISO 21434 Threat Analysis and Risk Assessment (TARA)
- Training courses for embedded systems with Arm
- SO-DIMM compute modules for PSOC™, TRAVEO™ and more for an easy entry into the Infineon MCs.

Stay informed: webinars, training sessions, knowledge labs
Find all the information at www.hitex.de