



Cyber Resilience Act

From Regulation to Real Systems



Julien Vermillard – julien@clunkymachines.com



Julien – Independent IoT Architect & Developer

IoT platform design & development:

- Device-to-cloud architectures emphasizing wireless and open-source
- CRA, Secure boot and end-to-end key management and OTA pipelines
- Embedded and Cloud software development (Java/Kotlin, Go, C, Rust, AWS,..)

<https://www.clunkymachines.com>

<https://www.linkedin.com/in/jvermillard/>



Agenda

What is the Cyber Resilience Act

- Product Classification
- Cyber Security Requirements

Interpreting and Implementing CRA

- IoT use case
- Security architecture
- Demo

Thanks: Joe Lomako | TÜV SÜD!



From Regulation to Requirements: Making Sense of CRA





Opening: why CRA exists?

Recitals set the scene:

- Risks to society and economy
- Potential impact on critical services
- And indirectly, risks to democratic processes

Regulatory response:

- Shift responsibility to manufacturers
- Make cybersecurity a legal requirement
- Harmonize rules across the EU market



What CRA actually is: product regulation



A lifecycle cybersecurity law

- Design → development → post-market
- Updates and vulnerability handling



A CE-marking framework

- Cybersecurity part of product compliance
- Conformity assessment and documentation



A manufacturer responsibility model

- Obligations remain throughout the product lifecycle
- Not transferable to the user



What CRA is not!



Not a best-practice framework: Compliance is mandatory



Not limited to cloud or IT systems:

Applies to the product itself (device + embedded software)



Not a one-time certification:

Obligations continue after the product is shipped



Not only about data protection:

Focus on security of the product, not just personal data



Not replacing existing regulations: Complements RED, GDPR, NIS2, etc.



Device Manufacturer: Before / After





ATTENTION

**Cette réglementation
n'a pas de cerveau,
utilisez le vôtre !**





Scope & Applicability

- **“Products with Digital Elements”**: product with software and data connectivity
- Direct or indirect **connection** (e.g. via smartphone or gateway)
- Standalone **software** (if placed on the EU market)
- **Hardware** products (devices, embedded systems)
- Including their **remote data processing** solutions!



Quizz: CRA or not CRA?

- **Army tank ?**
- **Civil plane ?**
- **Motor vehicle ?**
- **Connected medical device ?**
- **Marine equipment ?**
- **SaaS ?**
- **Smartphone app ?**
- **Digital weight scale ?**
- **Washing machine with a microcontroller ?**
- **An infrared TV remote ?**
- **Wireless charging device ?**
- **FPGA IP blocks (e.g. Digital Signal Processing) ?**



Quizz: CRA or not CRA?

- **Army tank** ? → No (exclusive defence product are excluded)
- **Civil plane** ? → No (industry specific regulation)
- **Motor vehicle** ? → No (industry specific regulation)
- **Connected medical device** ? → No (industry specific regulation)
- **Marine equipment** ? → No (industry specific regulation)
- **SaaS** ? → No (NIS2 only if no connected devices)
- **Smartphone app** ? → Yes (Connected device + Cloud)
- **Digital weight scale** ? → No
- **Washing machine with a microcontroller** ? → No
- **An infrared TV remote** ? → Yes (connection and data exchange)
- **Wireless charging device** ? → No (no data exchange)
- **FPGA IP blocks** (e.g. Digital Signal Processing) ? → Yes



Classification: Default vs Important (I/II) vs Critical

Default products

- All products not classified as “important” or “critical”
- Example: most consumer connected products

→ Self-assessments (CE Marking)

Important products I

- Security related software or components
- Example: password manager, VPN, Identity manager, MCU with security elements, wearable with health feature or for children, smart locks

→ Self-assessment if applied recognized standards (e.g. ETSI baseline) or notified body



Classification: Default vs Important (I/II) vs Critical

Important products II

- Higher impact on systems and infrastructure
- Example: Hypervisors, Firewalls, IDS, tamper resistant MCU

→ Mandatory third party involvement (notified lab)

Critical

- High systemic impact is compromised
- Example: Smartcard, Secure Elements, HSM

→ Accredited labs + National Cybersecurity Certification Authorities; eg: ANSSI, BSI



Product cybersecurity requirements

- Secure design & development
- No known exploitable vulnerabilities
- Secure by default configuration
- Reduce attack surface
- Protection against unauthorized access
- Data Protection
- Secure communication
- Resilience and availability
- Monitoring & logging



Vulnerability handling requirements

- Identify and document components
- Vulnerability process management
- Timely remediation
- Coordinated vulnerability disclosure
- Security updates
- Transparency to the users
- Reporting obligations (ENISA)
- Regular security testing



Conformity & CE marking

Cybersecurity is part of the CE marking

- CRA integrate into CE compliance framework
- Same as safety, EMC, radio compliance

Manufacturer responsibilities

- Perform a conformity assessment
- Ensure compliance with Annex I requirements
- Produce technical documentation
- Issue an EU Declaration of Conformity (DoC)

“No CE marking → no legal access to the EU market.”



Technical documentation must include

- Risk assessment
- Security design and architecture
- Vulnerability handling process
- Update policy



Post-market obligations

Security is a lifecycle responsibility

- Obligations continue after the product is placed on the market
- Manufacturer remains responsible during the support period

Vulnerability management

- Monitor and identify vulnerabilities
- Fix without undue delay
- Maintain a coordinated disclosure process

Security updates

- Provide free of charge updates for the defined support period
- Ensure updates are: secure & reliable



Support period ?

Manufacturers must define a support period

- Security updates must be provided for a defined period
- Period must be communicated to users

Not explicitly defined but

- Regulation in place (e.g. spare part for appliance)
- Become a marketing argument and communicated upfront



Economic operators responsibilities

Importer

- Verify product has: CE marking, Declaration of Conformity, Required documentation
- Ensure manufacturer is compliant before placing on EU market

Distributor

- Act with due care
- Verify CE marking and documentation presence
- Do not sell products they know are non-compliant



Penalties & enforcement

Authorities (ANSSI, ENISA, market surveillance authorities)

- request technical documentation
- perform inspections and testing
- investigate vulnerabilities and incidents
- Require manufacturers to:
 - Fix non-compliance
 - update products
 - inform users
- Can impose:
 - Sales restrictions or bans
 - product recalls or withdrawals

Up to €15 million or 2.5% of global annual turnover



Practical implications

Security becomes a design constraint

- Must be considered from day one
- Impacts architecture, not just implementation
- Documentation is a delivery

You must support your product over time

- Define a support period
- Provide updates and fixes
- Plan long-term maintenance

Vulnerability management and Update capability is mandatory!



Timeline

- **October 2024** → CRA published
- **December 2024** → Entry into force
- **September 2026** → Vulnerability reporting obligations apply
- **December 2027** → Full compliance required



Timeline 🤪

Harmonized standards (HEN)

- Not fully published yet
- No definitive “presumption of conformity” baseline
- ETSI work still ongoing

Vulnerability reporting infrastructure

- Reporting to ENISA required (from Sep. 2026)
- Practical platform / processes still TBD



Interpreting and implementing CRA





From legal text to reality

CRA defines **outcomes**, not implementations (caveat: for default class)

Product team must translate:

- “secure by design” → architecture decisions
- “handle vulnerabilities” → processes

You need to decide *how*.



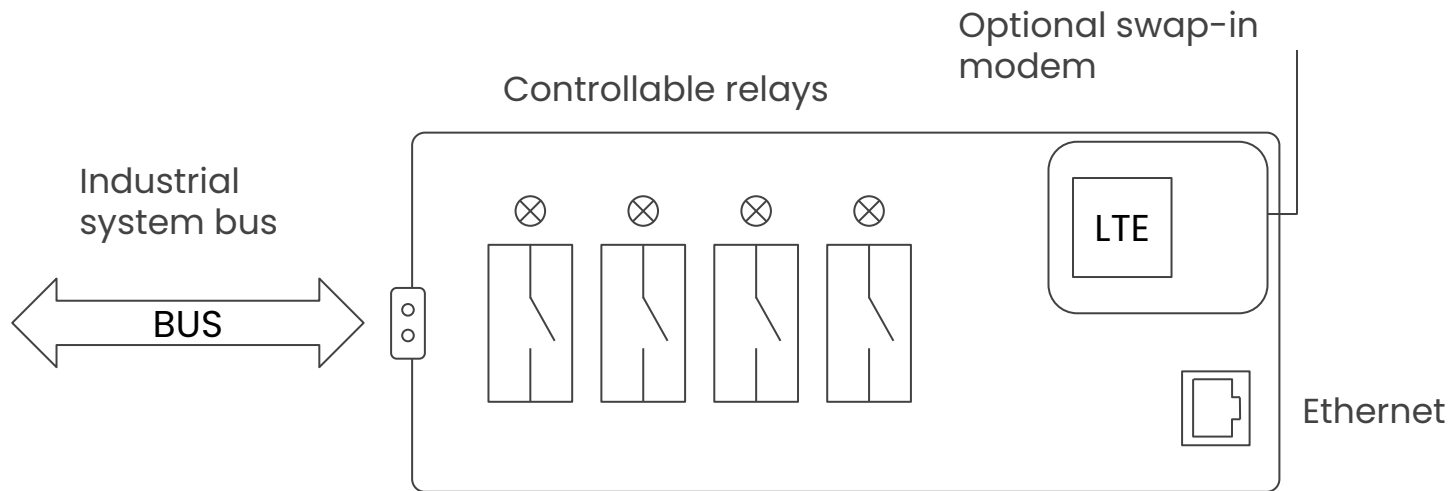
What CRA Actually Forces You to Do

Think in terms of:

- System boundaries
- Risk
- Product support lifecycle

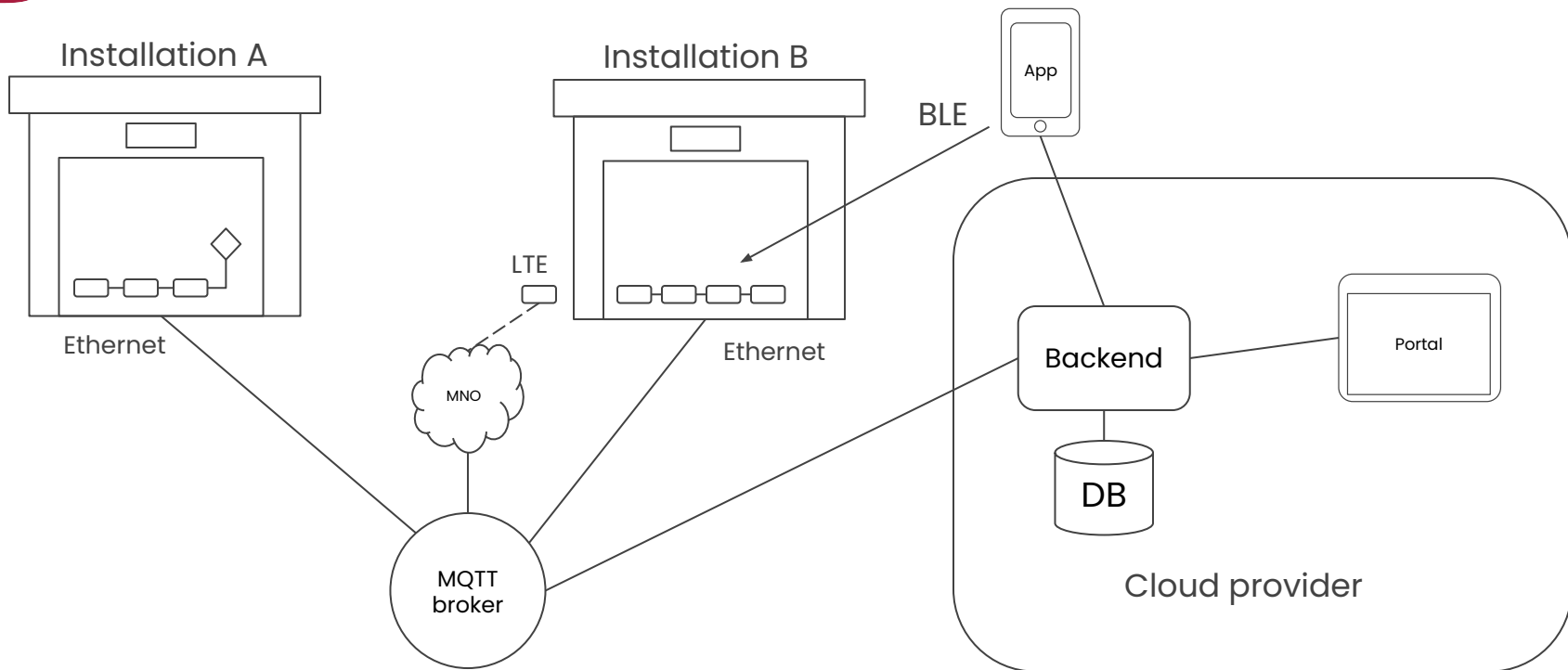


Example: Industrial Control Nodes



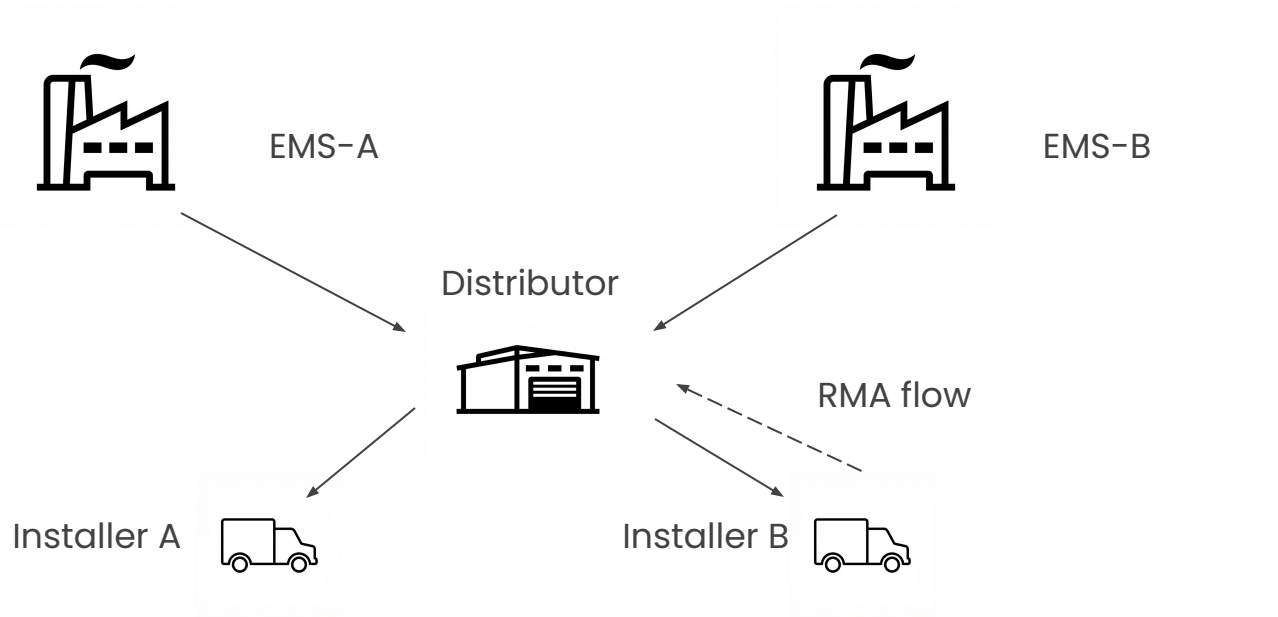


First: Boundaries?





Find all the boundaries!





What are we protecting?

Define the Identified assets to protect, by priority order:

- Physicals Systems (Relays and the physical assets)
- Command & Control (Remote relay trigger)
- Device integrity (Firmware, Configuration, Device Identity & Credentials)
- Operational data (Status, Log, Configuration Data)
- Connectivity (Ethernet interface, LTE, bus)



STRIDE model = 6 types of threats

STRIDE is a checklist to make sure we don't forget an entire class of attacks

- **Spoofing** → pretending to be something else
 - Unauthorized command send, fake backend/device
- **Tampering** → modifying data or commands
 - Modifying command in transit, open another relay
- **Repudiation** → denying actions
 - No trace of who sent the "open" command
- **Information disclosure** → leaking data
 - Leak other customer during RMA
- **Denial of service** → blocking the system
 - Flood server, block device communication
- **Elevation of privilege** → gaining more access
 - Inject malware firmware in the device



Attack trees: how to break things

Goal: Trigger relay without authorization

- Attack device $\leftrightarrow$ server network/communication
 - Spoof backend
 - Weak or no authentication
 - Tamper traffic
 - Weak or no encryption/integrity
- Compromise the device
 - Exploit vulnerability
 - Debug interface exposed, inject malware
- Physical access
 - Inject the command in the control bus
 - Short the relay
- Attack backend

etc..



From Thread Analysis to CRA Documentation

Threat analysis

- STRIDE → coverage of threat categories
- Attack trees → realistic attack paths
- Evaluate likelihood and impact

Select Security measures

Risks → Mitigations

Documentation 🎉

System → Assets → Threats → Risks → Mitigations



Security Solution: Secure communication

Authentication & Integrity

- mTLS MQTT device $\Leftrightarrow$ broker connections
- Device/Topic permission for strict device isolation
- PKI with offline Root CA for X509 certificate
- Secure factory PC with attached HSM loaded with intermediate CA
- Certificate Signature log from the factory PC
- Device private key generated in MCU secure key storage
- Telemetry flow with dashboard and monitoring for device activities



Secure communication continued

DoS protection

- Store & forward for device logs & telemetry in case of network disruption
- Configurable firewall and load-balancer

Secure Update

- MCUboot to verify images ECDSA signature (over MQTT and BLE)
- No secure boot but physical access to the device is secured
- RMA process to re-provision already used devices



Security Solution: Data Integrity

IT/Cloud Security

- OAuth2 provider for Phone/Web authentication with RBAC
- Secure cloud infrastructure (SOC2) with infrastructure segregation
- Database encrypted at rest

Vulnerability scan & management

- SBOM Software Bill of Material generation for Zephyr (west spdx)
- cve-bin-tool to scan for firmware vulnerabilities
- Trivy for cloud software CVE scanning
- Secure updates, customer communication process & deployment

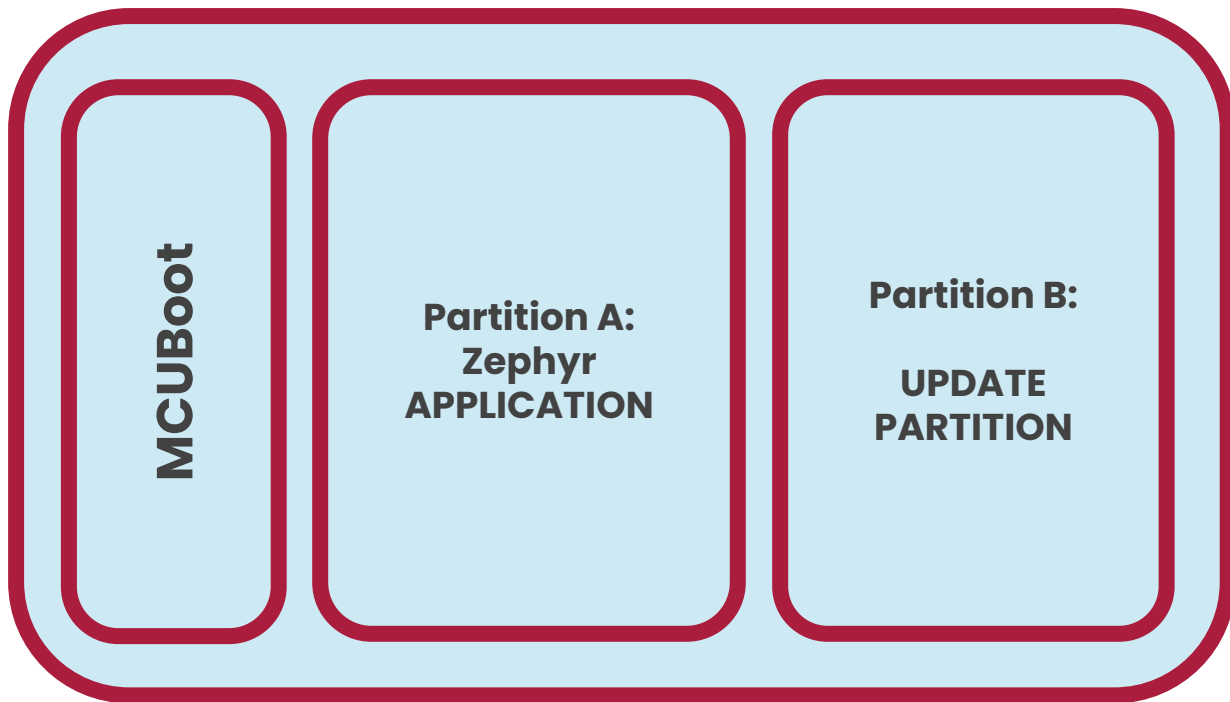


Demo: Zephyr+MCUboot SPDX+cve-bin-tool/grype





MCUboot: secure update made easy





MCUboot: Reliable Firmware Updates

- Cryptographic image validation (ECDSA / RSA signatures)
- Supports A/B (dual-slot) update strategy (XIP and overwrite)
- Integrates natively with Zephyr and sysbuild
- Test → Confirm → Revert, because you can't test every real world configuration



SBOM made easy: Zephyr SPDX

Snapshot and analysis of your application dependencies:

```
west spdx -d build/zephyr-fota-demo
```

```
grype sbom:./modules-deps.spdx
```

```
✓ Scanned for vulnerabilities [12 vulnerability matches]
└─ by severity: 4 critical, 4 high, 3 medium, 1 low, 0 negligible
   by status: 10 fixed, 2 not-fixed, 0 ignored
```

NAME	INSTALLED	FIXED IN	TYPE	VULNERABILITY	SEVERITY	EPSS	RISK
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34877	Critical	0.1% (35th)	0.1
hostapd	2.11		UnknownPackage	CVE-2025-24912	Low	0.2% (42nd)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34874	High	< 0.1% (22nd)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34875	Critical	< 0.1% (16th)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-25833	High	< 0.1% (15th)	< 0.1
mbed_tls	3.6.5	3.6.6, 4.1.0	UnknownPackage	CVE-2026-34873	Critical	< 0.1% (10th)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34872	Critical	< 0.1% (3rd)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34876	High	< 0.1% (4th)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-25834	Medium	< 0.1% (5th)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-25835	High	< 0.1% (2nd)	< 0.1
mbed_tls	3.6.5		UnknownPackage	CVE-2025-66442	Medium	< 0.1% (5th)	< 0.1
mbed_tls	3.6.5	3.6.6	UnknownPackage	CVE-2026-34871	Medium	< 0.1% (2nd)	< 0.1



CRA: What now?

2027 is fixed, architecture decision are now!

Design for updates

- Updates, monitoring, vulnerability handling
- Not optional anymore

Make it defensible

- Risks → mitigations → documentation
- If you can't justify it, it won't pass

Need help making your system CRA-ready? julien@clunkymachines.com

Thanks!



Let's tame the CRA!



<https://linkedin.com/in/jvermillard>

<https://clunkymachines.com>

Julien Vermillard – julien@clunkymachines.com