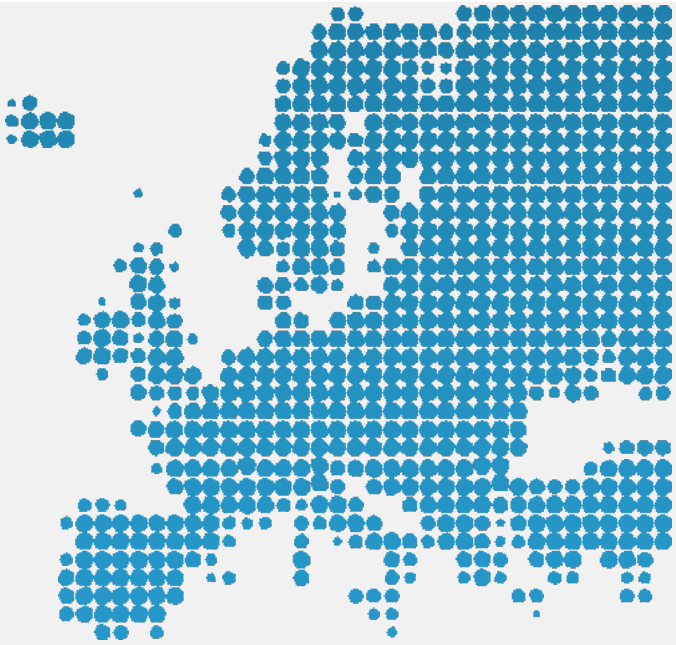
CRA and AIA – What to do?

Status: July 2026

CRA and AIA are IT topics? No!



Contents

CRA and AIA are IT topics?

No!

Cybersecurity, AI, software, data, etc. are no longer pure IT topics, but are "product features", with market access, liability and CE marking issues.

These new topics are addressed to all manufacturers of (e.g.):

- Automatic doors and industrial doors
- Fire and safety doors
- Access control systems
- Smart Locks

with applications and/or connectivity of (e.g.)

- gate controls
- building-integrated systems with Ethernet, WLAN, Bluetooth, GSM/LTE
- Cloud or app-connected products

Perhaps one could describe the current situation as a phase in which mechanics and software are merging. Or have we already got past this stage?

1. What can door manufacturers expect?

The EU regulator is pursuing a clear goal: In the future, cybersecurity will be treated in a similar way to machine safety or product safety.

If a door can hurt people, it must be designed safely.
If a door can be hacked, the same will apply in the future.

The three major drivers

1. Cyber Resilience Act (CRA)

The CRA applies to products with digital elements and data connections. These include many modern door and gate systems. In the future, manufacturers will have to demonstrably integrate cybersecurity into development, operation and maintenance.

Affected are, among others:

- Gate control with network connection
- Smart Lock
- Access control system
- Door controller
- Cloud Portal
- Service app
- Remote maintenance access
- Gateway for building automation

2. NIS2 effect

Even if the manufacturer itself does not fall directly under NIS2, the following are:

- Airports
- Energy suppliers
- Data Centres
- Hospitals
- Logistics centres
- Critical infrastructure

increasingly audit their suppliers.

The question then is: "How do you ensure the cybersecurity of your door controls?" If you don't have an answer, you lose tenders.

3. Product liability

A future claim could look like this:

- Attacker compromises remote maintenance access
- Industrial door opens uncontrolled
- Loss of production
- Property damage
- Personal injury

Then the question is asked:

- Was there cyber risk management?
- Was there security-by-design?
- Have known vulnerabilities been fixed?
- Were there any update processes?

If there are no reliable answers here, the liability risk increases considerably.

4. Misconception 1

Door manufacturers are not a software company.

Door manufacturers are not an IT company in the classic sense, but as soon as a product:

- includes firmware
- exchanges data
- updates
- is maintained remotely

software becomes part of the product.

5. Misconception 2

The door manufacturer buys in the control system, so IT issues are not an issue.
No, the door manufacturer remains responsible! The responsibility cannot simply be shifted to the electronics supplier.

In particular:

- Embedded Software
- Open Source Components
- Communication modules
- Cloud Services

must be controlled.

6. Misconception 3

There has never been a cyberattack.
But who would even notice?

Many manufacturers today do not have:

- Vulnerability Management
- Security Monitoring
- SBOM (Software Bill of Materials)
- Vulnerability Processes

and therefore, often cannot detect attacks or vulnerabilities at all.

2. What should be done right now

Priority 1: Classify product portfolio

Create a list:

- Which products contain software?
- Which ones have a network connection?
- Which ones have remote maintenance?
- Which ones use cloud services?
- Which apps use?

For many companies, it turns out that not 10%, but 60 - 80% of the portfolio is affected.

Priority 2: Security Gap Assessment

Questions:

- Are there any security requirements?
- Is there such a thing as threat modelling?
- Is there Secure Development?
- Are there penetration tests?
- Are there patch processes?
- Is there security documentation?

Priority 3: Software Bill of Materials (SBOM)

- Which libraries are installed?
- Which open-source components are used?
- Which CVEs (unique identifier of a vulnerability) are affected?

Priority 4: Establish vulnerability management

Vulnerabilities must not be discovered by chance; processes are needed for:

- Detection
- Rating
- Remediation
- Communication

The CRA also introduces reporting obligations for actively exploited vulnerabilities and serious security incidents. The first reporting obligations will take effect as early as September 2026.

Priority 5: Security governance at the management level

Cybersecurity must no longer be limited to:

- IT
- Development

- external service provider

Responsibility is increasingly shifting to management and product manufacturer level.

3. What happens if you do nothing?

Short-term (1 - 2 years)

- Loss of tenders
- Customer audits failed
- Demand from large integrators
- Increasing insurance requirements

Medium-term (2 - 4 years)

- Considerable retrofitting effort
- Development projects delayed
- Products must be re-documented
- High external consulting costs

Long-term

Once the CRA is fully applicable, affected products must meet the cybersecurity requirements and demonstrate the corresponding compliance requirements.
Cybersecurity thus becomes a de facto part of the CE/market access system.
Products without sufficient evidence can have significant marketing problems in the EU.

Text / Editorial team:

Status: July 2026

E.D.S.F.
European Door and Shutter Federation e.V.
Neumarktstr. 2 b
58095 Hagen · Deutschland

Fon +49 2331 2008-0
Fax +49 2331 2008-40
info@edsf.com
www.edsf.com