Embedded Systems Cybersecurity Trends & Implementation

L'Association des représentants Français des logiciels et des systèmes Embarqués

Working Group:
Embedded Cybersecurity

Paris, le 09 Décembre 2025

Embedded France
L'EMBARQUÉ MADE IN FRANCE

Working Groups

Embedded France
L'EMBARQUÉ MADE IN FRANCE

L'Association des représentants Français des logiciels et des systèmes Embarqués

Les groupes de travail actifs

Cybersécurité embarquée

Ecoconception

Edge computing

NSL Normes pour la Sûreté de fonctionnement Logiciel et système

IA embarquée

ISEC. Ingénierie des systèmes embarqués critiques sûrs

Embedded France
L'EMBARQUÉ MADE IN FRANCE

COMPANIES	NAMES
Ampere	Pierpaolo Cincilla
ANSSI	Salio Bâ
Asterios Technologies / Safran SED	Damien Chabrol
Cap'Tronic	Jean-Christophe Marpeau
Cetrac	Gerulf Kinkelin
Cryptonext Security	René Martin
ELISA-Aérospace	Jean François CARPENTIER
ESIEE	Abir Rezgui
INP ESISAR	Charles Reboul
Mathworks	Alexandre Langenieux
MOABI	Jean-Michel Brossard Nicolas Gaume
ProvenRun	Dominique Bolignano
Sciensys	Olivier Maumus
Secure-IC	Sylvain Guilley
Sysgo	José Almeida Bruno Coppens
Thales	Antoine Leroy
Trust-in-Soft	Rolland Dudemaine
Viveris	Romain Guilloteau
We-are-cyber	Guillaume Fenez Maximin Coste-Leenhardt

Embedded Systems Cybersecurity - Trends & Implementation

Embedded France
L'EMBARQUÉ MADE IN FRANCE

Agenda 1/2

- **Embedded France Overview**
- **Executive Summary**
- **Regulation as a driver for cybersecurity**
  - State of the Union
  - Methodology overview
  - Debunking Horizontal Regulations
    - EU CRA (Cyber Resilience Act)
    - AI Act
  - Debunking Vertical Regulations
    - RED (Radio Equipment Directive)
    - NIS2 (Network and Information Security Directive)
    - "Machines" Directive
    - UN Regulation No. 155 (UN R155) – Cybersecurity Management System (CSMS)
    - UN Regulation No. 156 (UN R156) – Software Update Management System (SUMS)
    - ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering
    - DORA (Digital Operational Resilience Act)

Embedded France
L'EMBARQUÉ MADE IN FRANCE

Embedded Systems Cybersecurity - Trends & Implementation

Agenda 2/2

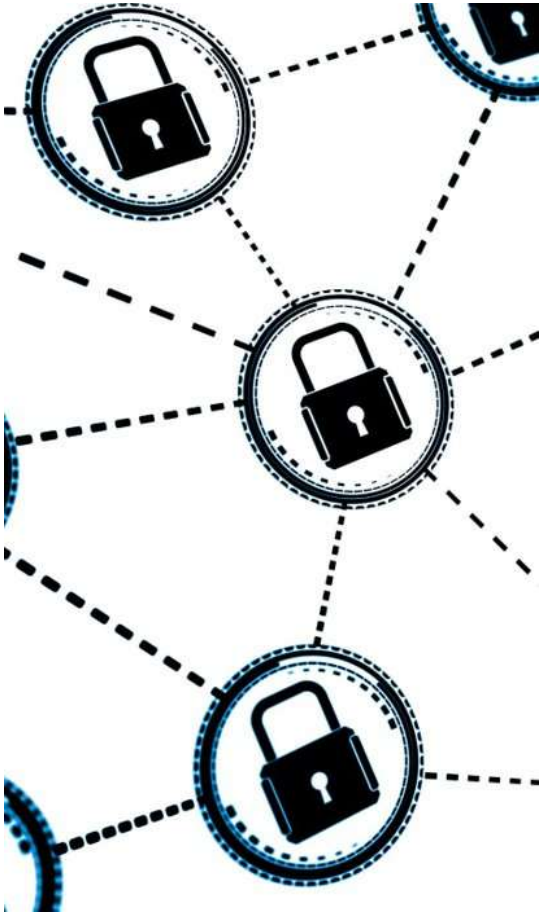
- **How to ensure compliance**
  - Your Compliance, Through Cybersecurity Journey
  - Certification is One Stream
  - Technology is Another
- **Call for Action**
- **Q&A**

Embedded France
L'EMBARQUÉ MADE IN FRANCE

Embedded Systems Cybersecurity - Trends & Implementation

Executive summary

- Cybersecurity is now driven by mandatory regulations, especially in the EU.
- The EU is leading a regulatory mega-trend, enforcing cybersecurity across all digital products.
- All connected products (directly or indirectly) must undergo conformance procedures and issue a declaration of conformity.
- Non-compliance = sanctions. Compliance processes are still evolving, but deadlines are approaching (full enforcement by 2027).
- This white paper provides a clear synthesis:
  - What needs to be done?
  - Who is impacted?

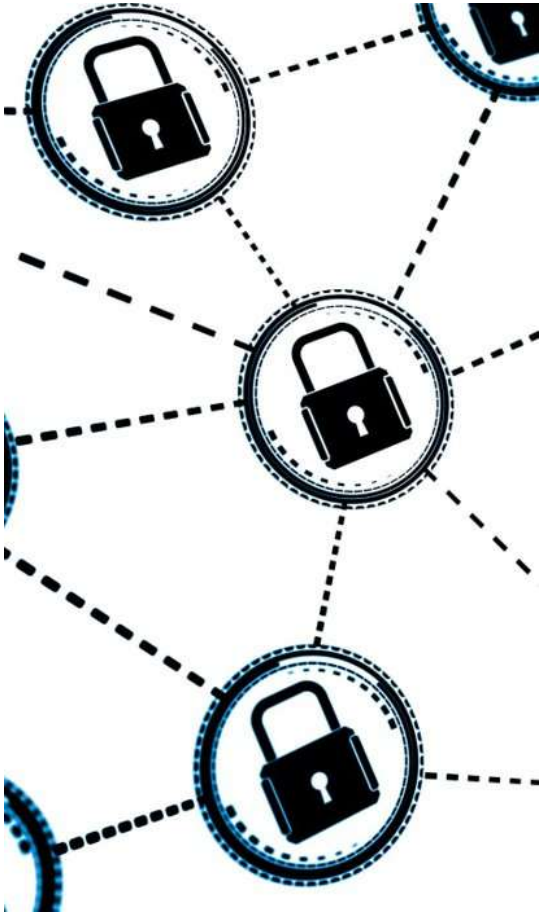


Embedded France
L'EMBARQUÉ MADE IN FRANCE

Embedded Systems Cybersecurity - Trends & Implementation

Executive summary

- Target audience:
  - Corporate cybersecurity governance
  - Developers seeking practical compliance guidance
- The document is a vade mecum to understand the operational impact of EU regulations on:
  - Processes
  - Products
  - Market access (even outside the EU)
- Includes:
  - Mandatory actions



Embedded Systems Cybersecurity - Trends & Implementation

Regulation as a driver for cybersecurity : State of the Union.

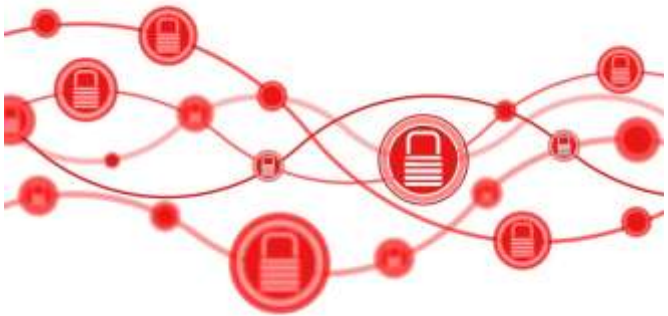
Navigating Embedded-Oriented Mega-Trends & Regulatory Complexity

- The embedded systems ecosystem is facing **urgent regulatory challenges**, as highlighted at Embedded World 2025.
- The **EU Cyber Resilience Act (CRA)** is just one of **many overlapping regulations**.
- Think tanks (e.g., Renaissance Numérique, The Digital New Deal) warn of a **legislative puzzle**.
- While **compliance is complex**, most regulations are **aligned** — but must be addressed **proactively**, not retroactively.
- Our **white paper** and **step-by-step methodology** provide guidance to navigate this landscape.
- Without clarity, regulatory complexity risks **hindering cybersecurity progress**.

Embedded Systems Cybersecurity - Trends & Implementation

Methodology Overview

Three Layers of Cybersecurity for Embedded Systems



Organizations must address cybersecurity at **three distinct but interdependent levels** :

- **Organizational Level** : Secure IT & OT infrastructures (e.g., internal networks, customer interfaces, supplier portals).
- **Supply Chain Level** : Ensure traceability and protection from design to delivery (e.g., software components, key distribution, updates).
- **Product Level** : Embed cybersecurity into the product itself, ensuring resilience once in the hands of the customer.

Embedded Systems Cybersecurity - Trends & Implementation

Methodology Overview

Illustrative Example : Automotive Industry

- Organizational : Protect connected infrastructures (manufacturing, dealerships, suppliers).
- Supply Chain Level : Secure every ECU (up to 100 per car), manage software & encryption keys, ensure secure updates.
- Product Level : Design secure electronic architectures to withstand real-world threats.

🔍 Though the automotive sector is outside EU CRA scope, it illustrates the complexity and necessity of a structured, multi-layered approach.

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

European Union

What is the EU Cyber Resilience Act (CRA)?

- Objective : Enhance cybersecurity of *Products with Digital Elements* (hardware & software) across their entire lifecycle.
- Key Requirements for Manufacturers:
  - Integrate cybersecurity by design
  - Conduct cyber risk assessments
  - Implement vulnerability management
  - Indicate end-of-support date
  - Report vulnerabilities within 72 hours
- Scope:

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

Who is Concerned & When?

- Stakeholders:
  - Manufacturers
  - Importers
  - Distributors
- Exemptions:
  - Medical devices
  - Automotive (covered by UN ECE R.155)
  - Aerospace
  - Defense (non-EU competence)

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

Key Takeaways & Risks

✅ Positive Aspects:

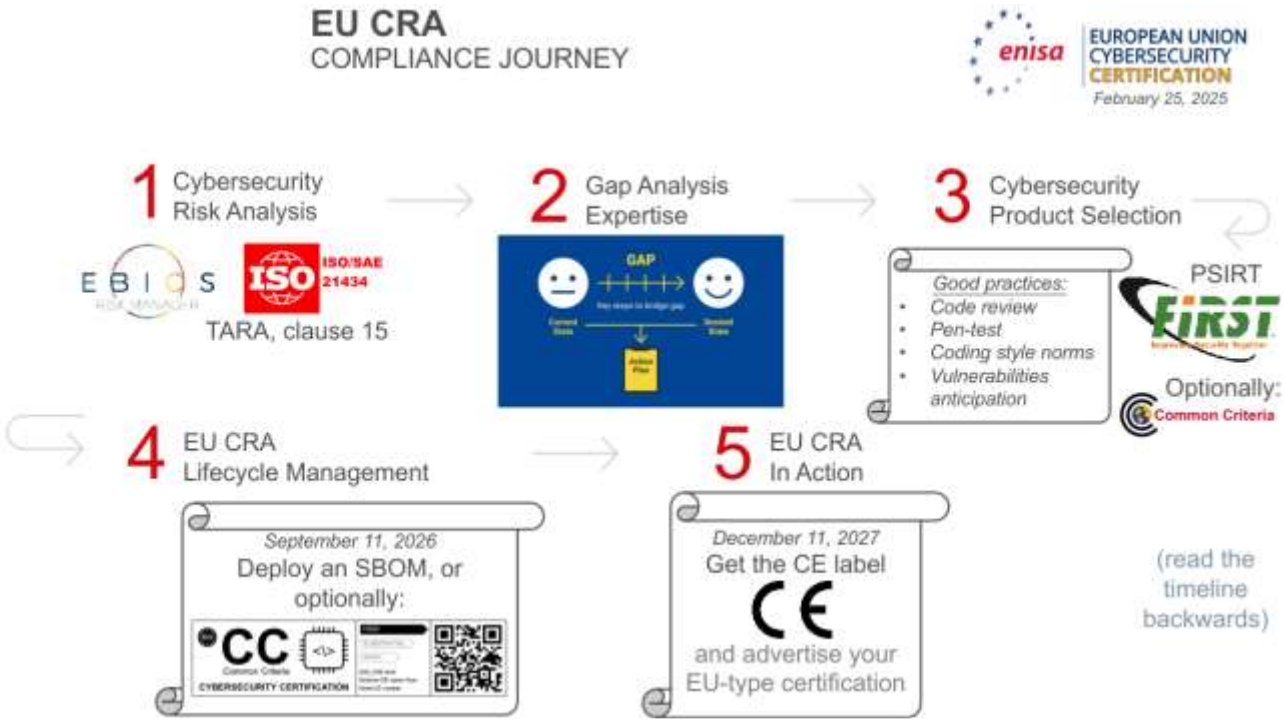
- Harmonized cybersecurity standards across the EU
- Encourages proactive security integration
- Supports product lifecycle security

⚠️ Risks of Non-Compliance:

- No CE marking
- Fines
- Product withdrawal from the market

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)



Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

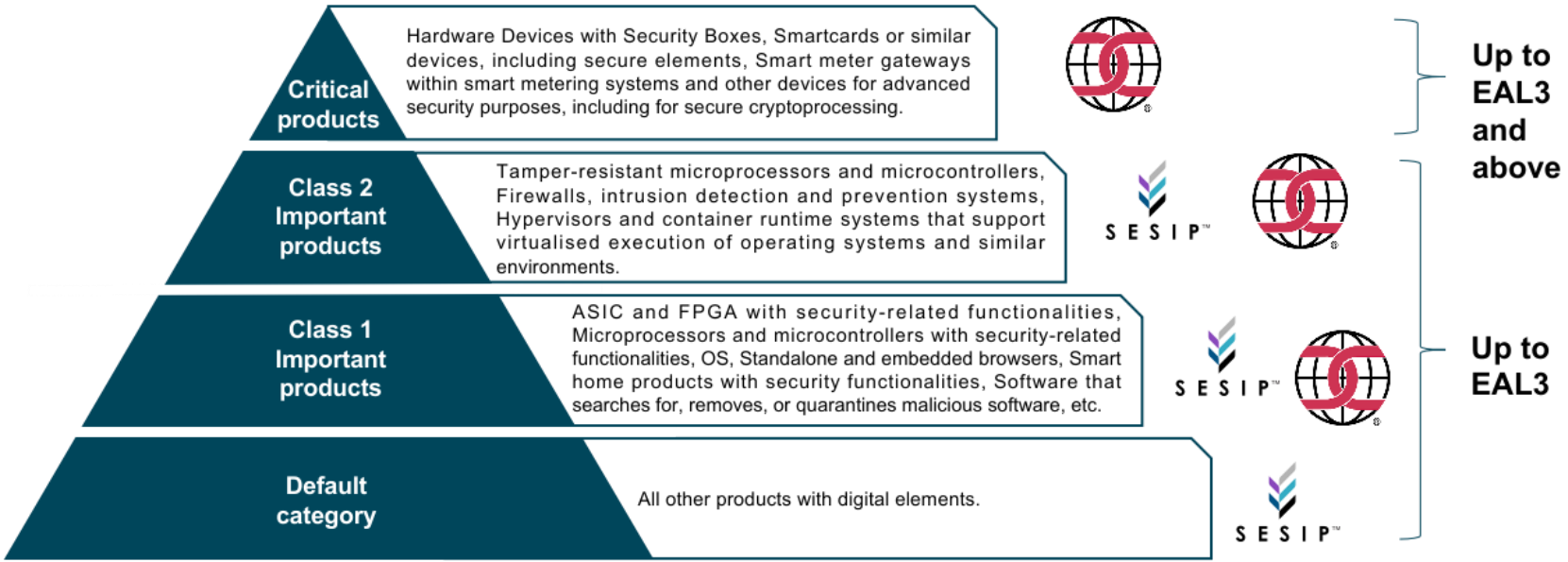
EU CRA Compliance – 3 Possible Paths

1. Non-regulated Applications
   - ✅ Follow existing domain-specific standards
   - ✔ Mandatory and already in use within the industry.
2. European Cybersecurity Certification (EUCC Scheme)
   - ✅ Apply ISO/IEC 15408 via EUCC
   - ✔ Well-established framework
   - ✔ Similar to traditional CC, with differences in lab organization and pricing
   - ✔ EU CRA requirements can be mapped to EUCC compliance
3. Full Certification Required
   - ✅ When no applicable standard or CC certification exists
   - ✔ Full process must be followed

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

Classes can be mapped with standards and Evaluation Assurance Levels (EALs)



CEN EN 17927:2023 : Security Evaluation Standard for IoT Platforms (**SESIP**).
An effective methodology for applying cybersecurity assessment and re-use for connected products.

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

EU CRA Compliance – Recommended Steps

1. Cybersecurity Risk Assessment
   - Partner with experts for initial assessment (consulting service)
2. Gap Analysis
   - Use EBIOS workshops to identify gaps in risk management
3. Action Plan
   - Adopt good practices:
     - Vulnerability anticipation
     - Code review
     - Pen testing
     - Secure coding & verification

Embedded Systems Cybersecurity - Trends & Implementation

EU CRA (Cyber Resilience Act)

Technical Measures for Compliance

4. Software Bill of Materials (SBOM)
   - Define granularity
   - Choose tools & automation

5. Vulnerability Management System
   - Set up PSIRT
   - Align with:
   - ISO/IEC 29147:2018 (disclosure)
   - ISO/IEC 30111:2019 (handling)

6. Supply Chain Mapping
   - Link technologies to risks across the supply chain

Embedded Systems Cybersecurity - Trends & Implementation

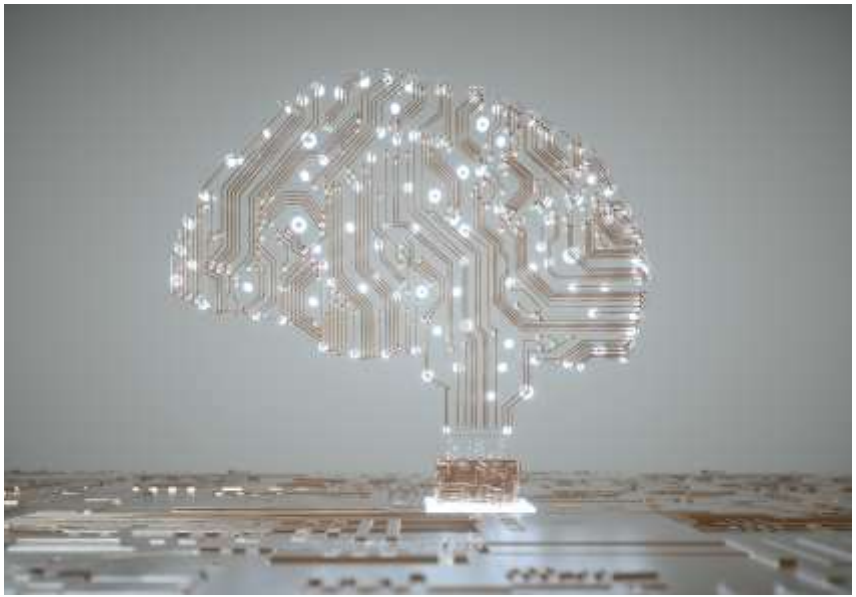
EU CRA (Cyber Resilience Act)

Compliance Outcomes & Legal Framework

- Benefits of Compliance
  - ✅ Product quality & added value
  - ✅ Alignment with 41 recommended standards (e.g., IEC 62443, EN 18031:2024, IEC 63452)
- Penalties for Non-Compliance
  - ⚠️ Up to €15 million or 2.5% of global turnover
- Final Checklist
  - ✔ Risk assessment
  - ✔ Secure-by-design & default
  - ✔ Regular updates & patches
  - ✔ Documentation & audit readiness
  - ✔ Staff training on cybersecurity

IA Act

What, Who, When ?



What?

Regulates AI systems based on risk levels:

- Unacceptable risk: banned (e.g., social scoring)
- High risk: strict obligations (e.g., hiring, healthcare)
- Limited risk : transparency required
- Minimal risk: voluntary codes

Who?

AI developers, users, and service providers

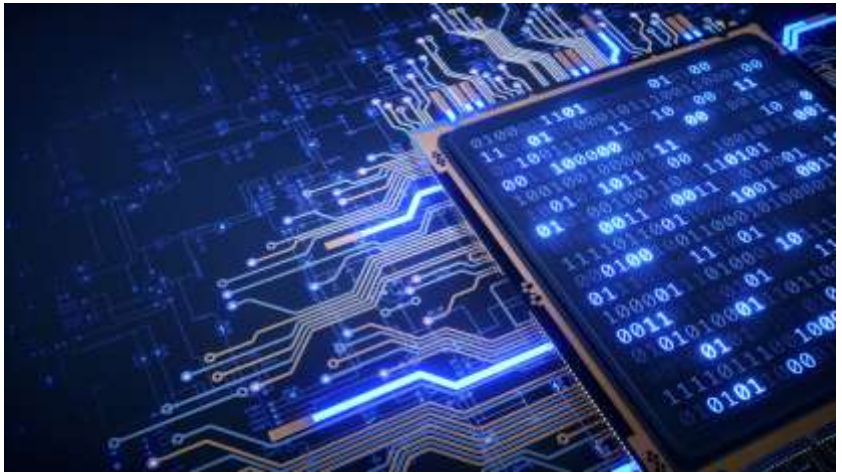
When?

- Feb 2025: Initial rules in force

Embedded Systems Cybersecurity - Trends & Implementation

IA Act

Compliance & Penalties



- Steps to Ensure Compliance
  - ✓ Classify AI systems by risk
  - ✓ Apply safeguards for high-risk systems
  - ✓ Conduct audits & assessments
  - ✓ Ensure data protection & privacy
  - ✓ Provide documentation & user instructions
- Penalties

  Up to **€35M or 7%** of global turnover for serious violations

  Up to **€15M or 3%** for other breaches

Embedded Systems Cybersecurity - Trends & Implementation

RED – Radio Equipment Directive

What?

Ensures safety, compatibility & cybersecurity of radio equipment

Who is concerned?

- Manufacturers
- Importers
- Distributors

When?

In force since **2014,** new cybersecurity rules apply from **Aug 2025**

Steps to Ensure Compliance

- ✓ Meet essential safety & EMC requirements
- ✓ Conduct conformity assessments (e.g., CE marking)
- ✓ Maintain technical documentation
- ✓ Monitor updates & technical changes
- ✓ Train staff on RED obligations

Penalties

NIS2 (Network and Information Security Directive)

Cybersecurity Compliance Overview

What?

The **NIS2 Directive** strengthens cybersecurity across the EU by setting unified requirements for networks and information systems.

Who is concerned?

- Operators of essential services
- Digital service providers
- Medium & large enterprises in 18 critical sectors

When?

- **2024**: Directive enters into force
- **2025**: Compliance obligations begin (pending national transposition)

Penalties

⚠️ Up to **€10 million** or **2% of global turnover**

⚠️ Personal liability for senior management

Steps to Ensure Compliance

“Machines” Directive

Compliance Overview

What?

Establishes **safety requirements** for the **design and manufacture of machinery** in the EU.

Who is concerned?

- **Manufacturers**
- **Importers** of machinery

When?

- In force since **2006**
- Will be replaced by **Regulation (EU) 2023/1230** in **Jan 2027**

Penalties

⚠️ Fines and product recalls

⚠️ Amounts vary by **member state**

Steps to Ensure Compliance

UN Regulation No. 155 (UN R155) – Cybersecurity Management System (CSMS)

Cybersecurity Management System for Vehicles

What?

Mandatory CSMS to manage risks from cyber threats across vehicle lifecycle.

Who is concerned?

- Manufacturers
- Suppliers
- Type approval authorities

When?

Since **July 2022 for** new vehicle types; certificate renewal every 3 years

Penalties

⚠ Loss of type approval

⚠ CMS revocation

⚠ Sales block

UN Regulation No. 156 (UN R156) – Software Update Management System (SUMS)

Road Vehicles Cybersecurity Engineering

What?

Secure software update process with traceability, validation, and authority access.

Who is concerned?

- Vehicle **manufacturers**
- Embedded system **suppliers**
- Type approval **authorities.**

When?

Applies to new vehicle types; compliance during design and every update cycle.

Penalties

⚠️ Loss of type approval

⚠️ SUMS certificate revocation

⚠️ Blocked updates

ISO/SAE 21434 – Road Vehicles Cybersecurity Engineering

Road Vehicles Cybersecurity Engineering

What?

Cybersecurity standard for vehicle systems across lifecycle

Who is concerned?

- Manufacturers
- Suppliers
- Subcontractors
- Auditors

When?

Design to end-of-life; update after major changes or audits.

Penalties

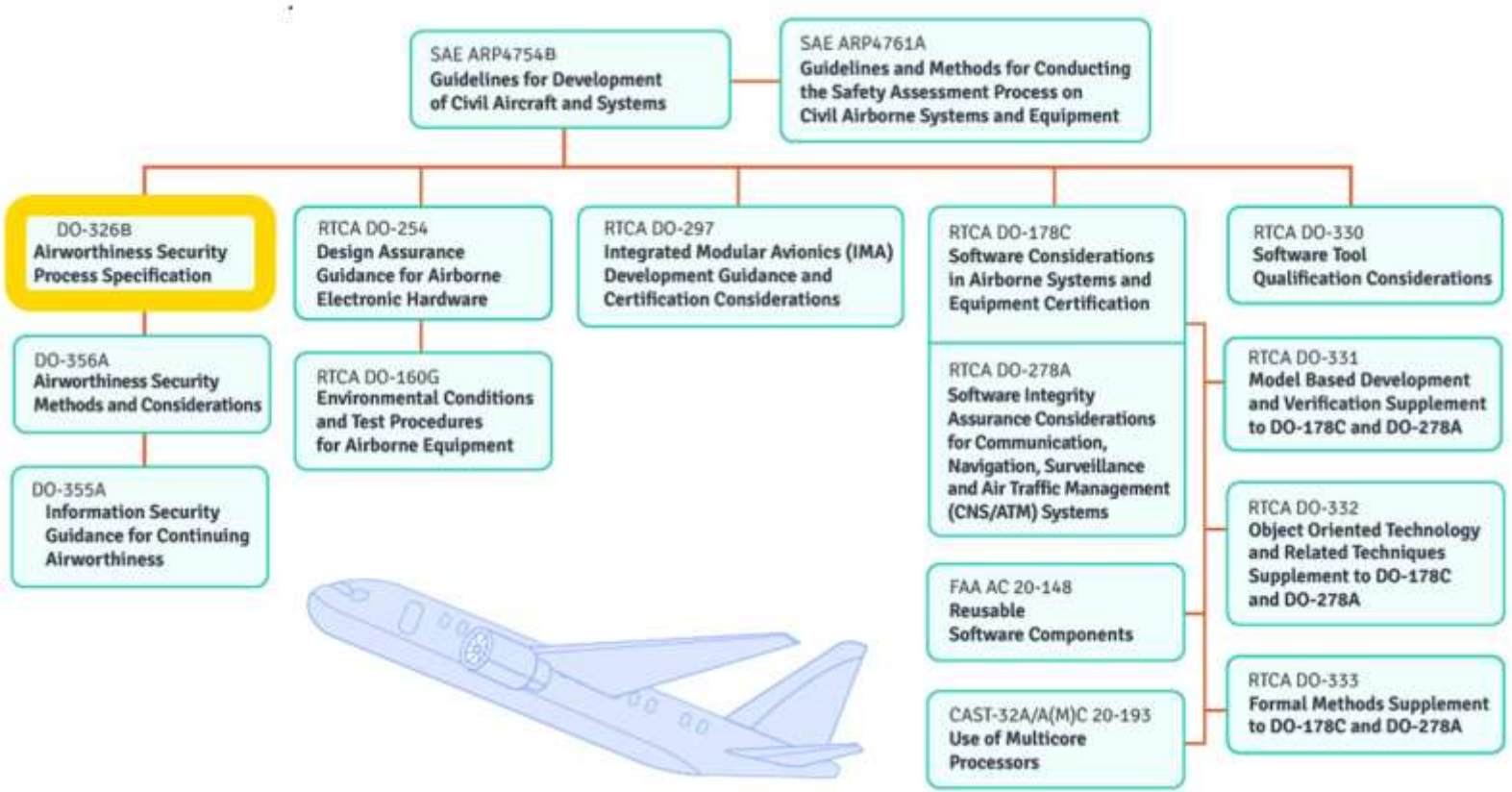
⚠️ Audit failures, Loss of certification, Commercial risks

Steps to Ensure Compliance

✔ Governance

Embedded Systems Cybersecurity - Trends & Implementation

Regulatory framework for airworthiness



DORA (Digital Operational Resilience Act)

What?

Enhances the **digital resilience** of financial institutions against cyber threats and ICT disruptions.

Who is concerned?

- Financial institutions
- ICT service providers

When?

- **2024**: Enters into force
- **2025**: Compliance obligations begin

Penalties

⚠️ Up to **2% of global turnover**
⚠️ Up to **€5M** for critical third parties
⚠️ Up to **€1M** for individuals

Steps to Ensure Compliance

✓ Implement strong IT security measures
✓ Conduct resilience testing & assessments

Embedded Systems Cybersecurity - Trends & Implementation

Your Compliance, Through Cybersecurity Journey

We offer **end-to-end solutions** to help you meet regulatory compliance:

- Risk Assessments
  - 🔍 Identify and mitigate potential risks
- Security Implementations
  - 🔐 Deploy tailored cybersecurity measures
- Continuous Monitoring
  - 📊 Track compliance status & respond quickly
- Training Programs
  - 🎓 Educate staff on best practices & requirements

How to comply and become resilient ?

Certification is One Stream

Achieving certification is a key step in demonstrating compliance.

For example:

- EUCC (European **C**ybersecurity **C**ertification): Part of the EU CRA, leveraging Common Criteria to certify the security of digital products. – Publication of a *vade mecum* Feb 18, 2025,
- ISO/IEC 27001: International standard for information security management systems.

Technology is Another

Leveraging advanced technology can also ensure compliance:

- AI and Machine Learning: Automate compliance monitoring and threat

Embedded Systems Cybersecurity - Trends & Implementation

Providing the Means for Compliance

Takeaways & Call to Action

Key Takeaways

- ✅ Regulatory complexity clarified
- ✅ Compliance elements presented
- ✅ Local partners are available to support you

Call to Action

- 🔐 Organize your company to be cybersecure & compliant
- 🧭 Adopt our step-by-step methodology
- 🤝 Consider joining **Embedded France** association to share & grow expertise

Embedded France
L'EMBARQUÉ MADE IN FRANCE

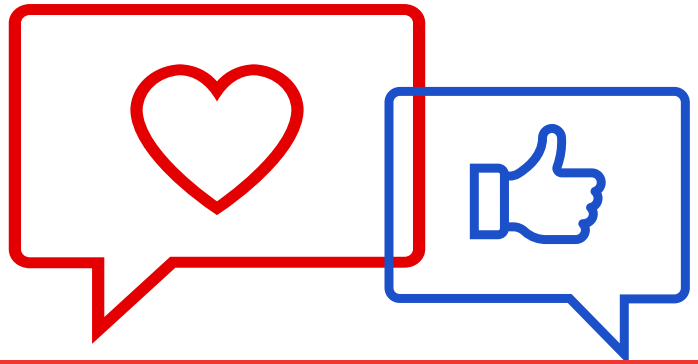
Embedded Systems Cybersecurity - Trends & Implementation

Agenda

numeum
Engager
le numérique

Embedded France
L'EMBARQUÉ MADE IN FRANCE

numeum
Engager le numérique



Cendrine Barruyer, Déléguée générale
contact@embedded-france.org

06 61 84 53 70

Visitez notre site web :
Http://www.embedded-france.org/