FM Approvals

Questions & Answers from “CRA & RED Explained: Compliance, Timelines & Impact”

Q1: Does RED-DA also apply to products that 'can' connect to the internet but are not intended to? For example, industrial Ethernet products that operate on a local network on-site but are not connected to the public internet.

A1: The **RED Delegated Act (EU) 2022/30** can apply to products that are **capable** of connecting to the internet, even if they are **not intended** to be used that way in a specific deployment - such as industrial Ethernet products operating only on local networks.

- The RED cybersecurity requirements (Articles 3.3 (d), (e), and (f)) apply to **radio equipment that is capable of connecting to the internet**, whether directly or indirectly.
- This means that even if a device is **not connected to the public internet in its intended use**, it may still fall under the scope if it has the **technical capability** to connect.

Q2: For IIoT equipment that can receive over-the-air (OTA) updates to improve performance or introduce new features, do these products need to be recertified for new feature releases if we already have an SDLA certificate?

A2: Before responding to the question, let’s look at two important terms: update and upgrade, as defined in the ISA/IEC-62443 standards.

Update – “incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues”.

Upgrade – “incremental hardware or software change in order to add new features”.

Coming back to the question, an SDLA or Secure Development Lifecycle Assurance certification based on the ISASecure® scheme requires that the product supplier’s development processes and practices are compliant with the SDL practices defined in the ISA/IEC-62443-4-1. One of these practices is the Security Update Management (SUM). Under this practice, the product supplier is required to not only provide timely security updates for any security related issues but also test and document them, ensure their validity, and that they do not introduce regressions, etc. An SDLA certified product supplier is expected to do this for the **updates**. Hence there is no retesting of the product involved.

However, for the product to maintain its 4-2 (or 3-3) certification, any **upgrades** to the product—which adds new features and functionality to the product—requires additional assessment to ensure these new features and functionality does not impact the security of the product negatively.

© 2025 FM Approvals. All rights reserved.

Q3: Can you provide an estimated timeframe for each certification program (SDLA, SSA, and CSA) for Industrial IoT products?

A3: Firstly, industrial IoT products, or IIoT products, have their own ISASecure® certification called the IIoT Component Security Assurance (ICSA). This is based on ISA/IEC-62443-4-2 standard but with a few additional technical requirements which are applicable to an IIoT product.

As for the timeframe for the certification programs, it depends on several factors. For instance, the SDLA assessment depends on the availability of the processes and policies documentation for the 4-1 practices; developer resources assigned to the assessment project, and the responsiveness of the developers to our questions and clarifications. The duration also depends on whether the required secure development tools such as static code analysis (SCA), fuzzing tools for the communication protocols, etc., are deployed and utilized by the development team. Typically, assessment of a mature organization which has most of the processes and tools in place and has been utilizing them could potentially be done in as little as **three months**. For a company that is fairly new to SDL, it may take **up to a year**.

Similarly, product assessments (CSA, SSA, or ICSA) will depend on several factors including the targeted security level, product complexity, availability of artefacts, resources assigned, etc. CSA and ICSA may take anywhere from **3 to 6 months**, whereas SSA will take longer depending on how many zones and interfaces are supported by the system.

Given the time all this takes, as was mentioned in the webinar, it is strongly recommended that product manufacturers targeting CRA compliance embark on this journey sooner than later.

Q4: Can you say with confidence that the CRA harmonized standards will be based on the ISA/IEC 62443?

A4: We can say with **high confidence** that the **Cyber Resilience Act (CRA)** will be **closely aligned** with the **ISA/IEC 62443** series of standards, but it is **not guaranteed** that the harmonized standards under the CRA will be exclusively based on IEC 62443 alone.

CEN/CENELEC and **ETSI** have accepted the request from the European Commission to come up with the harmonized standards for CRA. The **CLC/TC 65X WG3 has been working on adapting the ISA/IEC-62443 standards as the basis for the CRA harmonized standards.**

The ISA/IEC-62443 standards are **globally recognized**, **vendor-neutral**, and **already widely adopted** for industrial cybersecurity. You can **confidently use ISA/IEC 62443** as a **foundation** for CRA compliance, especially for **Industrial IoT and OT products**. However, once the **official CRA harmonized standards** are published, you'll need to **verify alignment** and **adjust accordingly**.

Q5: Please clarify the last part of the flowchart on CRA applicability to a product - If it is SaaS and there is another product .. what does that exactly mean?

A5: If another product is utilizing the cloud or Software as a Service (SaaS), then that product has to comply with the CRA.

Q6: CRA - Assessment Types. Row 2, column 2 of the table in your presentation says "Manufacturer DOES NOT apply harmonized standards or certification..." Is this correct?

A6: The slide should have said "**IF** the manufacturer does not apply harmonized standards...". In which case a third-party assessment is needed. The third party takes care of this assessment, so the manufacturer does not have to apply harmonized standards by themselves.

© 2025 FM Approvals. All rights reserved.

Q7: Does the SBOM requirement in CRA cover embedded software, firmware, etc. as well?

A7: Under the **Cyber Resilience Act (CRA)**, the **Software Bill of Materials (SBOM)** is expected to cover **all software components**, including:

- Embedded software
- Firmware
- Third-party libraries
- Open-source components
- Proprietary modules

The CRA applies to **"products with digital elements"**, which explicitly includes:

- Hardware with embedded software
- IoT devices
- Industrial control systems
- Firmware-driven components

Q8: Is the ISA/IEC-62443 Part 3-3 based certification (System Security Assurance) applicable to asset owners?

A8: The **ISA/IEC 62443 Part 3-3 (System Security Requirements and Security Levels)** is **highly relevant for asset owners** who are operating **Industrial Automation and Control Systems (IACS)** or **Industrial IoT environments**. **ISA/IEC 62443-3-3** defines **technical security requirements** for systems and is intended to be applied by:

- **Asset owners** (e.g., factories, utilities, infrastructure operators)
- **System integrators**
- **Service providers**

However, ISASecure's **System Security Assurance (SSA) certification** itself is aimed at assessing and certifying systems as developed by product manufacturers.

© 2025 FM Approvals. All rights reserved.

Q9: For ISA/IEC-62443 Part 4-2, you mentioned an ISASecure® IIoT certification scheme. Is this only for IIoT or for all types of components?

A9: The **ISASecure® IIoT Component Security Assurance (ICSA) Scheme** is **specifically tailored for IIoT components**, but it is **not the only scheme** available under the ISASecure® certification umbrella. Here's how it fits into the broader picture:

ISASecure Certification Schemes Overview

Scheme	Target	Based on	Applicability
SDLA (Security Development Lifecycle Assurance	Development organizations	ISA/IEC 62443-4-1	Product manufacturers‘ development practices
CSA (Component Security Assurance)	Embedded devices, software applications, network devices, and host devices	ISA/IEC 62443-4-2	All IACS components
ICSA (IIoT Component Security Assurance)	IIoT devices and gateways	ISA/IEC 62443-4-2 + IIoT specific enhancements	Specifically for IIoT components
SSA (System Security Assurance)	Integrated systems (e.g., SIS, SCADA, DCS systems, skids and packages, etc.)	ISA/IEC 62443-3-3	System-level certification

Q10: How should NIS 2 entities use CRA and RED?

A10: Entities subject to the **NIS 2 Directive** (NIS2) should view the **Cyber Resilience Act (CRA)** and the **Radio Equipment Directive Delegated Act (RED-DA)** as **complementary frameworks** that help them meet their broader cybersecurity obligations:

- **CRA** ensures that digital products (hardware/software) meet baseline cybersecurity requirements.
- **RED-DA** ensures that **radio equipment** (e.g., wireless routers, IoT devices) is secure by design.
- **NIS2 entities** should **prioritize purchasing CRA- and RED-compliant products** to reduce supply-chain risk and meet their own risk management obligations.

Q11: What is the source for applicability of the CRA (products put in the market 36 months from the entry of this regulation)?

A11: The **Cyber Resilience Act (CRA)** will apply to products **placed on the EU market 36 months after its entry into force**. This timeline is officially confirmed by the **European Commission** and the Council of the EU.

© 2025 FM Approvals. All rights reserved.

Q12: What is the minimum SDLA maturity level needed to meet the minimum requirements for CRA?

A12: As of now, the **Cyber Resilience Act (CRA)** does **not explicitly mandate a specific SDLA Maturity Level (ML)** from the **IEC 62443-4-1** standard. However, based on current guidance and industry interpretation, the **bare minimum maturity level** that may align with the CRA expectations is considered to be **at least Maturity Level 2 – Managed** but it is strongly recommended that product manufacturers should really be targeting **Maturity Level 3 – Defined (Practiced),** which is when they demonstrate that the SDL practices are actually being utilized in the design and development of products.

Q13: Can a system be certified if you are at SLDA maturity level 2?

A13: A product could potentially **be certified** under **IEC 62443-3-3** (System Security Assurance) or a component under **IEC 62443-4-2** (Component Security Assurance) **if the organization's Secure Development Lifecycle (SDLA) is certified at Maturity Level 2 (ML2)**. However, during the assessment of the product (CSA/SSA), it must be clearly established that the organization's SDL processes were employed during design and development of that product.

Q14: What is the difference between an update and upgrade exactly? When does it count as a feature?

A14: The definitions of update and upgrade have been covered in an earlier Q&A. This distinction between **update** and **upgrade** is important, especially in the context of **product lifecycle management**, **cybersecurity regulations** like the **Cyber Resilience Act (CRA)**, and **technical documentation**:

-An **update** is:

- A **minor change** to the existing software or firmware.
- Intended to **fix bugs**, **patch vulnerabilities**, or **improve performance**.
- Does **not change the core functionality** or purpose of the product.

-An **upgrade** is:

- A **major revision** that introduces **new capabilities**, **significant changes**, or **enhanced performance**.
- May require **re-certification** or **re-evaluation** under regulatory frameworks.
- Often involves a **major-version jump**.

Under the **Cyber Resilience Act**:

- **Security updates** are **mandatory** and expected throughout the product lifecycle.
- **Upgrades or new features** may require:
  - **Reassessment of conformity**
  - **Updated technical documentation**
  - **Re-declaration of compliance** if the product's intended use or risk profile changes.

Q15: I am from Saudi Arabia. Is this CRA full compliance going to be rolled across the globe?

A15: **CRA** is an **EU regulation**, but its **impact is expected to extend globally,** similar to GDPR.

© 2025 FM Approvals. All rights reserved.

Q16: Is RED a layer on top of CRA? (In other words, to be RED compliant, is the CRA compliance a pre-requisite?)

A16: **CRA compliance is not a prerequisite for RED compliance**, but the relationship between the two is evolving. It is expected that **CRA will eventually replace RED cybersecurity requirements** for certain products.

Regulation	Applies To	Status	CRA Dependency
RED	Radio-enabled devices	Active until Dec. 2027	Independent (for now)
CRA	All products with digital elements	Mandatory from Dec. 2027	Will likely replace RED cybersecurity rules

So, while **CRA is not currently a layer on top of RED**, it is expected to **become the unified cybersecurity framework**, effectively **replacing RED's cybersecurity provisions**. Manufacturers aiming for long-term compliance should prioritize CRA readiness.

Q17: Do we know what will happen to EN18031 once CRA overtakes RED Cyber Requirements?

A17: EN 18031 will remain **valid and mandatory** for RED compliance until CRA fully takes over. EN 18031 is **expected to be integrated into the CRA framework** as a **technical standard** supporting CRA compliance. It is said that ENISA and CEN/CENELEC are already **mapping EN 18031 to CRA requirements**.

Q18: Do we know what Security Levels (SL) within ISA/IEC-62443 will be the requirements to meet CRA? Will it vary per requirement, or will it be one general level?

A18: As of now, **the EU Cyber Resilience Act (CRA)** does **not mandate a specific Security Level (SL)** from the **ISA/IEC 62443** series as a blanket requirement. Instead, the **required level of cybersecurity assurance will vary depending on the product category and risk classification**.

Q19: Is CE marking only for critical products?

A19: No, **CE marking is not only for critical products**. It is **mandatory for a wide range of products** that fall under specific **EU directives or regulations**, regardless of whether they are considered critical or not.

Q20: Apart from the descriptions in ISA/IEC-62443 Part 4-1, Table 1 – Maturity Levels, are there any specific verification differences for each practice across different maturity levels? Also, is there any corresponding documentation available for reference?

A20: There **may be specific verification differences across maturity levels** for each practice in **ISA/IEC 62443-4-1**, beyond what's described in **Table 1 – Maturity Levels**. These differences are especially relevant during **Security Development Lifecycle Process Assessments (SDLPA)** and **certification audits**. Contact ISASecure® or FM Approvals for more details.

Q21: Continuous upgrades are part of the lifecycle (and benefit) of modern, software-enabled products. Given the requirement for re-certification incurred by upgrades (which also reset or extend the support period), why would any OEM release regular enhancements to their products?

A21: See the Q&A on the difference between updates and upgrades above. A product manufacturer has many incentives to release **upgrades** such as adding new functionality and features to their products, differentiating themselves from others, etc. It only makes sense that these features are assessed for their security robustness before they are released. It is important to note that re-certification will only assess the areas impacted by the new functionality that was added, so it will be a much shorter assessment exercise.

© 2025 FM Approvals. All rights reserved.

Q22: If a company is already certified to IEC 62443-4-1, is there any additional benefit from SDLA certification?

A22: **SDLA certification** is a **third-party certification** offered by ISASecure® that **verifies and validates** a company's development processes for **conformance to ISA/IEC 62443-4-1**.

Certification to ISA/IEC-62443-4-1 is the same as getting certified for SDLA certification when the ISASecure® scheme is used. In other words, an ISA/IEC-62443-4-1 assessment done as per ISASecure® scheme is called SDLA certification.

Q23: Do you think it is valuable to follow EN18031 for CRA until the time harmonized standards for CRA are not publicly available?

A23: It is **beneficial and recommended** to follow the **EN 18031 series** as a **preparatory framework for CRA compliance**, even though these standards are currently harmonized under the **Radio Equipment Directive (RED)** and **not yet officially harmonized for the Cyber Resilience Act (CRA).** It helps:

- **Accelerate CRA readiness**
- **Reduce future rework**
- **Demonstrate proactive compliance** to authorities and customers
- **Align with RED cybersecurity requirements** (mandatory from August 1, 2025)

Q24: Are there products/services that are not in the scope of CRA but only in the scope of NIS2?

A24: **CRA** has a focus on product-level cybersecurity. **CRA applies to**: products with digital elements (hardware/software) placed on the EU market (smart devices, software, IoT, PLCs, embedded systems, etc.)

NIS2, on the other hand, has a focus on organizational cybersecurity. NIS2 **applies to**: essential and important entities operating critical services (energy, transport, healthcare, finance, public administration, cloud services).

Q25: Will CRA apply to end users, for example, oil and gas companies or car manufacturing companies, as they may be using smart devices?

A25: The **EU Cyber Resilience Act (CRA)** applies to the product supply chain **(economic operators who place Products with Digital Elements (PDEs) on the EU market),** including manufacturers, importers, distributors, and resellers. It does **not directly apply to end users** such as **oil and gas companies** or **car manufacturers just because they use smart devices**. However, there are **indirect implications** depending on their role in the supply chain.

Role	Does CRA Apply?	Notes
Manufacturer of smart devices	Yes	Must comply with CRA
Importer/distributor of smart devices	Yes	Must ensure CRA compliance
End user (e.g., oil & gas company using smart sensors)	No	Not directly affected
End user who integrates and sells smart systems	Possibly	Depends on market placement

© 2025 FM Approvals. All rights reserved.

Q26: If a PLC or smartwatch that is made in China is sold in the EU, will those manufacturers need to obtain CRA certification?

A26: Yes, **PLC (Programmable Logic Controllers)** and **smartwatches made in China and sold in the EU** will need to comply with the **EU Cyber Resilience Act (CRA)** if they qualify as **Products with Digital Elements (PDEs)** - which they almost certainly do.

Q27: Is CRA applicable to a system (as defined by ISA/IEC 62443-3-3)?

A27: **Systems as defined by ISA/IEC 62443-3-3** can fall under the scope of the **EU Cyber Resilience Act (CRA)** - if they are placed on the EU market as a product or solution.

If someone is developing or deploying a system that aligns with **ISA/IEC 62443-3-3** and plan to **sell or operate it in the EU**, they should:

- **Assess whether the system qualifies as a Product with Digital Elements (PDE)** under CRA.
- **Map their IEC 62443 compliance to CRA requirements** - identify gaps.
- **Prepare for CRA conformity assessment**, especially if the system is critical or high-risk.

Aspect	ISA/IEC 62443-3-3	CRA
Scope	Industrial systems (IACS)	All network-connected digital products
Focus	System-level security requirements	Product level cybersecurity and market compliance
Certification	Voluntary, industry-driven	Mandatory for EU market access
Lifecycle	Full system lifecycle	Focused on product placement and post-market obligations

© 2025 FM Approvals. All rights reserved.

Q28: It was mentioned that non-commercialized SW is out of the scope of CRA. Are there exceptions? Here is an example: Non-commercialized SW for programming critical products.

A28: **CRA** does **exclude non-commercial software** from its scope **in general**, but there are **important exceptions**, especially when such software is used in **critical contexts** like programming or configuring critical products.

The CRA **does not apply** to:

- **Free and open-source software** developed **with no commercial intent**.
- Software that is **not placed on the market** (i.e., not distributed or made available to users in the EU).
- Software used **internally** and not intended for external distribution.

However, if the software is **used in connection with a commercial product**, or if the developer **derives commercial benefit** (e.g., through support, integration, or licensing), it **may fall under CRA scope**.

Software Type	CRA Applicability
Free/open source, no commercial use	Not in scope
Free/open source, but monetized (e.g., support, integration)	In scope
Non-commercial software used to configure critical products	Possibly in scope
Internal-use-only tools not distributed	Not in scope
Software bundled with commercial products	In scope

Q29: If I am building a product with components that are not CRA compliant, but in scope, can my end product be compliant?

A29: CRA requires that the final product that is placed on the market is compliant. The assessment is done at this final product level.

Q30: About lifecycle support plans, can you please discuss why minimum is 5 years but then updates need to be available for 10 years? When you mean that updates are just cybersecurity related updates?

A30: Security updates must be provided for the entire support period of the product, which is:

- At least 5 years, or
- The expected lifetime of the product, whichever is longer.

After the support period ends, manufacturers must keep the security updates available for download for at least 10 additional years, even if they stop actively maintaining the product. Please consult Article 13 of the CRA for more information.

© 2025 FM Approvals. All rights reserved.

Q31: Can the Notified Body (NB) act as an authorized representative (as they hold the technical file) for the manufacturer based outside the EU?

A31: A **Notified Body (NB) cannot act as an Authorized Representative (AR)** under the **CRA**.

Key Distinction: Notified Body vs Authorized Representative

- A **Notified Body** is a **third-party conformity assessment organization** designated by an EU Member State to assess whether products meet the requirements of applicable EU legislation (like CRA).
- An **Authorized Representative** is a **legal entity established in the EU** that is **appointed by a manufacturer located outside the EU** to carry out specific compliance tasks on their behalf (e.g., keeping the technical documentation, cooperating with market surveillance authorities).

CRA Article 29 – Independence of Notified Bodies

According to **Article 29(4)** of the CRA:

A conformity assessment body (i.e., a Notified Body), its top-level management and personnel **shall not be**:

- The **designer, developer, manufacturer, supplier, installer, purchaser, owner, user or maintainer** of the products they assess.
- The **authorized representative** of any of those parties.

This clause ensures that Notified Bodies remain **independent and impartial**, avoiding any **conflict of interest** in the conformity assessment process.

FM Approvals

© 2025 FM Approvals. All rights reserved.