itk ENGINEERING

CYBER SECURITY AS A MARKET ACCESS REQUIREMENT

What the RED DA requires and how to get it right

ITK Engineering GmbH | www.itk-engineering.com | industry@itk-engineering.de

1. ABSTRACT

Starting in August 2025, the RED Delegated Act for cyber security (RED DA) will, for the first time, mandate binding security requirements for radio equipment (e.g. certain wireless-connected products). For manufacturers, this means: little time, lots of questions – and significant pressure to act. But those who see RED as just another regulatory burden miss the bigger picture. With RED, cyber security becomes a *prerequisite for market access* – and those who act now are already paving the way for the upcoming Cyber Resilience Act (CRA). In this article, we'll share why more manufacturers are affected than expected, show how to demonstrate compliance with the RED DA directive and explain what matters most when implementing the key standard EN 18031.

2. THE RADIO EQUIPMENT DELEGATED ACT – CYBER SECURITY BECOMES MANDATORY

From August 1st onwards, manufacturers of equipment that contain radio components must have a keen eye on the Radio Equipment Directive Delegated Act for cyber security (RED DA). This regulation comes with new cyber security obligations that must be fulfilled to make products available on the European market.

What is often overlooked: the RED DA could also apply to products that do not come to mind immediately. In particular, it applies to combinations of non-radio and radio equipment. This is the case if the radio equipment part is incorporated into the non-radio product and is permanently affixed (i.e. in such a way that it cannot be easily accessed and readily removed) to the non-radio product. Given that many products incorporate a radio module of some sort nowadays, the regulation applies to a wide range of products beyond just equipment with "radio" as its core function. Manufacturers must ensure that the radio module's compliance is maintained within the final product – which can mean that applying the RED requirements to the complete system becomes necessary, even if the module was already compliant as a standalone component.

While these new obligations may pose a challenge for many manufacturers at first, they also offer a chance in the long run. Building secure products reduces risks for manufacturers themselves – yet in the past, cyber security was often considered a cost driver, not a competitive advantage. That's now changing: under the new regulation, investing in cyber security is no longer optional or potentially disadvantageous.

All manufacturers who want to compete on the European market must meet the same cyber security requirements. This levels the playing field – and rewards those who take security seriously.

On top of that, the essential requirements of another major regulation – the EU Cyber Resilience Act (CRA) – will become fully mandatory in December 2027. The RED DA is a strong foundation for this: complying with RED already covers many key elements of CRA compliance. Both regulations share several core requirements, including cyber security risk assessments, documentation requirements and conceptional cybersecurity mechanisms. Meeting RED requirements now means manufacturers are already a big step closer to being CRA-ready.

In a nutshell, the RED DA defines 3 essential requirements regarding the cyber security of radio equipment [1]:

"Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(...)

(d)

radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(e)

radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(f)

radio equipment supports certain features ensuring protection from fraud;

(...)"

These essential requirements are fairly abstract and prone to interpretation. There are multiple ways to deal with this challenge.

3. THE ROAD TO RED DA COMPLIANCE

Compliance with the essential requirements that are set out in the RED DA can be demonstrated in three different ways – so-called "conformity assessment modules":

Module A – Internal production control

In this approach, the manufacturer ensures and declares on his sole responsibility that the product satisfies the essential requirements set out in the RED DA. This approach can only be followed if the manufacturer adheres to a standard that has been harmonized for the RED DA. The currently harmonized standard is EN 18031. Even though no third party notified body is involved in assessing the compliance of the product in this case, the manufacturer is still obligated to fully apply the standard. All documentation necessary to verify the correct execution of the process must be maintained and stored with the technical documentation, readily accessible to national authorities. These authorities may request these documents at any time to confirm that the internal assessment was properly conducted.

Module B and C – EU-type examination & conformity to type based on internal production control

In this approach, a notified body examines the technical design of the radio equipment and verifies and attests that it meets the essential requirements. This assessment may be based on the harmonized standard EN 18031, but it doesn't have to be. In this case, close collaboration with the notified body is recommended to align on the specific criteria they require for the assessment. If the evaluation is successful, the notified body issues an EU-type examination certificate. After receiving this certificate, the manufacturer must ensure that the products manufactured match the approved type and comply with the requirements of the RED DA.

Module H – Full quality assurance

In this approach, the notified body does not assess each specific product but rather evaluates the manufacturer's quality system used to develop and produce the products. In particular, this includes which standards are applied during development and how compliance with these standards is ensured in practice. The notified body verifies whether the proposed quality system can reliably ensure that all produced products are compliant with the RED DA essential requirements. The quality system must be periodically re-audited, and the notified body may also conduct unannounced inspections to ensure it is functioning properly. As with module A, the manufacturer must keep the technical documentation of both the products and the quality system and make them available to the national authorities upon request.

Due to the effort that assessments of a 3rd party notified body entails and due to the limited capacity of the notified bodies, it's likely that most manufacturers will opt for the "Module A" approach: following the EN 18031 harmonized standard. This allows them to self-assess the product and sign a declaration of conformity. Note however, that even if no third party is involved, the relevant documentation must exist at the time of declaring conformity and must be at the disposal of national authorities for at least 10 years.

4. HOW TO FULFILL THE EN 18031 STANDARD

From our perspective, multiple steps are required to fulfill EN 18031. In the following, we will highlight these steps and provide practical examples.

FULFILL EN 18031 STANDARD

STEP 1	STEP 2	STEP 3	STEP 4
Determination of scope and applicability of EN 18031-1 / -2 / -3	Compile technical documentation as basis for gap analysis against EN 18031	Cyber security risk assessment	Rating for all EN 18031 requirements (Pass / Fail / Not applicable)

Step 1: Determination of scope and applicability of EN 18031-1 / -2 / -3

Firstly, the system scope that falls under RED DA must be determined. In this context it's important to check for the already mentioned "combined product" property [2].
Examples for combined equipment could include:

- a non-radio product PCB that has a Bluetooth module soldered to it
- an IACS that contains a hard-wired telematics unit that is not easily removable

Once the system scope is clear, it must be determined which parts of the EN 18031 are applicable. EN 18031 is divided into three parts, each of which maps to one of the RED DA essential requirements d), e) and f). This also implies that not all three standards are applicable for every product, but it depends on whether the system is ...

- ... directly or indirectly connected to the internet?
  → EN 18031-1 is likely applicable.

Example: A smart home heating controller that is reachable over the internet via a dedicated IP address and communicates wirelessly to remote temperature sensors. This controller only allows a user to set the temperature of a home remotely based on the time and date.

- ... internet connected radio equipment, a childcare product, a toy or a wearable that processes personal or privacy related data?
  → EN 18031-2 is likely applicable.

Example: A wearable smartwatch tracking fitness and health related activity data. This personal data such as heart rate or location should be safeguarded under the EN 18031-2.

- ... enabling users to transfer money, monetary value or virtual currency and is potentially prone to fraud?
  → EN 18031-3 is likely applicable.

Example: That same smartwatch from the previous example which now has the capability to make contactless payments with a digital wallet supporting compatible payment cards. This is now additionally EN 18031-3 applicable.

The three EN 18031 standards overlap with each other to a large degree but also contain specific individual requirements for the intended scope.

Step 2: Compile technical documentation as basis for a gap analysis against EN 18031

The EN 18031 requires a technical documentation (see section A.2.5.2). This documentation also helps to assess the product based on the decision trees that are included for each cyber security requirement that is listed in EN 18031. It should at least contain the following items:

- information on the equipment's intended use
- information on the equipment's expected operational environment of use
- equipment's technical information
- declared state of the art and best practice
- specific details such as a list of external interfaces
- cyber security risk assessment
- security concept

Step 3: Cyber security risk assessment

While EN 18031 contains decision trees for each requirement that suggest a strict "yes/no" logic, arguments have to be documented as to why a "yes" or a "no" was chosen. In many cases, these "yes/no" decisions are not trivial as they depend on the intended use and the operational environment of the system. A cyber security risk assessment is required to take these product-individual factors into account – which is listed as required information in most EN 18031 requirements.

> „... If and how generic security objectives are to be achieved depends on the intended equipment functionality and the intended operational environment of use. They influence the actual required implementation of security measures and the strength of those controls in a specific equipment. A specific security measure might be appropriate for a product but might be too weak or strong for other products or the same product when used in another environment." [3]

Example: [SSM-1] Applicability of secure storage mechanisms [4]

- The goal of the requirement: "The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment ..."
- There are multiple secure storage mechanisms with varying security properties: "The security assets and network assets can be protected by e.g.:
  - cryptographic measures like encryption to ensure confidentiality,
  - cryptographic measures like digital signatures to ensure integrity and authenticity,
  - access control using authentication or authorization,
  - hardware protection measures
  - physical protection measures"
- But which of those are appropriate depends on the risk assessment: "The appropriate protection mechanism depends on the risks associated with the security assets or network assets to be stored ..."

EN 18031 does not specify how this cyber security risk assessment should be conducted. Therefore, companies have the flexibility to choose a methodology based on their individual needs. Companies with many product variants will likely reuse risk model components, and those with a single product may take a more straightforward approach to risk assessment.

Step 4: Rating for all EN 18031 requirements (Pass / Fail / Not applicable)

Each requirement has applicability criteria that can potentially render the requirement irrelevant for a given product. If a requirement is applicable, it has to be ensured that appropriate mechanisms are put in place to satisfy it. EN 18031 captures this process for each requirement in a decision tree. The path taken in the decision tree to end up in a "Pass" or "Not applicable" state have to be documented along with the according rationales.

Example: [ACM-1] Applicability of access control mechanisms [5]

- The smart home controller mentioned in a previous example is intended to allow only authorized homeowners to remotely adjust their home's temperature. It is not intended for public access to these temperature settings as well.
- The device is delivered to the end user configured for access via a public IP address, not secured behind a properly configured local network firewall.
- Finally, there are no legal restrictions which do not allow access control mechanisms. Therefore, the absence of an access control mechanism for this system would fail to meet the applicability criteria found in section 6.1 of EN 18031-1.

5. CONCLUSION

The timeline for RED DA compliance is challenging for many manufacturers. On top of that, many are not yet aware that they are affected by the RED DA and risk non-compliance with the associated penalties. However, even without RED DA, many systems already have cyber security mechanisms in place that just have to be documented and mapped to the EN 18031. In many cases this constitutes a big step towards compliance already.

Third-party certification is not required in many cases if EN 18031 is followed, but market surveillance can check this anytime. So, it is advisable to implement the required measures and document them as soon as possible. This effort is not wasted and is a first step towards EU CRA compliance – a horizontal cyber security regulation for which the clock is already ticking towards the deadline in December 2027.

Sources

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20241228
[2] https://ec.europa.eu/docs-room/documents/29121
[3] EN 18031-1
[4] EN 18031-1
[5] EN 18031-1

ITK ENGINEERING

Anything goes, from embedded systems to cloud computing and artificial intelligence – ITK Engineering, a global tech company, draws on methods-driven expertise to provide platform-independent software and system development services. The company is an innovative force in digital engineering. Customers in sectors ranging from automotive, industrial, and railway engineering to medical systems, agricultural/ construction machinery, and motorsports count on ITK to instill intelligence in highly complex systems. The company has been a wholly owned subsidiary of Robert Bosch GmbH since 2017.

Building digital solutions with a firm grasp of many methods

ITK Engineering's skill set has a deep methodological focus on model-based software development, safety, cyber security, artificial intelligence, and computer vision. This wide-ranging, methods-driven expertise enables us to develop digital and sustainable solutions for customers across industries. We are the go-to partner every step of the way, from the inceptive idea to industrialization and standards-compliant approval. What sets ITK Engineering apart is the range of our experience. Our international teams work in very different industries and can apply the insights gained in one sector to another. This diversity of perspectives opens up unprecedented possibilities for customers.

Jens Köhler
Chief Expert Cyber Security
Jens.Koehler@itk-engineering.de

William McCaig
Project Manager
William.Mccaig@itk-engineering.de

ITK. The Art of Digital Engineering.

ITK Engineering GmbH
Headquarter Ruelzheim
Im Speyerer Tal 6
76761 Ruelzheim
Tel.: + 49 (0)7272 7703-0
Fax: + 49 (0)7272 7703-100
info@itk-engineering.de

industry@itk-engineering.de

Follow us on: