WHITE PAPER

FOUNDRIES.IO

Compliance with EU cybersecurity law

The present threat to embedded device manufacturers, and the value of a platform Linux solution

Roger Edgar
Business Development Manager, QUIC
Member of the Foundries.io Team
August 2024

Introduction of new compliance regulations and legislation have often proved to be negatively impactful on an organization's ability to operate – EVEN WHEN there has been ample time and forewarning to integrate the appropriate modifications to systems and procedures. The last prime example is the adoption of GDPR and the impact it had on companies' abilities to maintain online operations.

There is a new requirement that will have a greater impact on businesses moving forward. Not addressing these clear requirements may result in immediate loss of revenue and market share.

Compliance in areas of a business such as health and safety, tax liability and employment are generally regarded as a staid, dry, technical function – something that a company should be able to get right 100% of the time.

Today, however, one compliance issue threatens to derail the operations of large numbers of embedded device OEMs. The European Union's (EU's) Cyber Resilience Act (CRA) is a strategically significant piece of legislation, which has been approved, but is yet to be adopted, that looks to place the responsibility of protecting a device from the risk of cyber attack not on its owner, or on the retailer which sold it to the owner, or on any provider of online services or internet access on which the device relies: responsibility for cybersecurity protection rests, under the CRA, with the device manufacturer.

And since the scope of the cybersecurity functions required under the CRA is broad, the compliance effort will affect every facet of an embedded device manufacturer's engineering operations, from development through production to fleet management.

The evidence today is that few companies are ready for implementation of the CRA, and time is running out: the law is due to be enacted in the near future, and manufacturers then have up to 36 months to apply the rules. Failure to comply carries severe penalties, including the potential for fines of millions of euros, and the obligation to withdraw non-compliant products from sale in Europe.

This white paper describes why the CRA is so important to the embedded world, and why OEMs are finding it so hard to prepare for compliance. It also explains why a horizontal Linux® platform model underpinning security feature development, deployment and maintenance processes provides the most effective and dependable approach to compliance, not only with the CRA but also with other similar regulatory initiatives coming into force worldwide.

The broad scope of the CRA's requirements

In drafting the CRA, the European Union's goal was to encode in law the best practices that industry leaders in cybersecurity already implement.

The CRA is a reasonable and proportionate response to the general failure of the embedded industry to help protect from cyber attack of IoT devices that have a direct or indirect connection to the internet.

This is a change from prevailing attitudes to cyber threats. In the 2010s, it is fair to say that cybersecurity was chiefly regarded as an issue for the enterprise computing world: PCs and servers were the obvious targets for malware and cyber-intrusion.

But the CRA recognizes that the threat now applies to every type of connected device – and since makers and users of enterprise computing equipment have succeeded in erecting effective defenses against hackers, the focus of cyber attacks is shifting towards the billions of IoT and embedded devices in the field. As the European Commission's introduction to the CRA points out:

'From baby-monitors to smart watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present. The act aims to safeguard consumers and businesses buying or using products or software with a digital component. The act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.' [1]

These last words – ‘extending throughout the product lifecycle’ – make clear that the CRA’s measures are wide-ranging and affect more than just the product development process. The EU outlines the requirements of the act like this [2]:

- Cybersecurity is taken into account in planning, design, development, production, delivery and maintenance phase
- All cybersecurity risks are documented
- Manufacturers will have to report actively exploited vulnerabilities and incidents
- Once sold, manufacturers must ensure that for the duration of the support period, vulnerabilities are handled effectively
- Clear and understandable instructions for the use of products with digital elements
- Security updates to be made available to users for the time the product is expected to be in use

These requirements are sensible, proportionate and – because they reflect industry best practice – effective. So it seems very likely that they will provide a model for governments around the world that are seeking to encode cybersecurity protections in law. Just as the EU’s GDPR (General Data Protection Regulation) has in effect set a global standard for protection of the privacy of citizens, so the CRA may set the standard for cybersecurity protection.

What the law says: how to implement the CRA in practice

So upon adoption, the clock will start ticking for embedded device manufacturers that produce in, or export products into, any member country of the European Union or European Economic Area – the region to which the CRA will be directly applicable.

In no more than 36 months from the date of ratification of the law manufacturers must have implemented product designs and developed a full set of processes and capabilities to fully secure their products for life. As it stands, the act does not specify the technical standards that will define how manufacturers should implement the legislation. The European Commission says:

‘To make it easier for manufacturers – in particular for those that build important products – to apply the essential requirements, the Commission will issue a standardization request, allowing the European Standardisation Organisations to develop technical standards for many of the product categories covered by the Cyber Resilience Act.’ [3]

The CRA will build on measures imposed by the EU’s CE RED (Radio Equipment Directive) 2014/53/EU certification for wireless devices, expected to come into force in August 2025. According to the European Commission, product developers aiming to achieve compliance with CE RED can work today on the basis of EN 18031, a harmonized standard governing cybersecurity. This new standard is still in draft form; the existing ETSI 303 645 and IEC 62443-4-2 standards can be used to guide the early stages of cybersecure product development until EN 18031 is ratified.

This same guidance applies to the compliance effort for the CRA until appropriate standards are ratified.

Even in the absence of a standardized model of cybersecurity implementation, however, the main requirements for compliance are already clear. Embedded devices will require features including:

- Secure boot
- Secure key storage
- Software bill-of-materials (SBOM)
- Ability to receive and implement secure over-the-air or local updates

These product functions will need to be backed by cybersecurity processes managed by the product manufacturer for functions such as:

- Storage and protection of secrets such as private keys
- Secure provisioning of production units
- Maintaining an up-to-date SBOM for all production units in the field
- Monitoring common vulnerabilities and exposures (CVEs), and reporting on and protecting against identified exposures

The broad scope of the CRA's requirements means that compliance calls for a prompt, concerted and effective response on the part of embedded device manufacturers. So why is it proving difficult for many manufacturers to mount such a response?

Cybersecurity in the complex and chaotic world of Linux-based device manufacturers

Given the scale of the known threat to embedded devices and the publicity given to successful exploits against connected devices such as baby monitors and toys, it is surprising that many devices are released to the market even today without basic security capabilities such as secure boot and a root-of-trust backed by secure storage of private keys.

In fact, if cybersecurity protection is provided at all in embedded devices today, it is most often bolted on to the product design at the end of a development project, an approach which undermines its ability to provide security over the lifetime of the product, as mandated by the CRA.

The drafting of the CRA rightly recognizes that cybersecurity protection is not a one-time-only event: new vulnerabilities in hardware and software are continually uncovered, and new threats and methods of cyber attack continually emerge. This means that every connected embedded device's protection requires a means of monitoring exposure to emergent threats, and of updating the device's security software to close any new loopholes.

Why is this provision of lifetime security a difficult feat for embedded device manufacturers to master?

Under the CRA, the device manufacturer must monitor common vulnerabilities and exposures notices for any risk to its product, notify the authorities when an exposure is identified, and promptly deploy an update either over-the-air (OTA) or locally to protect the device against the known risk.

To do so, the manufacturer requires a comprehensive and accurate manifest of all the software and hardware components in its product. In any single smart embedded device, there can be thousands of software components in its Linux operating system alone. There can be hundreds or thousands more in other firmware and application software derived – like the Linux OS – from free and open-source software (FOSS).

It is in the nature of FOSS, which can be freely used and modified by users, to branch and multiply into numerous variations. This applies to the Linux OS more than to any other software component. The result is that every embedded product on the market has its own unique 'recipe' of Linux and other software components.

It is a complex enough task to keep a record of this SBOM for a single product when it leaves the factory. But the problem has two other dimensions which makes the task of maintaining an SBOM still more complex: time and breadth.

- Over time after a product leaves the factory, the SBOM of a production unit changes as software updates are applied, either to improve functionality or performance, or to apply protection against a new security threat. So, the creation of an SBOM for a production unit is not a one-time-only event.
- Over the breadth of a product family, different variants have a different SBOM. For almost every embedded product design, the manufacturer will develop multiple variants that have small but important differences. These variants are produced to meet the needs of the markets in different countries, to meet different regulatory requirements, to respond to different customer segments and to address different price points. Each variant of the product requires its own SBOM. For a typical embedded device design, the number of variants in production is often more than 10 and can be over 100.

Deepening the problem: culture, know-how and resources

The difficulty of maintaining an accurate SBOM for every production unit in the field is just one aspect of the lifetime cybersecurity process, but it illustrates the complexity inherent to the task.

The difficulty in implementing cybersecurity protections in new product designs is compounded because it is not a core competence for many embedded device manufacturers. The makers of baby monitors and toys are experts in the design and production of products that perform the functions of monitoring sleeping babies or entertaining children. This is the source of their competitive advantage.

There is no competitive edge to be gained from recruiting, retaining and rewarding cybersecurity experts, who are in any case extremely scarce and expensive. So, the know-how does not exist inside device manufacturers to implement all the hardware and software capabilities required for cybersecurity protection.

And perhaps as a consequence, the culture of the embedded device industry does not put cybersecurity at the forefront of the product marketing process. Rather, priority is given to features and functions that the customer will pay for, and to getting the product to market as early as possible.

Cybersecurity protection is today seen as an impediment to this, and so security design is starved of resources such as time, staff and money.

The platform model: a proven way to implement Linux-based cybersecurity

This problem – of chaotic complexity hindering an explicit need to secure devices on production and subsequently in the field – plagued a different electronics market segment in the late 2000s: the smartphone industry.

Mobile phone manufacturers had deep expertise in the core functions of a phone, such as RF communication and low-power circuit design. This was because, at that time, connecting voice calls and delivering SMS texts was a crucial source of value to customers, as was extending battery run-time between charges.

On the other hand, the operating system provided no differentiation at all – and so smartphone manufacturers did not invest sufficiently to build in-house expertise in Linux software engineering capability. Various phone manufacturers suffered varying degrees of frustration and failure in their efforts to build expensive and clunky proprietary operating systems before the solution emerged: the Android™ Linux-based platform, providing smartphone makers with a universal operating system, built, secured and maintained on their behalf.

The provision of this horizontal platform freed smartphone makers to focus on the real sources of value in their products. It was only after the broad adoption of the Android system that the wider smartphone market flourished, thanks to phone makers' innovations in features such as the camera, touchscreen interface, multimedia support and more.

A platform like Android for embedded devices

The solution to the chaotic complexity of building security features into Linux-based embedded devices may follow the same pattern as the smartphone market has enjoyed. A standard Linux platform – built, secured and maintained on behalf of embedded device manufacturers – could help achieve compliance with the CRA.

It will also free embedded device manufacturers to focus their engineering effort on the real sources of value that their customers care about. The Linux operating system is not one of these sources of value.

FoundriesFactory: the Linux platform for a more secure embedded world

The FoundriesFactory™ software from Foundries.io eliminates the need for an OEM to create and manage their own Linux distribution and DevSecOps platform. The FoundriesFactory™ platform is ready-made, designed with security in mind, continuously updated and maintained, all within a cost-effective subscription service.

The FoundriesFactory™ software-as-a-service (SaaS) product abstracts a security layer – supplied and maintained by Foundries.io – from the application layer developed by the device manufacturer. This security layer is provided as part of the Foundries.io Linux microPlatform (LmP) operating system. The LmP is configurable to help meet each customer's needs using tools in the FoundriesFactory platform. The LmP platform itself is maintained and updated by Foundries.io.

The FoundriesFactory™ service also includes a full suite of comprehensive cybersecurity features, including:

- Secure boot anchored by a root-of-trust
- Installation and encrypted storage of keys and certificates. This provides for access to third-party cloud services
- Encrypted artifact installation and device onboarding
- Automatic generation of an SBOM for every production unit, updated to include every update. This helps to ensure compliance with licensing requirements, as well as enabling auditing of exposure to known exploits
- An update platform meeting the open TUF specification for secure updates and a process for off-line or OTA updates of all software (including firmware, kernel and applications)
- Security for maintenance and support activities such as remote access for service engineers

By basing the development of new products on the FoundriesFactory platform, device manufacturers can build cybersecurity protections into the product from the start of its development, avoiding the time and financial penalties involved in trying to bolt on security to a complete or near-complete product design – an approach which in any case gives rise to substantial risk of subsequent exposure to security threats.

The use of the FoundriesFactory platform also frees device manufacturers from the stranglehold that the Linux operating system has on them. Today, engineering teams are entangled in the chaotic process of documenting, maintaining and updating tens or hundreds of variants of the Linux operating system and other FOSS products.

By subscribing to the FoundriesFactory platform, manufacturers replace the chaos of multiple in-house Linux implementations, typically with few security features, with a tailored LmP that is maintained and updated by Foundries.io. The FoundriesFactory platform also provides a full DevSecOps workflow for developing, testing, deploying and maintaining Linux-based embedded devices.

The FoundriesFactory software is thus a solution to the twin crises facing makers of connected embedded devices today: the chaos of the Linux and FOSS environment, and the impending imposition of cybersecurity regulations including the EU's CRA.

For more information about the FoundriesFactory SaaS and LmP, go to www.foundries.io.

References

[1] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[2] **European Commission, Cyber Resilience Act fact sheet**
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

[3] **European Commission, questions and answers about the CRA**
https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375