Ensuring proportionate application of the EU Cyber Resilience Act to Semiconductor Manufacturing Equipment

A SEMI SMCC Position Paper

CONTENTS

Representation and Scope

This position paper reflects the perspectives of participants in the SEMI Semiconductor Manufacturing Cybersecurity Consortium (SMCC) and primarily represents the viewpoints of semiconductor equipment and tool manufacturers which is an essential and highly specialized segment of the semiconductor supply chain responsible for enabling advanced chip production.

While SEMI represents a broad cross-section of companies across the electronics ecosystem, this paper is not intended to reflect the views of the full SEMI membership, but rather to capture the specific operational, technical, and lifecycle considerations of the semiconductor manufacturing equipment (SemiEq) sector in the context of the EU Cyber Resilience Act (CRA). Within SEMI, SMCC provides a platform for member companies to collaborate on cybersecurity challenges and policy engagement affecting semiconductor manufacturing environments.

Executive summary

Semiconductor manufacturing equipment (SemiEq) stands apart when it comes to the Cyber Resilience Act (CRA), so it must be looked at in its own context. SemiEq is not available on the EU market via regular consumer stores, is tailored for specific ecosystems or industries, and operates only in highly segmented, access-controlled fab environments.

Applying the CRA's horizontal requirements without sector specific adaptation would impose disproportionate burdens, disrupt multiyear supply chains, and potentially hinder Europe's technological ambitions, that rely on the availability of advanced semiconductor chips produced in the EU. SemiEq suppliers and chipmakers often finalize system architectures and commercial agreements years before SemiEq's introduction to the market, meaning that equipment scheduled for delivery after 2027 may have been planned and agreed upon well before the CRA existed.

SEMI urges the European Commission to provide further clarifications needed for effective CRA implementation.

1. The unique nature of semiconductor manufacturing equipment

SemiEq is never placed on the EU Market for consumers or industrial users outside the semiconductor device manufacturing sector. The CRA applies to products with digital elements "made available on the market" in the course of commercial activities. SemiEq is sold mainly through long term industrial agreements between parties, and is not distributed through storefronts, websites, or consumer channels.

SemiEq is engineered to order. Equipment development commonly spans two to ten years, requiring co-development, validation and recipe integration that cannot be altered without jeopardizing performance uniformity. Even minor software or firmware changes can cause significant requalification costs and production delays. In high volume manufacturing, requalification of a single subsystem may require thousands of engineering hours and may introduce the risk of months of delay.

2. CRA provisions that disproportionately affect SemiEq

Both Recital 64 and Annex I, Part I, point 2(b) recognize a limitation to the default requirements of the Regulation for tailor-made products with digital elements supplied for a particular purpose to a particular business user. They indicate that, for such tailor-made products, the manufacturer and the business user may explicitly agree to different contractual terms in relation to secure-by-default configuration and related obligations.

Providing contractual flexibility for semiconductor manufacturers (and similar industries) to deliver products with different contractual terms in relation to secure-by-default configuration and related obligations at a customer's explicit request is justified, as it enables necessary industry-specific customization. The informed customers are the best positioned to manage the risks in their operational context.

At present, however, important questions remain regarding the scope and limits of that exception. Greater legal clarity would be valuable, especially on:

- What qualifies as a tailor-made product with digital elements;
- What level of customization is required;

- How explicit the contractual agreement must be;
- Which requirements may be varied by a contract, and which remain mandatory;
- How should market surveillance authorities assess compliance in such cases?

Article 13 requires vulnerability handling for at least five years or longer when products remain in use, yet semiconductor manufacturing equipment typically operates for fifteen to thirty years, and consistency and continuity for capacity purchases is important within this lifetime. Suppliers cannot realistically redesign legacy platforms, embedded controllers or obsolete operating systems within the CRA's three-year grace period. Vulnerability remediation is further complicated by the semiconductor supply chain, where each tool integrates numerous proprietary modules from multiple specialized vendors. Coordinated fixes require cross-tier engineering, full integration testing, and fab-level validation to avoid process instability or yield loss. This multi-layer dependency makes rapid remediation timelines unworkable and underlines the need for a proportionate, sector-specific approach for SemiEq.

Product cybersecurity is inherently time-dependent: a system that meets state-of-the-art security requirements at the time of placing on the market will inevitably degrade in resilience as threats evolve and component-level support and updates are discontinued, even while the overall product remains within its intended support period. This creates a structural mismatch between long product lifecycles and shorter security lifecycles, challenging the assumption that compliance at market entry ensures sustained security over time.

Article 32 requires module level conformity assessment when components are placed on the market separately. SemiEq modules cannot function independently and are designed exclusively for integration into a host platform within a controlled fab environment. Treating each module as a standalone CRA regulated product contradicts longstanding Machinery Regulation practice where partly completed machinery is not CE marked individually, especially in the semiconductor machinery case where the supplier of the module is the machinery OEM. Additionally, typically, these modules are not intended to be installed by the customer and are intended to be evaluated at the integrated system level.

3. Supply chain and competitiveness impact

The inertia in SemiEq design is exceptionally high. Technical and commercial terms for equipment introduced after 2027 were agreed to well before the CRA was known. Redesigning platforms at late stages would require requalifying entire production lines. For leading edge fabs, a single quarter of delay in ramping a new device-technology node can represent losses in the billions of euros across the downstream semiconductor ecosystem. In addition, implementing certain CRA provisions can lead to loss in production time. As an approximate measure, every second a production line is idle; 50 euros is lost. The production line must be stopped for certain security updates, and there is also the risk of unscheduled downtime associated with applying updates. For this reason, customers are reluctant to change being introduced in their products.

Qualification and change control requirements are uniquely stringent. High end SemiEq models must maintain near identical performance across units. In certain cases, the tolerance for variation is even tighter since the SemiEq pushes the boundaries of what is technically possible. Deviations caused by CRA driven redesigns would introduce unacceptable variability. Unlike consumer devices, a small software change can require extensive particle monitoring, recipe recalibration, and/or safety recertification.

The workforce and supplier capacity constraints further compound these issues. Recital 23 of the CRA confirms that the EU cybersecurity skills gap is already acute. Imposing immediate CRA redesign

obligations on SemiEq suppliers and sub suppliers would overburden an already stretched engineering pipeline.

The CRA may accelerate the end of life of critical components on the EU market, as increased compliance and lifecycle obligations render certain products economically unviable to maintain. This would lead to the reduction of the availability of essential semiconductor components, with potential detrimental impact on supply chains and long-lifecycle industrial systems.

4. Additional clarifications needed for effective CRA implementation and recommendations to the European Commission

SEMI respectfully requests the following actions:

1. Provide further clarification on the interpretation and application of Recital 64 and Annex I, Part I, point 2(b) of the CRA in relation to tailor-made products with digital elements. Given the interpretative nature of this matter, guidance would be a highly effective way to promote a consistent and harmonized understanding across Member States, while providing legal certainty to both manufacturers and business users.
2. SemiEq suppliers will require a significantly longer period to implement any harmonized standards once they are published, well before the CRA becomes mandatory. Given that none of the standards currently under the Commission's request for standardization address the specific characteristics of semiconductor products, at least eighteen months of implementation time is essential for this sector after the publication of the horizontal standards for CRA. SEMI therefore requests an extension of the 11 December 2027 compliance deadline, as the absence of semiconductor-relevant harmonized standards and the limited time available to adopt general-purpose standards create substantial uncertainty regarding what compliance would entail for our industry.
3. Provide a transitional exemption for all SemiEq systems and modules whose contractual commitments predate December 2024, as these were developed without knowledge of CRA requirements.
4. Align SemiEq module treatment with Machinery Regulation principles, so modules are not required to undergo standalone CRA conformity assessment, CE marking or vulnerability handling procedures.
5. SEMI requests clarity on how the CRA's spare parts exemption applies to semiconductor equipment. Article 2(6) and Recital 29 provide an exemption for spare parts manufactured according to the same specifications, yet many SemiEq spare parts originate from longstanding designs essential to fab stability. To avoid unintended downtime or redesign of legacy parts, the Commission should clarify what is meant by an "identical" spare part and confirm that SemiEq spare parts qualify for this exemption when they maintain compatibility and do not introduce new cybersecurity exposure in the fab environment.
6. SEMI also requests clarification on the definition of substantial modification. The CRA states that substantial modifications are those that affect compliance or change the intended purpose. The expectation to perform a comprehensive cybersecurity risk assessment is often unrealistic, as the necessary design knowledge and context typically resides with the original development team and may no longer be fully accessible, especially with expected lifetimes of products of more than 15 years. This results in higher costs, uncertain outcomes, and a structural question of how such obligations are intended to be fulfilled in practice.

Conclusion

The semiconductor supply chain is essential to the EU's strategic autonomy, innovation capacity, and competitiveness. A proportionate, sector-specific interpretation of the Cyber Resilience Act is necessary to avoid unnecessary redesigns, production risks and supply chain delays while maintaining robust cybersecurity. SEMI and its members stand ready to collaborate with the Commission, ENISA, and market surveillance authorities to implement an approach that achieves both resilience and industrial continuity. Specific interpretation of the Cyber Resilience Act is necessary to avoid unnecessary redesigns, production risks, and supply chain delays while maintaining robust cybersecurity.

Note: All references in the document are to the Cyber Resilience Act text that can be found via this link on the official journal of the European Union (OJEU):

https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

About SEMI

SEMI® is the global industry association connecting over 3,500 member companies and 1.5 million professionals worldwide across the semiconductor and electronics design and manufacturing supply chain. We accelerate member collaboration on solutions to top industry challenges through Advocacy, Workforce Development, Sustainability, Supply Chain Management and other programs. Our SEMICON® expositions and events, technology communities, standards and market intelligence help advance our members' business growth and innovations in design, devices, equipment, materials, services and software, enabling smarter, faster, more secure electronics. Visit www.semi.org, contact a regional office, and connect with SEMI on LinkedIn and X to learn more.

About SMCC

The Semiconductor Manufacturing Cybersecurity Consortium (SMCC) is a SEMI technology community founded in 2024 to develop and promote a standard based, semiconductor industry wide approach to improve cybersecurity and accelerate implementation of actionable solutions. The vision of SMCC is to strengthen cyber resilience and protection of the global semiconductor supply chain against evolving threats. SMCC's reach extends all over the world and enables our members to connect and collaborate on specific cybersecurity issues and challenges affecting different regions. It focuses on important key topics and seeks to find solutions that will benefit the entire industry.


semi™