PROEKSPERT

BLH NOBEL
A VPG Brand

BLH Nobel: CRA readiness for legacy industrial devices

BLH Nobel partnered with Proekspert to remove Cyber Resilience Act compliance risk from a long-lived industrial device – gaining clear, audit-ready guidance and confirming that no hardware redesign was required.

Client

BLH Nobel is a global provider of precision weighing and force measurement solutions, serving demanding industrial applications such as cranes, mining, and process industries. Part of Vishay Precision Group (NYSE: VPG), BLH Nobel combines decades of American and Swedish engineering expertise to deliver accurate, reliable systems used by customers in more than 100 countries. Known for robustness and long service life, BLH Nobel's products operate in mission-critical environments where reliability and compliance are essential.

Technologies

C#, Embedded Windows, threat modeling, static code analysis, SBOM

Case study

From CRA uncertainty to audit-ready compliance – without disrupting the product

The challenge: Understanding CRA impact on a long-lived industrial device

BLH Nobel, a global provider of industrial weighing and force measurement solutions, faced a growing regulatory challenge. One of their longstanding embedded devices – used in demanding environments such as cranes, mining, and factories – was developed before the upcoming EU Cyber Resilience Act (CRA).

With CRA requirements approaching, BLH Nobel needed to understand the gap between their existing product and future compliance expectations – and whether compliance would require disruptive redevelopment. The device is typically configured once and then operates for years in restricted or physically protected locations, yet in some use cases remote connectivity is essential, introducing new security considerations.

Their goal was not immediate redevelopment, but a clear, realistic assessment:

- What does CRA actually require for this type of product?
- Where are the real security risks – and which are theoretical?
- How much change is truly needed to remain compliant and competitive on the EU market?

Our role: Turning CRA requirements into practical, device-level certainty

BLH Nobel engaged Proekspert to perform an initial CRA compliance analysis and risk assessment for their embedded industrial device.

Our task was to translate abstract regulatory requirements into concrete, actionable decisions – without forcing unnecessary hardware redesign – and to create documentation that enables the design of solutions based on modern security architecture and supports audits and certification reviews.

What we did:

- Conducted a product risk assessment across different environments and applications, focusing on real-world usage, connectivity, and operational context
- Mapped EU CRA essential security requirements to the actual product architecture and lifecycle of an embedded industrial device
- Reviewed the embedded software implementation (C#, Embedded Windows), supported by threat modeling and static analysis, to validate security risks and mitigation priorities
- Identified typical embedded security pitfalls and defined processes to ensure they cannot reach production
- Delivered clear mitigation recommendations covering both software changes and development processes
- Built embedded-appropriate technical documentation, including a lightweight SBOM and an architecture overview, where no off-the-shelf tooling was available
- Provided guidance on improving documentation and release practices to support long-term CRA compliance and audit readiness

All findings and recommendations were delivered in a structured, audit-ready report that BLH Nobel can directly use for planning, budgeting, and certification decision-making.

The outcome: CRA readiness without unnecessary redesign

As a result of the assessment, BLH Nobel gained a concrete, device-specific understanding of where their product stands in relation to CRA requirements and what truly needs to change.

Most importantly, the analysis confirmed that no hardware redesign was required. CRA and CE-marking alignment can be achieved purely through targeted software upgrades, supported by improved security processes and documentation.

The assessment provided BLH Nobel with a clear view of which security risks matter in real operating conditions, along with practical guidance on securing remote access use cases. It also defined well-structured development and release processes that prevent security gaps from reaching production, while establishing a solid foundation for embedding CRA and security-by-design thinking into future product generations.

In addition, the work delivered valuable input for next-generation product development, enabling compliance and security considerations to be addressed early rather than retrofitted later.

Impact for the client's organization

BLH Nobel's CRA readiness work delivers direct business-critical value

- **Protected revenue and market access:** Clear, documented understanding of CRA obligations reduces regulatory risk and supports continued sales in regulated EU markets
- **Cost avoidance:** Confirming that no hardware redesign is required avoids unnecessary redevelopment, delays, and certification risk
- **Future-proof development:** Reusable compliance analysis, processes, and documentation reduce effort, risk, and cost for future product generations