SECURITY INSIGHTS

Security Can No Longer Be an Afterthought in Automation Industry

Hardware-based cryptography for industrial systems

Industrial products face stricter security requirements than before. Here’s what’s driving these changes

The Cyber Resilience Act sets a clear timeline:

Vulnerability reporting obligations apply
from 2026

Most product requirements apply
from 2027

If you sell connected products in the EU, you must:

- Design security into the product right from the start
- Take responsibility for compliance throughout the entire product life cycle
- Detect, report and remedy security gaps

These are legal requirements, not recommendations.

The average cost of a cyber breach in industrial sector is ~$5M

Source: Verizon

Industrial products are expected to last 10-20 years

During that time, both the operating environment and the threat landscape will evolve

National entities, such as National Institute of Standards and Technology (NIST), are standardising post-quantum cryptography, to complement and in time replace current public-key methods.

Industrial systems are no longer isolated

Typical systems include:

- Network-connected devices
- Communication between components and subsystems
- Integration with other machines and control systems

Each interface increases the attack surface.

This is structural change compared to earlier, closed systems.

Real-time performance sets strict limits

Industrial systems often operate in millisecond cycles

Timing must remain predictable

Security mechanisms that introduce latency or variability can affect system behaviour, and this limits the types of protection that can be used.

Nearly 60% of cyber threats in manufacturing are linked to cyber-crime, which also causes the most significant operational disruptions

Source: Verizon

These requirements must be handled together

Security must:

- meet regulatory requirements
- work over long lifecycles
- handle increasing connectivity

without affecting system timing

Many implementations fail at system level

Security is often added late and handled in software:

This leads to performance overhead, complex updates and inconsistent protection.

Instead:

- Design security in from the start
- Implement critical security functions in hardware
- Ensure predictable system behaviour

Security must be built into the architecture right from the start

You need to define early on:

- Your threat model
- The security architecture
- Which components implement cryptographic operations
- How cryptographic keys are managed

This leads to architectural choices:

- Moving critical cryptographic functions into hardware
- Reducing reliance on the main CPU for security functions
- Ensuring predictable system behavior

Manufacturing is one of the most targeted industries, with over 1,600 confirmed breaches, alongside healthcare (1,542) and finance (927)

Source: Verizon

Hardware-based cryptography secures automation industry

- Keeps system timing predictable
- Separates foundational security from application logic
- Reduces exposure to vulnerabilities

How are you addressing these requirements in your products?

Hardware-based security solutions

www.xiphera.com