



Product design security assessment

The problem

Many cyber-physical systems, such as vehicle control units or industrial controllers, are extremely difficult, if not impossible, to protect effectively against cyberattacks using bolt-on security measures if their built-in security mechanisms prove inadequate. Security requirements for such systems must be established at the design stage and incorporated into their architecture, and these requirements must be kept in mind when selecting engineering components and their suppliers at the earliest stages of development.

The solution

A comprehensive security assessment of a cyber-physical product's architecture and its low-level engineering components, including chips and communication protocols, as well as prioritized recommendations for built-in protection mechanisms needed to minimize the risk of successful attacks throughout the product lifecycle.

Target audience

Vendors of products for ICS, the internet of things (IoT), transport and transport infrastructure automation; OEMs and developers of engineering solutions for various industries, such as manufacturing, transport (including rail, river, sea, and air), medical systems, communication systems, etc.

The security challenges

As with any product functions, information security mechanisms can be implemented with flaws or not implemented at all. In cyber-physical systems, this poses risks to the real physical world: loss of control over equipment, vehicles, physical access to facilities, etc.

Research into the security issues of cyber-physical systems, including industrial automation systems, IoT and industrial internet of things (IIoT) solutions, automotive technology, avionics, etc., conducted by Kaspersky ICS CERT experts, shows that the most significant and difficult-to-remedy vulnerabilities are most often caused by poor architectural decisions and sub-optimal selection of engineering components.

It is often difficult to fix architectural and implementation defects without making profound changes to the product.

Vulnerabilities in the engineering components of mass-market commercial products often serve as entry points into systems. Compromising such components in a cyber-physical system essentially means compromising the

trusted environment for controlling a physical object (e.g., a manufacturing facility or a vehicle).

The security of the final solution is most frequently and severely affected by security issues in the following types of engineering components:

- Open-source software components;
- Various software and hardware modules from third-party suppliers (for example, [LTE/5G modems](#), [SoC](#) and other chips, their firmware and microcode);
- Standard protocol stacks used in new contexts (e.g., wireless protocols);
- Specialized low-level data transmission protocols ([industrial](#) and transport buses);
- [Development environments](#) and runtime environments for automated industrial process control programs (articles [1](#), [2](#), [3](#));
- Protocol stacks and interfaces connecting controllers, cryptographic modules, sensors, and actuators;
- Telemetry modules, modems, and gateways providing remote access;
- Service and diagnostic software, update mechanisms, and remote configuration tools.

Even when using only proprietary code without external libraries, expert assessment of architecture, algorithms, and protocols remains critically important. The most common flaw is a monolithic architecture without clear decomposition into components and security domains, and without control of communications between them. If there is a vulnerability, for example, remote code execution, in one of the system's functional components, this may lead to complete compromise of the product's functions. Other errors also occur — for example, a [custom implementation of cryptographic traffic protection algorithms in industrial controllers](#) is incapable of protecting not only the data but also the key used to encrypt it.

Furthermore, in the world of cyber-physical systems, the development of even the most modern products often requires integration with legacy technologies for compatibility or to implement interfaces for interacting with existing systems. Security threats associated with vulnerabilities in legacy technologies can, at the very least, be partially neutralized through correctly selecting secure architectural solutions.

Figures and facts

Kaspersky ICS CERT experts have identified more than 400 zero-day vulnerabilities in industrial systems, IIoT/IoT systems, and other types of solutions.

What we offer

Product design security assessment is a comprehensive consulting project. As part of this project, we help design or refine the architecture of a cyber-physical product to ensure that it reliably withstands existing and potential future threats, while remaining aligned with business goals, regulatory requirements, and operational constraints.

We are guided by the principle that security efforts should primarily focus on threat prevention rather than mitigating threats that have already been realized. This approach optimizes resource allocation for security and reduces the cost of future error fixes.

For example, sometimes simply changing the user authentication scheme or the separation of roles between components is enough to avoid the need for complex custom cryptography, which carries a high risk of error.

What we do

Define security goals and context

Together with the client, we identify the product's critical functions and assets, its use cases, standard and extreme operating modes, external systems, and users (including maintenance personnel, integrators, partners, and regulators).

Build and update the threat model

Based on the security context and goals, we develop a threat and adversary model for the product, taking into account:

- External and internal attack sources;
- Scenarios of compromise via communication channels, telemetry modules, wireless connections, diagnostic interfaces, and the supply chain;
- Threats associated with third-party components and open-source software;
- Industry-specific characteristics (manufacturing, transport, energy, critical infrastructure, etc.).

Analyze architecture and attack surface

We perform analysis at several levels:

- Functional architecture (core subsystems and their functions);
- Component architecture (software and hardware components, modules, and interfaces);
- Data flow diagrams for key operational scenarios;

- External interfaces and communication protocols (fieldbuses, IP networks, wireless channels, cloud services, and mobile applications);
- Internal inter-component communication protocols (processors, cryptographic modules, controllers, sensors, and actuators).

At this stage, we describe the attack surface, identify potential attack vectors and points through which an attacker could impact product security – both directly and through adjacent systems.

Perform compositional analysis and vulnerability analysis

Based on the architecture described and attack vectors identified in previous stages, we:

- Analyze the components used (libraries, firmware, OS, protocols) using open sources and vulnerability databases;
- Account for supply chain factors (versions, origin, availability of updates and patches);
- Evaluate resilience against unauthorized modification of pre-installed software and tampering with hardware connections (e.g., between the processor and modem, or the processor and cryptographic module);
- Examine vulnerabilities in service and diagnostic software, update procedures and remote access mechanisms.

Assess risks and develop recommendations

For key attack scenarios, we evaluate:

- Potential impact (on business, customers, human safety, and the environment);
- Scenario feasibility (availability of tools, required attacker expertise, difficulty of access);
- Aggregate risk (using industry-applicable methodologies and/or regulatory requirements, such as ISO/IEC 27005:2022 for all industries, IEC 62443-3-2 for industrial systems design, TARA methodology according ISO/SAE 21434:2021 for road vehicles etc.).

Based on the results of these efforts, we develop:

- A set of architectural patterns and countermeasures that eliminate or significantly mitigate key risks;
- Proposals for modifying the architecture, protocols, and policies for communication with external systems, including update and diagnostic procedures;
- Where necessary, alternative solutions for the information security issues identified, detailing their pros and cons, as well as their impact on the cost, development timelines, and product performance characteristics.

We use a systematic approach to threat modeling to identify all potentially dangerous attack scenarios against the product proactively. We provide a detailed breakdown of each type of security breach into specific threats, verifying them against real-world incidents and known attack patterns.

When analyzing threats and assessing the security of an architecture, we consider a wide range of factors that affect the overall security posture:

- How the manufacturer's development lifecycle is organized;
- Whether third-party code is used in the products, and the provenance of that code;
- Whether legacy technologies are used for backward compatibility;
- Network protocols for management and data exchange;
- Requirements for remote access to product functions;
- Interfaces and scenarios for accessing other systems;
- Requirements for specific guarantees with respect to functional safety, reliability, and resilience of the solution;
- Non-functional product requirements, such as resource constraints, performance requirements, and guarantees of properties in real time;
- Technical aspects of access, e.g., for installing security updates or using the solution in hard-to-reach areas;
- Use of the product in industrial facilities where the cost of downtime is high, etc.

Based on this in-depth analysis, we develop recommendations rooted in industry best practices. Our goal is to offer more than just minor fixes; we provide architectural solutions that ensure comprehensive enhancements to cybersecurity, stability, functional safety, and overall product reliability.

The service can be used

- At the initial stage of new product development.
- When planning a new release of a product or solution designed to fix deficiencies in previous versions that were prone to vulnerabilities, which is a sign of insecure architecture.
- At any stage when new cybersecurity requirements are imposed on the product (by regulators, partners, or the market), or following industry incidents that raise expectations for the security level.

What the customer gets

Upon completion of the project, the client receives:

- An applied threat model built with the product's specific security goals in mind, describing attack vectors in as much detail as is practically meaningful and possible based on the existing solution description.
- Specific recommendations for improving security architecture, including component structure, interaction methods and interfaces, core technologies, frameworks, and communication protocols.
- Clear requirements for key security components, including methods for verifying and ensuring their integrity and authenticity.

Additionally, we ensure compliance with standards. We help adapt the threat model and recommendations to meet the requirements of specific regulators or industry standards, such as:

- ISO/IEC 27005:2022, IEC 62443-3-2 for industrial systems design.
- TARA methodology according ISO/SAE 21434:2021 for road vehicles.
- Threat mapping on MITRE ATT&CK framework.
- IEC 62443: Security for operational technology in automation and control systems.
- ISO/SAE 21434: Road vehicles — Cybersecurity Engineering.
- UNECE WP.29: UN regulation for vehicle cybersecurity.

Key benefits

1. Reduced financial and reputational risks through identifying and remediating critical vulnerabilities before the product reaches the market.
2. Compliance with industry standards and regulatory requirements through an expert assessment that accounts for the specifics of the client's industry.
3. Optimization of long-term development and maintenance costs, as investment in security during the design phase is many times lower than the cost of subsequent fixes and losses due to incidents.
4. Confidence in the product's resilience against modern cyberattacks, ensured by a robust architecture rather than an often incomplete set of disparate, difficult-to-integrate security features.
5. A detailed roadmap for improvements with actionable recommendations that are easy to integrate into the development process.

We help restructure a product's architecture so that future threats are either impossible or prohibitively expensive for attackers to execute.

Learn more

- [God Mode On: Researchers run Doom on a vehicle's head unit after remotely attacking its modem](#)
- [Cinterion EHS5 3G UMTS/HSPA Module Research](#)
- [The secrets of Schneider Electric's UMAS protocol](#)
- [OPC UA security analysis](#)
- [ISaPWN – research on the security of ISaGRAF Runtime](#)
- [Security research: CODESYS Runtime, a PLC control framework. Part 1](#)
- [Security research: CODESYS Runtime, a PLC control framework. Part 2](#)
- [Security research: CODESYS Runtime, a PLC control framework. Part 3](#)
- [Cryptographic deadly sins and the security of Modicon M100/M200/M221](#)

Related services

- ICS vulnerability data feed
- Analysis of known ICS vulnerabilities for critical information security decision-making
- ICS vulnerability and threat intelligence
- Incident response at industrial enterprises

[**Request a consultation**](#)

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT)

is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com