ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Ensuring a Secure Future for Robotics: The Role of Cybersecurity

Manoj Rajashekaraiah, Principal Engineer

Abstract

This article explores security risks and effective security measures in robotic control systems. It covers industrial security standards and analyzes the essential requirements to meet these standards.

Introduction

Factory automation is at the center of Industry 4.0 and industrial robots, autonomous mobile robots (AMR), and collaborative robots play a crucial role in enabling the implementation of modern Industry 4.0. Robots are becoming smarter, more collaborative, and better positioned to handle complex tasks with and without human intervention. Higher levels of automation and higher use of robots also drive the demand for higher safety and security of robotic control systems. Robots were initially mostly used on factory floors but now robots are used in different domains like medical, military, logistics, and agriculture. The need for safety and security is of much more importance than a decade back. Accidents are bound to occur, but the ones caused by malicious attacks are critical. Malicious hijacking and control of robots can cause serious economic and financial losses.

Security Risks in Robotic Control Systems

Figure 1 shows typical security risks that can lead to malicious attacks on robotic control systems.[1]

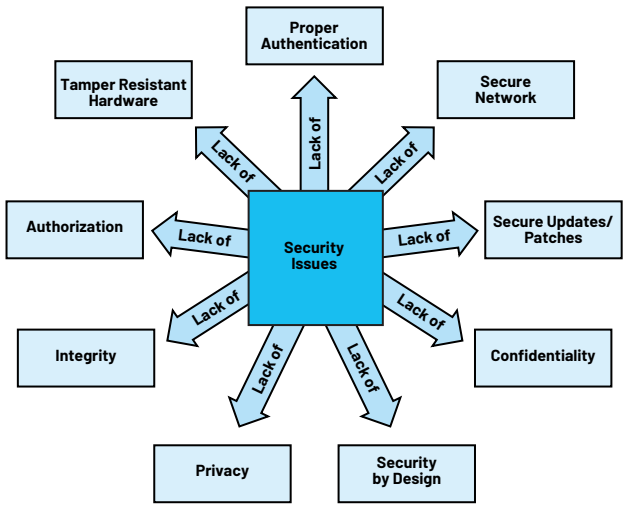

Figure 1. Security risks in robotic control systems.

An overview of some of the concerns can be found in Table 1.

Table 1. Security Risk Concerns

Lack of	Impact and Description
Secure networking	Renders the communication between robotic control systems insecure and prone to spoofing, tampering, and eavesdropping. It may impact the availability of the system as well.
Proper authentication	▶ This leads to unauthorized access using default usernames and passwords. ▶ Lack of device or peripheral authentication may lead to the use of counterfeit peripherals/accessories in robotic systems presenting safety or security risks. ▶ Also leads to accepting data inputs from untrusted, nonidentified sources.
Confidentiality	Lack of encryption or weak encryption algorithms leads to the interception and exposure of robotic sensitive data and design plans.
Integrity	This can lead to the alteration of robotic sensitive data, configuration, and firmware either stored or in transit.
Secure boot and update	▶ Without this, we are unsure if authentic firmware/software is running on our robotic control system. ▶ Lack of secure updates could potentially enable hacking into robotic control systems by doing either rollback to vulnerable older software or by programming nonauthentic software into robotic control systems.
Tamper-resistant hardware	Sometimes robots store extremely sensitive information (for example, robots used in military/defense). It is very crucial to protect this information from access to unintended actors. Without tamper-resistant hardware, it becomes difficult to protect information against invasive attacks.
Secure by design	Most control system developments until recently did not adopt the principle of secure by design approach. This leads to breaking into the robotic system's architecture and design to scan and exploit its vulnerability for launching an attack.
Updates	Lack of updates for the robotic operating system, firmware, and software may result in cyberphysical attacks.

Note: Significant proportion of security risks do come from software vulnerabilities.

Regulations and Acts for Industrial and Robotics Sectors Promote Cyber Resilience and Safeguarding Operations

The cybersecurity landscape is rapidly evolving, and there are a growing number of regulations as well as acts that target the industrial and robotics sector. Among the many, some of the acts that target cybersecurity are EU Cybersecurity Act, EU Cyber Resilience Act, and U.S. Cyber Incident Reporting for Critical Infrastructures Act. There are regulations and acts evolving in China and India as well. The NIST Guide to Operation Technology (OT) Security and standards like IEC 62443 provide us guidance, enable us to take the secure-by-design approach and design, and develop our control systems to be resilient against cybersecurity attacks.

IEC 62443 Requirements for Industrial Automation and Control Systems Security (IACS)

IEC 62443 is security for IACS.[2] It is a widely adopted standard for developing industrial automation control systems, and most regulations recommend it and recognize its importance. It enables us to be compliant with relevant regulations, mitigate potential cybersecurity risks in control systems, address security gaps in control systems, protect critical assets, and many others.

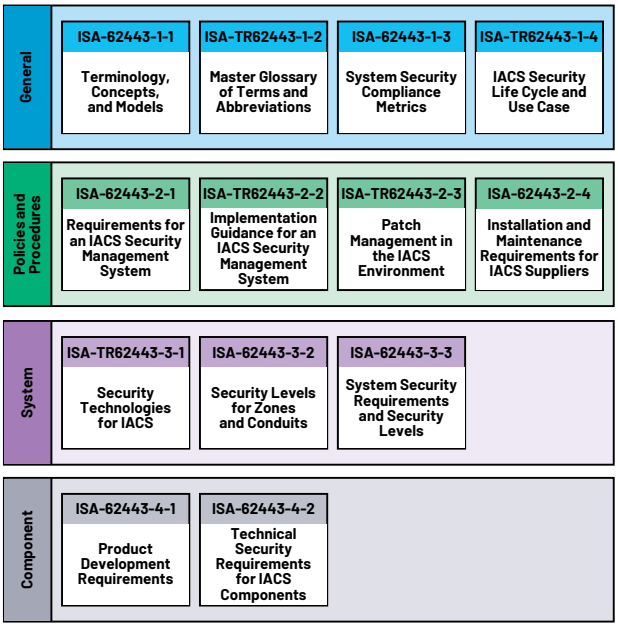

Figure 2. The IEC 62443 is a comprehensive security standard.

While some parts of the standard focus on processes and procedures, IEC 62443-4-1 and IEC 62443-4-2 specifically address component security. According to IEC 62443-4-2, component types include software applications, host devices, embedded devices, and network devices. The standard defines the capability security level (SL) for each component type based on the component requirement (CR) and requirement enhancement (RE) they meet. It defines four security levels (SL) SL0 to SL3. The SL2 and SL3 levels specifically require hardware-based security.

What Capabilities and Technologies Are Necessary When Developing Robotic Security System Solutions?

To build secure robotic control systems, we need to address the risks highlighted in the Security Risks in Robotic Control Systems section. Key technical capabilities and technologies needed include:

- Secure authentication: Integration of secure authenticators to verify device/component identity.
- Secure coprocessors: Utilization of dedicated hardware for secure storage and cryptographic operations.
- Secure communication: Implementation of encrypted protocols for protected data exchange.
- Access control: Enforcement of granular permissions to restrict unauthorized system access.
- Physical security measures: Incorporation of measures to protect against physical tampering.

Turnkey security ICs, such as secure authenticators and coprocessors, are purpose-built to meet these requirements, offering ease of implementation and cost efficiency. These fixed-function ICs are complemented by comprehensive software stacks designed for host processors.[2]

Note: Using a discrete secure element enhances system resilience by preventing a compromised application processor from accessing credentials stored in a separate IC (isolation).

In addition to these aspects, system developers must adopt a structured approach to secure development that encompasses requirements gathering, threat modelling, secure design, implementation, testing, certification, and maintenance. Following a secure development life cycle (SDL) ensures security is built into the development process from the beginning.

What Makes Analog Devices an Ideal Partner for Engaging in Robotic Security System Solutions?

ADI goes beyond being a mere vendor of turnkey security ICs like the MAXQ1065 and DS28S60—we empower customers to fulfill diverse security requirements in the robotics industry. By integrating extensive expertise in security and robotics, ADI emerges as an ideal solution provider capable of tackling the distinctive challenges involved in securing robotic systems. Profoundly acquainted with these domains, we enable customers to construct comprehensive solutions that encompass hardware, software, and system-level considerations.

Recognizing that security in robotic systems requires a comprehensive approach, ADI goes beyond component-level offerings and adopts a system-level perspective. We consider factors such as hardware, software, communication, and integration, ensuring all critical components are seamlessly integrated.

ADI's collaboration with the automotive industry is exemplified by its wireless battery management system (wBMS), showcasing its exceptional capabilities in implementing robust security measures. Through close collaboration with customers, ADI has developed a fully safe and secure ISO 21434-certified wBMS system, underscoring ADI's commitment to delivering comprehensive solutions. Encouraging similar collaborative efforts within the robotics industry would leverage ADI's expertise in security implementation. By partnering closely with stakeholders, ADI can contribute to the development of safe and secure robotics systems, drawing from its experience and success in the automotive sector.

With its extensive capabilities and dedication to security, ADI emerges as the preferred partner for system design, offering unparalleled expertise and support in all cybersecurity-related endeavors.

To learn more:

- Engage with the embedded security community by joining discussions on security-related blogs at EngineerZone™. Search for "security" to find valuable articles and resources dedicated to the topic. Contribute to the ongoing dialogue by sharing insights, asking questions, and participating actively.
- Explore our range of security products and gain valuable insights at Embedded Security and 1-Wire®. Access recent technical articles, application notes, and videos to enhance your understanding of the subject. Stay up to date with the latest advancements in the field and discover more about our security offerings.
- Look at how security takes the spotlight in the ADI wBMS system in the *Analog Dialogue* article "In the New Era of Wireless Battery Management Systems (wBMS), Security Takes the Spotlight."

A Sample Use Case in a Robot Joint Controller

A potential system design of a robotic joint control system within a robotic joint is illustrated in Figure 3.

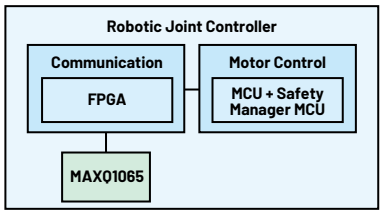

Figure 3. Potential use of the MAXQ1065 in a robotic joint control system.

In this design, the potential application of the MAXQ1065 becomes apparent as it enables the implementation of secure boot functionality, thereby enhancing the overall security of the system. The MAXQ1065 also encompasses an array of additional features, such as secure key storage, secure communication protocols, and cryptographic operations. Subsequent articles will delve deeper into these use cases and explore their practical applications.

Conclusion

In securing the future of robotics, cybersecurity is paramount. Robust measures, such as secure authentication, encrypted communication, and supply chain security are crucial to protect against threats. By prioritizing cybersecurity and leveraging ADI's expertise, we can unlock the full potential of robotics while safeguarding against emerging risks in an interconnected world.

In the next article "Robotic Security Use Cases and Implementation for a Secure Future", we delve further into the intersection of cybersecurity and robotics, showcasing practical implementations of ADI's security products in real-world scenarios.

References

[1] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, and Ali Chehab. "Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations." *International Journal of Information Security*, March 2021.

[2] Christophe Tremlet. "The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks." Analog Devices, Inc., April 2023.

About the Author

Manoj Rajashekaraiah is a principal engineer specializing in software systems design within the Security Business Unit at Analog Devices. With a strong focus on embedded device security, he excels in creating safety, security, and sensor software for automotive and IoT applications. Manoj is a seasoned presenter and blogger with a passion for sharing knowledge, having shared his insights at conferences like IEEE INIS and VDA Automotive SYS. He is a published author on embedded.com and regularly delivers talks at institutes in Karnataka. Manoj holds a master's degree in embedded systems from BITS Pilani, India.