ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

# Robotic Security Use Cases and Implementation for a Secure Future

**Manoj Rajashekaraiah,** Principal Engineer


## Abstract

In our previous article "Ensuring a Secure Future for Robotics: The Role of Cybersecurity", we offered a comprehensive overview of the security challenges faced by robotic control systems. We highlighted the criticality of adhering to industrial security standards in robotics and explored the essential security capabilities necessary to fortify the protection of robotic control systems. Additionally, we provided a preview of how Analog Devices' security products could be utilized to implement a specific robotic security use case. In this article, we will provide an overview of the components that constitute an industrial robot/cobot. It's worth noting that many of these similar components are also commonly used in autonomous mobile robots (AMRs) and pick-and-place systems. Subsequently, we will explore various robotic security use cases, showcasing how ADI's security products simplify the implementation of security in these diverse robotic control systems.


## Building Secure Robotic Control Systems: Essential Technical Capabilities and Development Approach

We are revisiting this section from the previous article for a better understanding of key technical capabilities and technologies required to implement secure robotic control systems, which 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.

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

## An Overview of Components in Industrial Robots and Cobots

Figure 1 shows typical components associated with the operation of industrial robots/cobots. Table 1 gives a quick overview of the different components.

**Table 1. Overview of Components of Industrial Robots/Cobots**

| Component Name | Description |
|---|---|
| Sections | The central physical component, several sections are interconnected using joints and driven by motors. The arm enables precise movements. |
| Joint | Two sections are interconnected using a joint and the joint has a motor and motor controller, which controls the movement of the section connected to it. Sometimes only the motor is kept in the joint and the motor controller itself is outside of the joint in industrial robots. |
| Robot controller | Serves as the central intelligence of the robot, coordinating kinematic movements and actions. It enables communication from the controller to various joints and the end effector. The controller itself connects to the external world using industrial communications protocol like EtherCAT® PROFINET®. |
| End effector | Tooling attached to the robot arm can carry out actions like gripping, welding, cutting, etc. The end effector may have sensors that directly interact with the cloud and there are cases where the end effector directly connects to the robot controller. |
| Programming interface (teach pendant) | Allows operators to teach and configure robot actions. |
| Programmable logic controller (PLC) | Can be used in conjunction with a robot controller to enhance a robotic system's automation and control capabilities. A standalone robotic system might not connect to a PLC. |

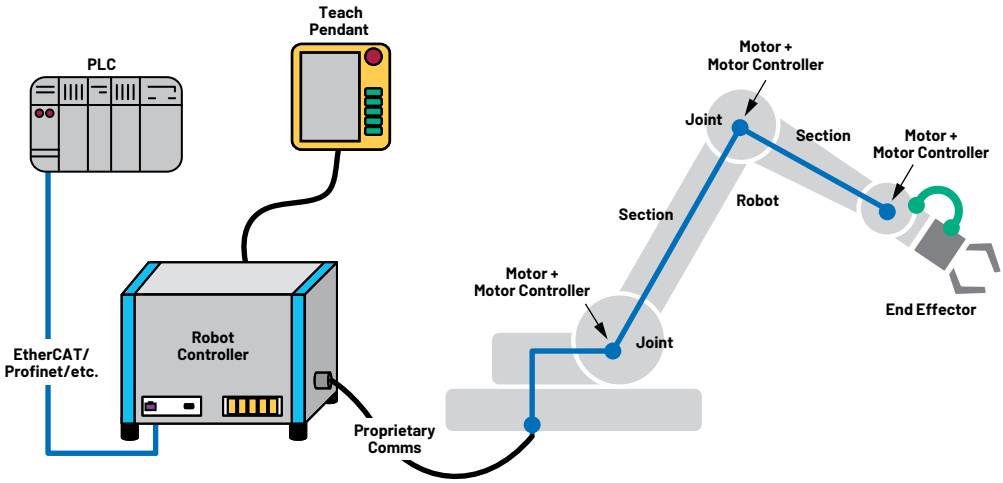


*Figure 1. Components of industrial robots/cobots.*

## Robotic Security Use Cases: Harnessing ADI's Expertise and Products for Design and Implementation

### Trusted PLC Operation and Gateway Protection

The combination of PLCs and robotic controllers offers precise control in factory automation setups, enabling fine-grained control over various processes. In recent years, advancements in robotic technology have led to the development of integrated controllers that possess PLC-like functionality. Ensuring the reliability and security of PLC operation is of utmost importance when it comes to maintaining the safe operation of a factory automation setup. See Figure 2.

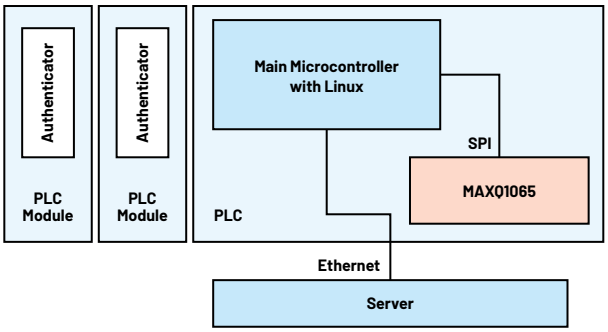


*Figure 2. Enabling security with PLC.*

Usage of devices like the MAXQ1065 (the ultra low power cryptographic controller with ChipDNA® technology for embedded devices) within PLCs can support the following use cases:

NOTE: ChipDNA technology harnesses unique traits of electronic components to generate a secure cryptographic key. This key isn't stored in memory or any fixed state, greatly enhancing protection against cyberattacks.

- Secure identification and clone prevention of the PLC modules.
- Secure boot and firmware download.
- Asymmetric key mutual authentication between PLC modules and PLC servers.
- Establish secure communication session with ECDH key exchange.
- Use of AES for encryption and decryption of network packets.

### Direct Node to Cloud Security

Node-to-cloud communication (see Figure 3) in robotics enables several functionalities such as remote monitoring, data analysis, software updates, etc. It is crucial to secure the communication happening between the node and the cloud.

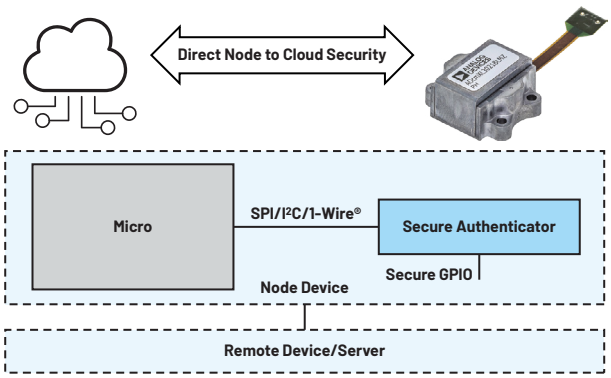


*Figure 3. Integration for the MAXQ1065 to enable the direct node to cloud security.*

The MAXQ1065 offers enhanced security features for sensor-to-cloud and sensor-to-gateway communication:

- Enables the implementation of transport layer security (TLS) protocol, ensuring secure and encrypted data transmission. TLS verifies authenticity and safeguards sensitive information, making it essential for secure communication between nodes and the cloud.
- Facilitates secure communication for proprietary sensor-to-gateway or node-to-gateway connections. The controller helps establish a protected communication channel by enabling key exchange and data encryption, enhancing security for RF-based or other proprietary protocols.
- Offers additional security features like node authentication, trusted node operation, secure boot, and secure firmware updates. These features enhance system security by validating node identity, ensuring trusted operations, and protecting against unauthorized modifications.

## Sensor Data Protection

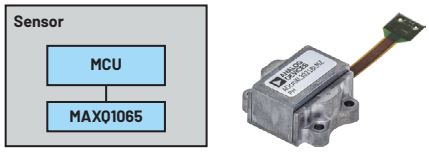


*Figure 4. Sensor data protection.*

- Data at rest can be encrypted with ChipDNA technology.
- Critical calibration data of sensor or sensor configuration information can be stored within the secure storage of the MAXQ1065 to prevent it from tampering or leaking. Further, it can be stored encrypted in the system. See Figure 4.

## Supply Chain Security

Supply chain security includes broad topics. See Figure 5.

- Prevention of product clones (counterfeit).
- Securing software-based feature enablement to prevent IP loss and revenue loss.
- Verification of hardware authenticity. See Figure 6.

Supply chain security can be easily enabled by using ADI's secure authenticators.

- Preprogrammed authenticators from ADI provide robust protection against counterfeiting.
- Secure life cycle management and key management ensure that assets remain secure throughout the device/product's life cycle.
- ADI's authenticators enable secure feature enablement, protecting valuable intellectual property.

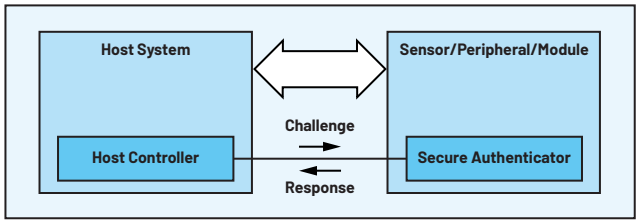


*Figure 5. Testing for authenticity with a challenge-and-response sequence.*

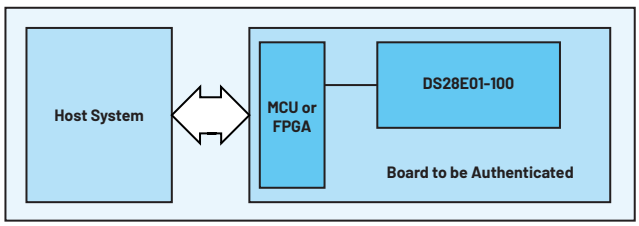


*Figure 6. A hardware authentication example using the DS28E01-100.*

## Secure PLC to Node Communication

Secure authenticators can help secure communication, for example, between PLCs and actuators or sensors and between PLCs and the supervisory control and data acquisition (SCADA) control system (in the PLC, not in the SCADA system). It helps enable TLS protocol, which is a widely used transport layer security protocol in internet protocol-based communications.

## Joint Authentication in Robots

Implementing joint authentication (see Figure 7) in robots significantly enhances overall security by ensuring that only legitimate and authorized entities can interact within the robotic system. It effectively prevents unauthorized access, strengthens communication security, and contributes to the system's overall integrity and reliability.

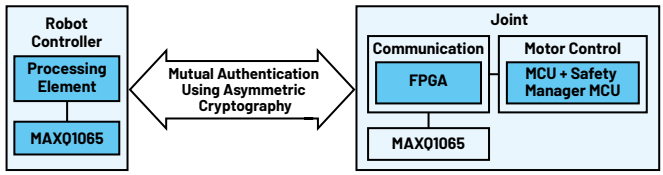


*Figure 7. Joint authentication.*

## Joint Secure Boot

Joint secure boot (see Figure 8) in robots provides a strong foundation for a secure and trusted operating environment. It protects against unauthorized software execution, malware, and tampering, enhancing system security and reliability. By establishing a chain of trust and verifying the integrity of software components, joint secure boot ensures the overall integrity and authenticity of the robotic system's operation. Joint secure updates are also enabled in a similar way.

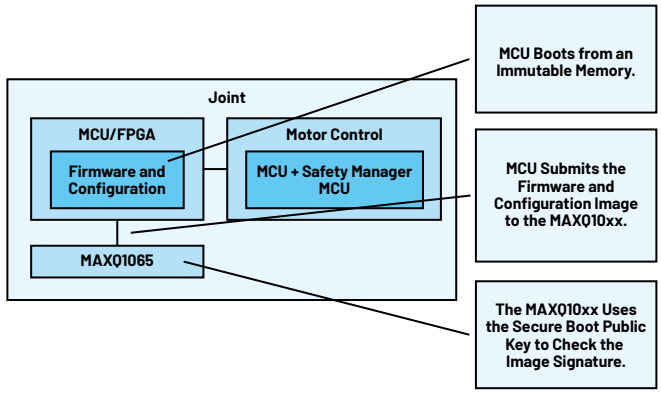


*Figure 8. Joint secure boot.*

## Selective Feature Enablement in Joint and Robot Controller

Post successful secure boot the application microcontroller unit (MCU)/processor/field programmable gate array (FPGA) can read the secure configurable memory of the authenticator/coprocessor to selectively enable the feature in the joint/robot controller. See Figure 9.

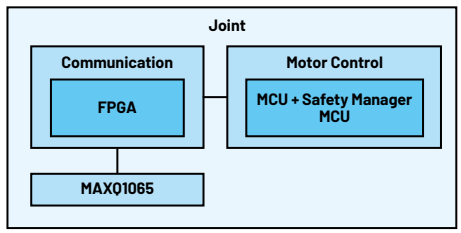


*Figure 9. A typical joint block diagram.*

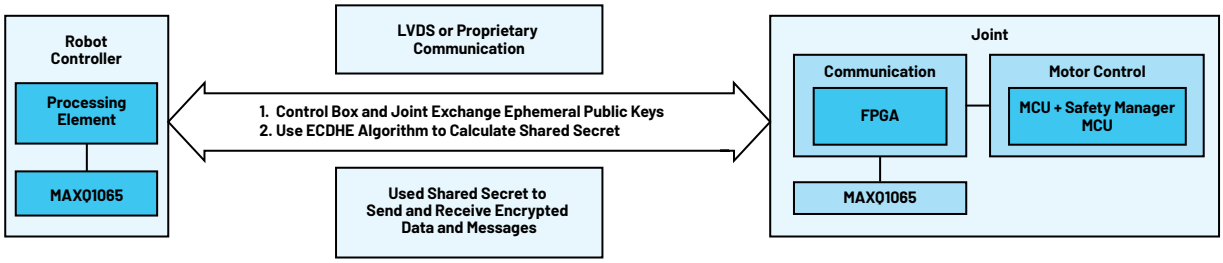


*Figure 10. Joint secure communication.*

### Calibration Data Storage—Joint and Robot Controller

Calibration data storage is critical to maintaining accurate measurements in peripherals that undergo individual calibration at the factory. By securely storing this data within an authenticator, organizations can ensure its integrity and protect it from unauthorized access. The host system can then retrieve and utilize this stored data, enabling more precise and reliable measurements from the peripherals. Secure calibration data storage enhances the overall accuracy and performance of the system, providing valuable insights and maintaining high quality standards.

### Joint Secure Communication

Joint secure communication enhances the overall security posture of a robotic system, ensuring trusted and protected data exchange. See Figure 10.

## 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. ADI's products and solutions provide advanced security features, ensuring the integrity and reliability of robotic systems. 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.

## References

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.

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

"Protect Your R&D Investment with Secure Authentication." Analog Devices, Inc.

"The Basics of Using the DS28S60." Analog Devices, Inc.

## 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.