NEWS FOR THE ELECTRONICS INDUSTRY

eTECH JOURNAL

ISSUE 11

Farnell
AN AVNET COMPANY

ROBOTIC SECURITY

+

THE INVISIBLE WORLD OF NEAR-INFRARED

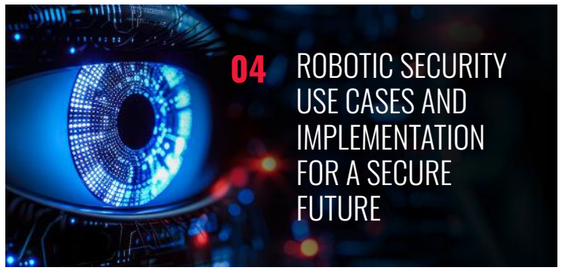
NEW IOT SECURITY STANDARDS

EFFICIENT & ACCURATE DRIVES

X-SEMI MOSFETS: MODERN POWER APPLICATIONS

SECURITY STRENGTHS & TECHNOLOGIES

CONTENTS



To register for all future editions and to access all back issues of eTech Journal, scan QR code

Editor-in-chief: Cliff Ortmeyer, Managing Editor: Ankur Tomar

WELCOME

The security and surveillance industry is transforming significantly as technology evolves rapidly. From autonomous robotic patrols to the potential of near-infrared (NIR) imaging, cutting-edge innovations are redefining how we protect homes, businesses, and public spaces. This progress is driven by the growing need for more intelligent, adaptive, and reliable security solutions that perform seamlessly in diverse environments.

Robotic security systems, for instance, are paving the way for a safer future. These intelligent machines patrol properties, detect anomalies, and respond in real time, offering unmatched precision and scalability. Meanwhile, NIR imaging reveals invisible opportunities, unlocking applications such as advanced facial recognition and environmental monitoring. At the same time, new IoT security standards, built on certified microcontrollers and root-of-trust architectures, are creating more substantial and trustworthy connected systems.

In this edition of the Tech Journal, we explore these advancements with a series of insightful articles. Discover how robotic security is transforming industries, learn about the untapped potential of NIR technology, and navigate the latest IoT security standards to future proof your designs.

We hope you enjoy this edition and welcome your comments and suggestions. Please feel free to drop us a note.

Cliff Ortmeyer Editor, eTech Journal
Email: editor-TJ@element14.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

VISIT ANALOG DEVICES

ROBOTIC SECURITY USE CASES AND IMPLEMENTATION FOR A SECURE FUTURE

Manoj Rajashekaraiah, Principal Engineer

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.

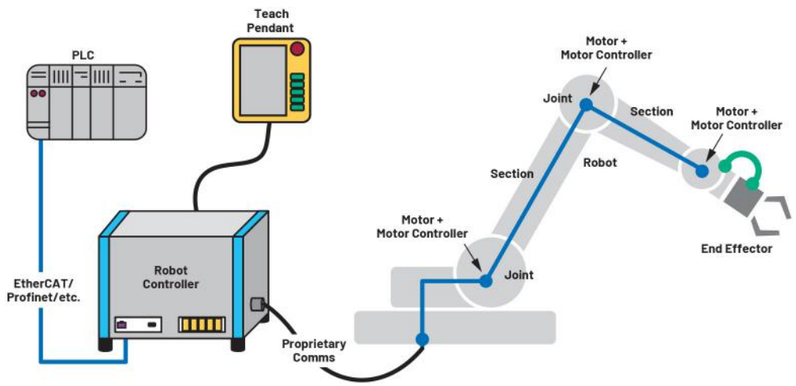


Figure 1 – Components of industrial robots/cobots.

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.

Table 1 – Overview of 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

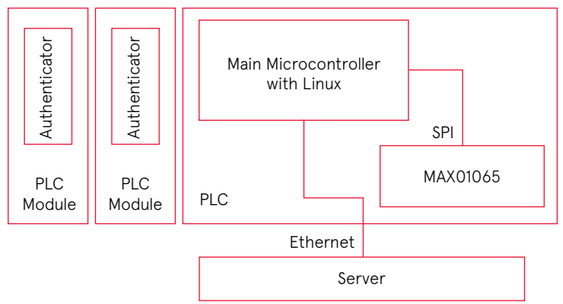


Figure 2 – Enabling security with PLC.

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.

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.

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.

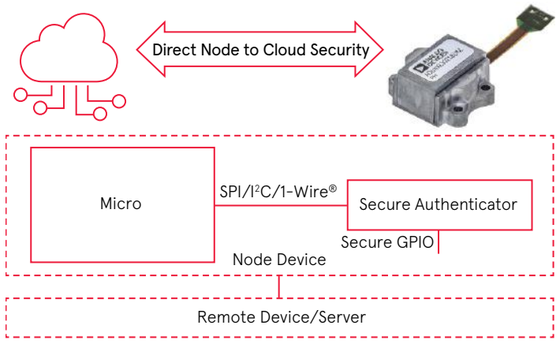


Figure 3 – Integration for the MAXQ1065 to enable the direct node to cloud security.

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

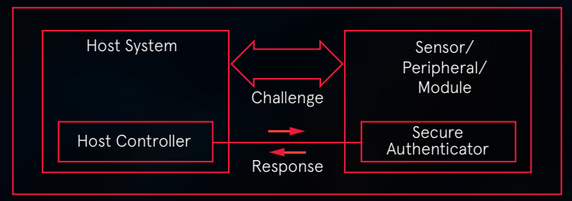


Figure 5 – Testing for authenticity with a challenge-and-response sequence.

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.

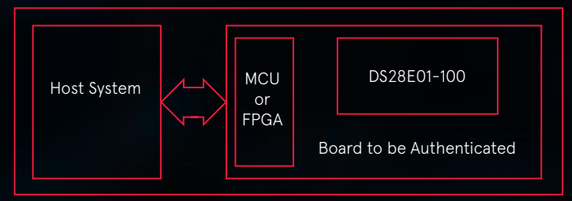


Figure 6 – A hardware authentication example using the DS28E01-100.

- 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.

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.

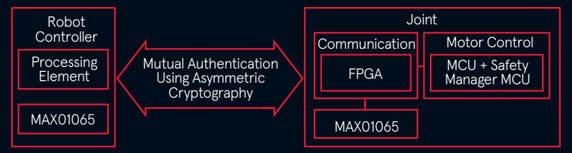


Figure 7- Joint authentication.

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.

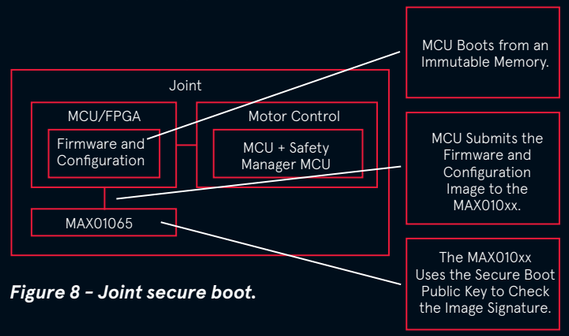


Figure 8 – Joint secure boot.

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.

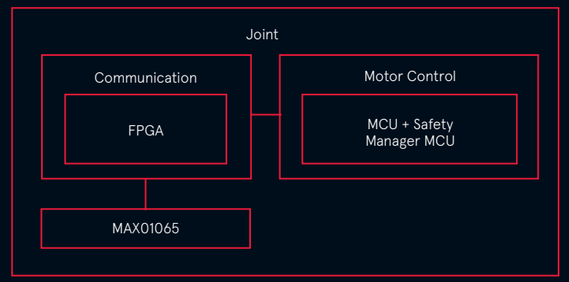


Figure 9 – A typical joint block diagram.

JOINT SECURE COMMUNICATION

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

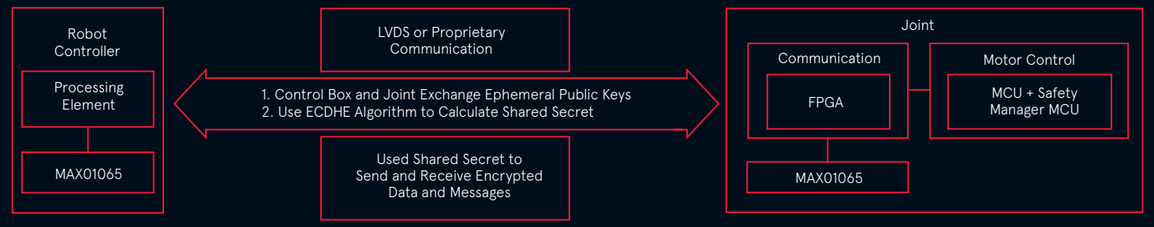


Figure 10 – Joint secure communication.

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.

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.emerging risks in an interconnected world.

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.

CLICK HERE

A GLIMPSE INTO THE INVISIBLE WORLD OF NEAR-INFRARED (NIR): EXPLORING ITS APPLICATIONS & POTENTIAL

THE INVISIBLE SPECTRUM

Infrared (IR) radiation, an invisible portion of the electromagnetic spectrum, exists between the longer wavelengths of visible light and the shorter wavelengths of microwaves. As defined by the ISO 21348 standard, IR covers a wavelength range of 760nm to 1,000,000nm (1mm). This broad spectrum is further categorized into three distinct regions based on wavelength: NearInfrared (NIR or IR-A, 760nm–1400nm), Mid-Infrared (MIR or IR-B, 1400nm–3000nm), and FarInfrared (FIR or IR-C, 3000nm–1mm).

The FIR radiation occupies the longest wavelength of the infrared spectrum and is often is associated with thermal radiation where its emission intensity directly corresponds to the temperature of an object. This unique property makes FIR technology critical for thermal systems and astronomical research, enabling applications like thermal imaging and astronomical observations through its capacity to detect and analyze heat signatures. In contrast, the NIR occupies the spectral region closest to the visible light spectrum and plays a vital role in many daily technologies and industrial applications. From enabling the communication between remote controls and devices, to safeguarding human lives.

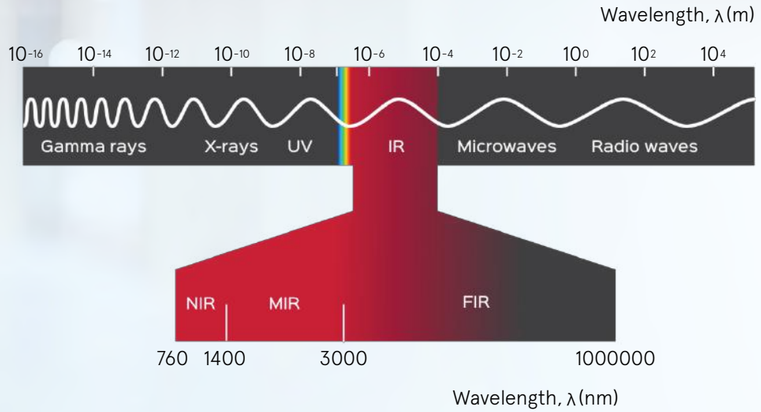


Figure 1 - The electromagnetic spectrum. Definitions are based on ISO21348 - Space environment (natural artificial).

The source of infrared (IR) radiation can be derived from both natural and man-made origins. The Sun, as the dominant natural source, emits approximately half of its total energy as IR radiation towards Earth, directly influencing the planet's temperature and climate. Man-made IR sources have undergone significant advancements, with near-infrared IR LEDs emerging as a game-changer.

Unlike traditional IR sources that emit a broad spectrum, IR LEDs offer precise control over both the wavelength and intensity of emitted IR radiation, enabling highly targeted functionalities in diverse applications.

SURVEILLANCE & SECURITY MONITORING

Capturing clear and detailed footage in low-light conditions or during the night has long been a formidable challenge for surveillance systems. Conventional lighting solutions such as floodlights or streetlights often prove inadequate, being energy-intensive, susceptible to glare, and compromising the covert nature of surveillance cameras, thus reducing their effectiveness in specific scenarios. These challenges were significantly overcome by the integration of IR LEDs into modern surveillance cameras, marking a game-changing advancement in surveillance technology.

In low-light or pitch-black environments, IR LEDs are utilized to illuminate the area under surveillance, emitting infrared radiation that is then detected by the specialized IR sensor (CMOS) within the camera. This IR radiation is subsequently converted into high-resolution footage for monitoring and recording purposes, enabling enhanced visibility and clarity surveillance even in complete darkness.

IR LEDs also offer around-the-clock surveillance when incorporated with adaptive features such as IR cut filters, enabling seamless transitions between day and night modes.

During the daytime, the IR cut filter blocks infrared light to prevent interference and maintain optimal image quality. When light levels decrease to a certain level, the filter is disabled, allowing the camera to utilize IR illumination for night vision.

The selection of IR LED wavelength plays a critical role in ensuring discreet surveillance effectiveness without compromising visibility or drawing attention from subjects under observation.

Consumer-grade surveillance cameras typically use IR LEDs that emit light at a wavelength of around 850-880nm which often produce a faint red glow that might be noticeable under certain conditions, particularly in very low-light environments or when viewed through specific types of night vision equipment.

For surveillance systems requiring greater stealth and discretion, IR LEDs with 940nm wavelength are often preferred over the 850-880nm range. This longer wavelength falls closer to the upper end of the infrared spectrum, making it invisible even to some types of night vision equipment.

Covert surveillance serves critical purposes, including preventing theft, ensuring personal and corporate security, discreet wildlife observation, as well as serving government and national security interests.

In specific surveillance scenarios requiring long-range illumination, high-power IR LEDs are the preferred choice due to their higher irradiance output and efficiency compared to LED arrays. These LEDs are capable of managing heat effectively, allowing them to operate efficiently for extended periods without compromising performance.

For larger areas like parking lots and warehouses where wide coverage is crucial, high-power LEDs with wide beam angle distribution designs are typically employed, ensuring uniform brightness across the entire monitored space. Moreover, certain IR cameras with integrated AI features can dynamically adjust IR LED output based on object proximity, resulting in consistent and balanced illumination that prevents image overexposure or washout.

SMOKE DETECTION SYSTEM

Smoke, often recognized as a leading cause to fire-related fatalities, serves as a critical indicator signaling the early stages of a potential fire hazard. As there is no fire without smoke, providing early warnings allow crucial time for evacuation and fire suppression measures, significantly reducing the risks posed by fire incidents and safeguarding lives and property. Recognizing the importance of early detection has led to the widespread implementation of smoke detection systems in residential, commercial, and industrial settings.

Although technological advancements have substantially improved the reliability and effectiveness of smoke detectors, manufacturers continue to face challenges in achieving an optimal balance between high sensitivity and minimal false alarms while maintaining costeffectiveness and long-term reliability. Regulatory bodies like Underwriters Laboratories (UL) have raised the bar for smoke detectors by enforcing stringent regulatory requirements and demanding extensive testing and certification. Among these tests is the "hamburger test" to ensure that smoke detectors will not trigger false alarms when exposed to cooking smoke.

Two primary technologies are generally employed in modern smoke detectors: ionization and photoelectric. Ionization smoke detectors utilize an ionizing source, typically Americium-241, to measure air ionization levels and trigger an alarm upon disruption caused by smoke particles while photoelectric smoke detectors employ light scattering principles to determine smoke density. Photoelectric smoke detectors are effective at detecting larger smoke particles associated with smoldering fires, while ionization detectors, despite their high sensitivity to smaller particles from fast-flaming fires, are prone to false alarms from environmental factors like dust, dirt, cooking fumes, and shower steam.

INFRARED PRINCIPLES IN PHOTOELECTRIC SMOKE DETECTORS

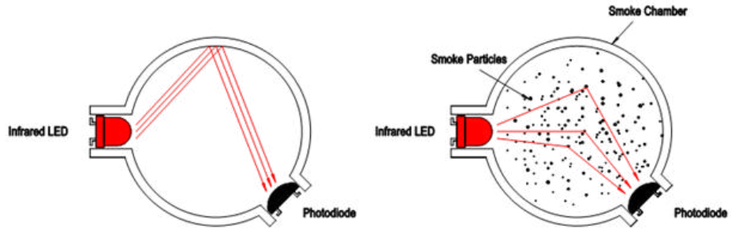


Figure 2 - Smoke detector operating principle with (right) and without (left) the presence of smoke particles

The photoelectric smoke detector operates by employing an IR LED and a photodetector within a chamber allowing the passage of air and smoke particles. During normal operation, the IR LED emits a pulse IR light directed towards the photodetector. This uninterrupted light generates an electrical current in the photodetector. However, smoke particles entering the chamber disrupt the light path, causing scattered and diminished IR light to reach the photodetector, consequently lowering the electrical current. The detector's electronic circuitry analyzes this change, triggering an alarm if it exceeds a predefined threshold, indicating a potential fire. By continuously monitoring the received IR light, the detector distinguishes between normal conditions and smoke presence, enabling early fire detection and mitigating potential damage. IR LEDs are a key component in the latest generation of smoke detectors due to their numerous advantages, including:

- Penetration Through Smoke - Compared to visible light, IR exhibits better penetration capabilities through smoke particles, enabling IR LEDs to "see" smaller and less dense smoke particles invisible to the naked eye. This enhanced light penetration facilitates earlier fire detection, ultimately leading to faster response times. While the 940nm wavelength generally exhibits slightly better smoke penetration than 850nm, the latter remains the preferred choice for most residential smoke detectors due to its costeffectiveness, compatibility with existing technology, and adequate penetration for typical smoke scenarios.
- Reduced False Alarms - Due to their minimal scattering by non-smoke particles and environmental factors like dust, humidity, and small airborne contaminants, IR light offers significant potential for reducing false alarms in smoke detection systems. Smoke detectors such as Dual-Scattering Angle (DSA) detectors analyze the angular distribution of scattered light received by the photodetector, allowing them to distinguish smoke-induced light scattering from non-threatening particulates like dust or pollen, preventing false alarms.
- Optimized Detection Sensitivity - IR demonstrates its highest sensitivity when detecting smoke particles around the 1-micron (µm) size, aligning well with common fire scenarios involving materials like burning wood, plastics, or textiles where smoke particles often fall within the 0.3-1µm range. However, modern smoke detectors now integrate Dualwavelength technology, combining IR with Blue light at a 470nm wavelength. Studies suggest that Blue light is ideal in detecting smaller particles compared to IR, typically ranging from 0.05µm to 0.3µm. This combination enables the detection of a broader spectrum of particle sizes, enhancing the sensitivity of the detector.
- Signal Boost - Narrow-angle IR LEDs focus their beams into a specific cone, minimizing the amount of light bouncing around within the smoke detector chamber. This reduces stray light interference, allowing the detector to concentrate on the light scattered by smoke particles, leading to improved sensitivity and accuracy. Additionally, the concentrated beam increases the radiant intensity reaching the photodetector, amplifying the signal strength.
- Data Analysis - Valuable information including smoke particle size, heat signatures, gas compositions, and airflow patterns can be acquired and analyzed through the integration of IR LEDs with multiple sensors like ionization, heat, gas, and airflow detectors. This integration enables the differentiation between smoke and dust, adapt to specific environments, pinpoint the fire's origin and could potentially predict the fire's behavior and spread based on real-time information.

SAFETY LIGHT CURTAIN

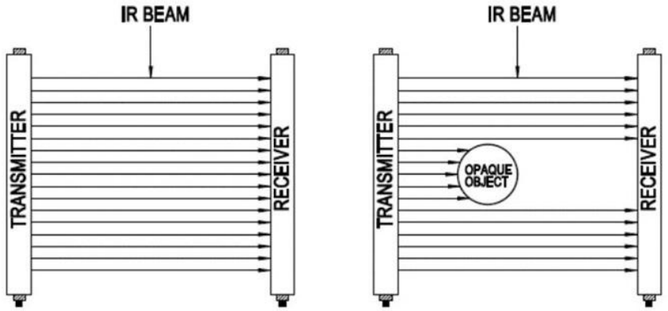


Figure 3 (left) - Structure of a safety light curtain with transmitters and receivers. Figure (right): Multiple IR beams disruption occur with object detection.

In manufacturing industrial settings, ensuring the safety of human operators is paramount for cultivating a productive work environment and throughout the years, safety light curtains have been heavily relied upon as a dependable and effective measure. Yet, according to the Occupational Safety and Health Administration (OSHA), there were over 20,000 nonfatal injuries caused by machinery in the manufacturing industry each year from 2018 to 2022 Among the most common types of machinery accidents were incidents involving being caught-in or between machinery, being struck by machinery, and contact with objects or equipment, highlighting the ongoing need for enhanced safety measures.

A safety light curtain, as its name implies, utilizes light to create a curtain-like protective barrier. It primarily comprises an array of IR LEDs serving as transmitters and corresponding photodetectors as receivers. The IR LEDs emit synchronized and parallel IR light beams, forming an invisible grid across the designated area. These beams are modulated through pulse width modulation (PWM), generating a unique frequency only detectable by the dedicated photodiodes, effectively mitigating interference from external light sources This synchronization between transmitters and receivers ensures quicker response times, enhancing overall system efficiency and reliability.

While IR LEDs form the fundamental element that generates the protective field of a safety light curtain, their compact nature also enables the development of more flexible designs. Light curtains, unlike physical barriers, are typically lightweight, sleek in design, and available in a range of shapes and sizes. This versatility ensures effortless and adaptable installation, accommodating various mounting options and allowing easy integration into a wide array of industrial environments, machinery types, and safety setups without occupying excessive space. The miniaturization of IR LEDs correspondingly enhanced the beam resolution of a safety light curtain, which defines their object detection capabilities. Measured by the spacing between the individual light beams, a finer beam resolution is achieved when more LEDs are accommodated within a unit length. Depending on the required precision level, beam resolutions typically range from 14mm for detecting small objects like fingers to 50mm for detecting large objects like arms and legs. Through advanced design techniques such as precise alignment and beam shaping of IR LEDs, cutting-edge safety light curtains can achieve beam resolutions as fine as 2mm and even eliminate any gaps or blind spots between light beams, resulting in a "zero dead zone" configuration.

UTILITY SMART METER

The growing global consciousness of the need for a more sustainable future has propelled the widespread adoption of smart meters across the globe. Recognizing the potential of smart meters to curbing carbon emissions and minimize energy wastage, several countries, including China, Japan, Europe, and the United States, have taken the lead in mandating nationwide adoption through various initiatives and policies. These efforts aim to achieve full adoption rates in the coming years, paving the way for a more sustainable and environmentally conscious society.

Smart meters offer numerous benefits to both consumers and utility providers, promoting energy efficiency, reducing wastage, and enhancing customer service. For consumers, these devices offer real-time consumption data, make informed decision-making to cut down tariff bills by recognizing usage patterns. They promote greater control over usage, encourage energy-saving habits, and offer convenient remote access to consumption data. Additionally, smart meters eliminate the risk of inaccurate billing, ensuring that consumers are charged accurately for the energy they have consumed. For utility providers, smart meters provide real-time data on consumption across their service area, enabling them to optimize grid operations, balance supply and demand, and optimize resource allocation. They also reduce power outages, facilitate demand response programs, and enhance customer service. Furthermore, smart meters offer two-way communication, allowing for remote meter reading and troubleshooting, reducing operational costs eliminating manual meter readings.

IR LEDs are utilized in smart meters primarily for short-range, bi-directional data transmission via IrDA (Infrared Data Association) protocols. These protocols facilitate on-site data retrieval, configuration updates, and interactions with nearby handheld devices. IR LEDs emit infrared light pulses, which are received by a photodiode on the data collection device. These pulses represent digital information such as energy consumption readings or diagnostic data for troubleshooting. By aligning the IR LED on the meter with the receiver on the device, data can be exchanged securely and efficiently within a short range, typically within a few meters.

In terms of security measures, IR LEDs safeguard smart meters against unauthorized access and data breaches by enabling secure data transmission between the meter and authorized devices through encrypted infrared signals. Each authorized handheld device carries a unique IR signature that is recognized by IR photodiode embedded within the smart meter. This unique identifier facilitates a secure pairing process, establishing authenticated access for data retrieval and maintenance operations. Conversely, smart meters emit specific infrared signals that are detected and interpreted by infrared sensors on the handheld devices. This bidirectional exchange of infrared signatures establishes a robust two-way authentication mechanism, ensuring secure and authorized communication between the devices. To further enhance security, some smart meters integrate IR LEDs within seal enclosures or compartments to prevent tampering or unwanted alteration to the meter.

PRODUCT OFFERINGS

Broadcom offers an extensive range of IR LEDs covering 820nm to 945nm wavelengths in various package platforms and footprints. Available in power output ranging from 0.1W to 5W, we offer solutions across key product families, including High-Power DFNs, PLCCs, SMT Lamps, Through-Hole Lamps, PolyLEDs, and ChipLEDs to suit various needs in different IR applications. ChipLED IR LEDs family features the smallest industrial standard footprint ranging from 1.0mm × 0.5mm with different mounting configurations such as top mount, right-angle mount and reverse mount for light channeling.

For applications demanding long-range illumination and precise beam control, such as surveillance cameras and industrial sensing systems, Broadcom's Through-Hole and Surface Mount Lamps IR LED product families are well-suited. These LEDs feature a robust design with high-quality optics, capable of achieving viewing angles as narrow as 6° and 18°. Additionally, the PolyLED IR LEDs are subminiature surface-mount LEDs with integrated 2mm domes, making them suitable for data and signal transmission systems.

Broadcom's IR LED portfolio includes both single-junction and high-efficiency double-junction options packaged in the industry-standard PLCC footprint, offering viewing angle selections of 30°, 50°, and 120°. For applications demanding superior thermal efficiency, Broadcom presents its high-power IR LEDs in compact 3.45mm x 3.45mm and 3.85mm x 3.85mm surface mount packages. Offering a wide power output range from 1W to 5W and viewing angles reaching 150°, these LEDs are ideal for applications requiring extensive and wide-coverage illumination

For photodetectors, Broadcom's IR photodiodes and phototransistors are available in ChipLED, Through-Hole and SMT Lamps packages. These silicon-based PIN photodetectors exhibit a typical peak spectral sensitivity ranging from 800nm to 940nm, enabling high-speed response times, low noise, and minimal dark current and capacitance. To filter out visible light, the packages are encapsulated with black epoxy.

ChipLED

- Mounting option: Top / Right-Angle / Reverse
- Peak wavelength: 850nm / 940nm
- Viewing angle: 18° / 20° / 55° / 65° / 130° / 140°

PolyLED

- Lead option: Straight / Gull Wing / Z-bend
- Peak wavelength: 850nm / 880nm / 940nm
- Viewing angle: 18° / 24°

ChipLED Photodiode

- Mounting option: Top / Right-Angle
- Wavelength of Peak Sensitivity: 690nm / 940nm
- Angle of Half Sensitivity: ±65° / ±70° / ±75°

Through-Hole Lamps Phototransistor

- Package Type: 3mm Radial / 5mm Radial
- Wavelength of Peak Sensitivity: 830nm
- Angle of Half Sensitivity: ±10° / ±12° / ±25° / ±36°/ ±40°

Through-Hole Lamps

- Package Type: 3mm Round / 5mm Round
- Peak wavelength: 850nm / 880nm / 940nm
- Viewing angle: 6° / 20° / 30° / 45° / 50°

PLCC

- Junction Type: Single / Double Junction
- Peak wavelength: 820nm / 830nm / 850nm / 870nm / 890nm / 940nm
- Viewing angle: 30° / 50° / 120°
- AEC-Q101 qualified for Automotive

ChipLED Phototransistor

- Mounting option: Top / Right-Angle
- Wavelength of Peak Sensitivity: 600nm / 940nm
- Angle of Half Sensitivity: ±16° / ±45° / ±70°

SMT Lamps

- Package Type: 5mm Radial
- Wavelength of Peak Sensitivity: 960nm
- Angle of Half Sensitivity: ±9°

SMT Lamps

- Peak wavelength: 850nm / 880nm / 940nm
- Viewing angle: 18° / 30° / 40°

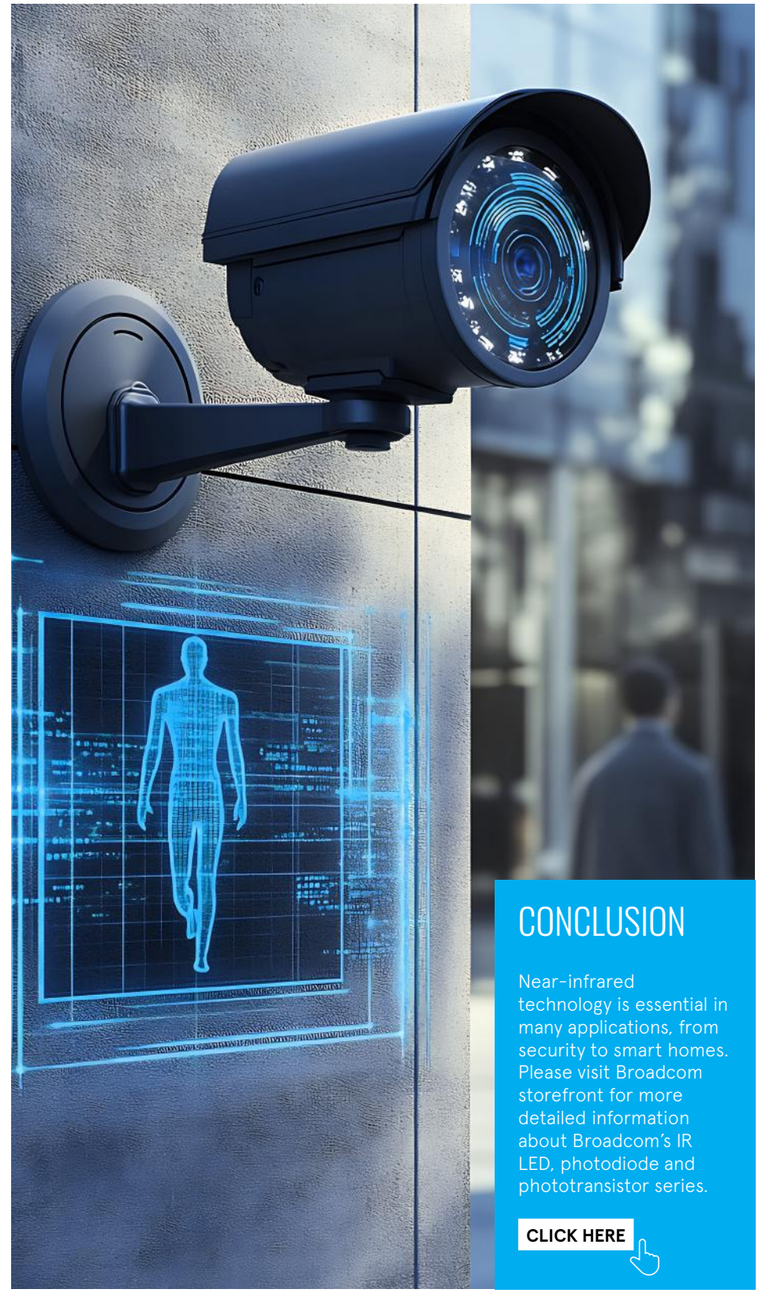
High-Power DFN

- Junction Type: Single / Double Junction
- Peak wavelength: 850nm / 855nm / 940nm / 945nm
- Viewing angle: 50° / 80° / 90° / 140° / 150°

Through-Hole Lamps Photodiode

- Package Type: 5mm Radial
- Wavelength of Peak Sensitivity: 960nm
- Angle of Half Sensitivity: ±10° / ±20° / ±30°

For more detailed information about Broadcom's IR LED, photodiode and phototransistor series, please visit Broadcom official website at www.broadcom.com



CONCLUSION

Near-infrared technology is essential in many applications, from security to smart homes. Please visit Broadcom storefront for more detailed information about Broadcom's IR LED, photodiode and phototransistor series.

CLICK HERE

VISIT STMICROELECTRONICS

NEW IOT SECURITY STANDARDS: GET READY WITH A CERTIFIED MICROCONTROLLER AND ROOT-OF-TRUST

Choosing a microcontroller and RoT that are certified to SESIP Level 3 will make it quicker and cheaper for IoT device makers to comply with the upcoming EU Cyber Resilience Act and revised Radio Equipment Directive.

Connected devices have completely changed the way we live and work. From the smart lighting in our homes to the toys children play with, and from mobile point-of-sale terminals to industrial automation and monitoring systems, we are currently experiencing a golden age for those designing and building connected equipment.

For anyone involved in this space, security has always been significant. More than 60% of respondents to an internal 2020 customer survey by STMicroelectronics said security was an important factor when creating products for the IoT. And over 75% said that having formal security certification was a powerful way to build trust with customers in this space.

As the complexity and frequency of cyberthreats increase, so it becomes ever-more important to gain this customer confidence, if a product is to be successful.

In this whitepaper, we will explore the importance of SESIP 3 certification for IoT device manufacturers, explain the specific compliance, security, and scalability challenges of connected products, and how ST can help you reduce the complexity and costs of these processes and get your products to market more efficiently.

WHAT IS A ROOT OF TRUST?

A root of trust is a security concept that refers to a trusted entity or component in a computer system that is responsible for verifying the integrity and authenticity of other components or software in the system. The root of trust is typically a hardware component, such as a secure boot chip or a trusted platform module (TPM), that is designed to be tamper-proof and resistant to attacks. It serves as the foundation for establishing trust in the system and ensuring that only authorized software and components are allowed to run. The root of trust is critical for securing sensitive data and protecting against cyber threats such as malware, viruses, and hacking attempts.

NEW REGULATIONS FOR CONSUMER AND INDUSTRIAL IOT DEVICES

From an IoT security perspective, the bar is now being raised. New mandatory EU device-level regulations will become applicable, improving the security of all IoT connected devices for use in the consumer and industrial sectors. Once the regulations are in place, if a device does not comply, it cannot be sold in this market.

In force since 2014, the EU Radio Equipment Directive (RED) became applicable in 2016.

It established a regulatory framework for anyone placing radio equipment on the market, and covers areas such as health and safety, electromagnetic compatibility, and the efficient use of the radio spectrum.

The requirements provided in articles 3(3) (d), (e) and (f) of the new EU cybersecurity law become applicable to all RF communication devices placed in the EU market as from August 2025.

The RED can be viewed as a preliminary step toward the EU Cyber Resilience Act (CRA).

This will require those manufacturing and selling hardware or software with a digital component to meet mandatory security requirements, and to continue providing this protection throughout the product's lifecycle.

While there is no formally published timeline for implementation of the CRA at this point, a reasonable expectation currently would be that it will come into application during 2027.

Connected devices* being sold in the EU market will need to comply with both the CRA and the RED if they are to get their CE marking.

The following table lists the requirements related to the Radio Equipment Directive. By complying with these requirements, device manufacturers can ensure that their products are safe and reliable for their customers.

Include elements to monitor and control network traffic, including the transmission of outgoing data, for item (d)	Is designed to mitigate the effects of ongoing denial of service attacks: for point (d)	Implement appropriate authentication and access control mechanisms: for point (d)/(e)/(f)
Are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the points (d)/(e)/(f)	Are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to points (d)/(e)/(f)	Protect stored, transmitted or otherwise processed (e)/(f) against accidental or unauthorised storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability of points (e)/(f)
Include functionalities to inform the user of changes that may affect data protection and privacy: for point (e)	Log the internal activity that can have an impact on points (e)/(f)	Allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information, for point (e)

THE EU RADIO EQUIPMENT DIRECTIVE (RED)

The new measures defined in Articles 3(3)(d), (e) and (f) will help to:

- Improve network resilience
- Better protect consumers' privacy
- Reduce the risk of monetary fraud

The four main aims of the Cyber Resilience Act (CRA):

1. Ensure that manufacturers improve the security of products with digital elements since the design and development phase an throughout the whole life cycle;
2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
3. Enhance the transparency of security properties of products with digital elements, and;
4. Enable businesses and consumers to use products with digital elements securely.

WHAT DEVICE MAKERS NEED TO KNOW ABOUT RED AND CRA COMPLIANCE

At the time of writing, the exact pathways to RED and CRA certification are still to be established. Devices may be certified against harmonized standards, though the formal list is not yet available.

What is clear, however, is that complying with the RED and CRA will place additional demands for baseline security on many device makers in the industrial and consumer IoT spaces. Both are areas that have until now only been lightly regulated in this regard.

It will no longer be enough to create a secure application. The underlying microcontroller must also be demonstrably secure and offer important security capabilities. These include:

- Device attestation: Ensuring devices can be commissioned securely.
- Update capability: Mandatory so that devices can be remotely patched if vulnerabilities are identified.
- Secure storage: To store cryptographic keys, customer credentials, and other information securely.
- Resilience against physical attacks.

Delivering these microcontroller-level capabilities requires security expertise at the microcontroller and semiconductor level. Understandably, given this is something IoT device makers may have not considered, many may not have access to this lowlevel security knowledge in-house.

With this in mind, how do the thousands of IoT device makers ensure their new equipment can meet the necessary security requirements in compliance with RED and CRA, and thereby continue to sell their products in Europe once the changes come into force?

SESIP CERTIFICATION

The Security Evaluation Standard for IoT Platforms, or SESIP, is a vendor-agnostic, multilevel security certification standard for devices being deployed in the IoT. It's essentially a simplification of the Common Criteria for Information Technology Security Evaluation, to be applicable for the unique demands of the IoT.

SESIP has been published as a European standard EN 17927 in November 2023, allowing the methodology to be recognized within the European market.

STM32Cube ecosystem: Increased flexibility and reduced design effort STM32Cube is a combination of software tools and embedded software libraries:

- A full set of PC software tools addressing all the needs of a complete project development cycle
- Ready-to-use embedded software bricks with example code (from component drivers to more advanced application-oriented features)

SESIP 3 CERTIFICATION HAS SEVERAL ADVANTAGES:

- Improved security: SESIP 3 certification ensures that an organization's security is up to par with industry standards. This means that an organization's security measures are more robust, reducing the risk of security breaches.
- Compliance: SESIP 3 certification ensures that an organization is compliant with relevant regulations and standards. This can help an organization avoid fines and legal issues.
- Enhanced reputation: SESIP 3 certification can enhance an organization's reputation by demonstrating its commitment to security. This can lead to increased trust from customers, partners, and stakeholders.
- Cost savings: SESIP 3 certification can help an organization save money by reducing the risk of security breaches. This can lead to reduced costs associated with cyber security measures and lower cyber liability insurance premiums.

UNDERSTANDING SESIP CERTIFICATION LEVELS

There are five levels of SESIP certification. The higher the level, the more secure the device.

SESIP Level 1, which is self-assessed, is the baseline requirement for most IoT device-level programs today. But with CRA and RED changes on the horizon, we expect these requirements to be raised, so we always advise customers to aim for Level 3.

With a black-box penetration testing level, SESIP Level 2 is the highest level that can be applied to a closed-source platform without cooperation by the developer. It provides a moderate level of assurance.

Achieving SESIP Level 3 involves an independent whitebox vulnerability analysis, which consists in a thorough assessment of the robustness by the evaluation lab that will look for attack paths while having full access to the detailed baseline architecture of the hardware and to the source code and binary of the root of trust firmware.

Inherited from the well-known Common Criteria methodology used in the IT industry to assess the security of IT products, this type of impartial validation is important in providing confidence that the security claims being made by the microcontroller manufacturer are both true and robust.

When device designers and manufacturers select a microcontroller with a root of trust (RoT) that has achieved SESIP Level 3 certification, they get the independent assurance that the security features the vendor is providing cover some essential requirements of the CRA and the RED, and have been correctly and robustly implemented. Higher levels of SESIP certification are required by applications such as secure elements, but this goes beyond the needs of the consumer and industrial IoT use cases discussed here.

THE BENEFITS OF SELECTING A SESIP LEVEL 3 CERTIFIED MICROCONTROLLER AND ROOT-OF-TRUST

Streamlining and accelerating RED and CRA compliance

Simply put, selecting a microcontroller and RoT that are certified to SESIP Level 3 makes it quicker and simpler for IoT device makers to achieve SESIP Level 3 certification for their full device.

This is because of the concept of reuse, or composition, in SESIP. When you build your IoT device around a SESIP Level 3 certified microcontroller and RoT, this implies that the microcontroller and its RoT meet the essential security requirements of RED and CRA, meaning no further validation of this component is required when you are going through full-device certification.

Device makers can therefore use SESIP Level 3 certified components to confidently and robustly meet the core aspects of their own device-level certification requirements and can apply for the same level of certification for the overall device.

This removes much of the complexity surrounding RED and CRA compliance from the IoT device maker and it can significantly speed up the end-to-end process.

Peace of mind around security

The financial and reputational damage that can result from an IoT security breach is significant. Knowing the microcontroller and RoT have been independently certified to SESIP Level 3 gives device makers and their customers much greater confidence in the security robustness of the foundations on which they build the security of their equipment.

More resources for product development

As touched on earlier, many device makers won't have the low-level security expertise required to comply with the CRA and RED in-house. Choosing a SESIP Level 3 certified microcontroller and RoT means the IoT device maker does not need to build and maintain the low-level security functionality themselves, since this is taken care of by the microcontroller vendor.

In addition, the device maker does not have to go through the process of independently validating their low-level microcontroller security, because the silicon vendor will already have done this.

Put together, this means IoT device makers will not need to invest in and maintain their own costly low-level security expertise. This will leave more resources available to focus on enhancing core product functionality.

HOW ST HELPS IOT DEVICE MAKERS MEET THEIR RED AND CRA REQUIREMENTS

To help IoT device makers comply with CRA and RED requirements, ST provides pre-certified STM32 microcontrollers including ultra-low-power STM32U5, STM32U0, high-performance STM32H5 and STM32H7R/S, and wireless STM32WBA series as well as STM32 microprocessors. These devices, including the RoT, now target SESIP Level 3 certifications with both software and physical attacker resistance.

In addition to the STM32 Open Development Environment, ST provides a range of tools and resources to help device makers ensure compliance with the regulatory requirements. These include reference designs, software libraries, and development kits that are designed to help developers build IoT devices that meet the regulatory requirements. This includes providing tools to manage the low-level security capabilities robustly, such as over-the-air updates.

STM32Trust simplifies your approach to security

To ensure designers have all the necessary resources to meet the ever-increasing challenges of today's security requirements, ST's STM32Trust solution provides a robust, multilevel strategy to enhance security and comply with the different regulations mandated by the latest certification schemes.

Based on our STM32 microcontrollers and microprocessors combined with our STSAFE secure elements, STM32Trust ensures stronger, more scalable security for your embedded systems. With a set of 12 security functions offering hardware, software, and design services from ST and third parties, STM32Trust complies with the new requirements of national regulations and security standards for applications.

Overall, ST's solutions and services are designed to help IoT device makers comply with the regulatory requirements for wireless devices and bring their products to market quickly and efficiently.

STM32 Trust

WHAT IS STM32TRUST?

A robust multilevel strategy to enhance security in embedded systems, STM32Trust is a security framework that offers a complete toolset for code and execution protection and ensures IP protection, firmware authenticity and secure firmware updates, as well as secure data and the use of validated credentials.

STM32Trust helps protect your assets by identifying and analyzing threats and vulnerabilities to define protections and countermeasures and mitigating them with ready-to-use security functions and services.

To further ensure a high level of security, STM32Trust is based on two product certification schemes aligned with numerous national & application security standards:

- Security Evaluation Standard for IoT Platforms (SESIP) published by GlobalPlatform for IoT devices
- PSA Certified (Platform Security Architecture) by Arm® protecting IoT devices

CONCLUSION

Trust in embedded systems now hinges on transparency. Open-source firmware, with its inherent transparency and continuous improvement, plays a crucial role. However, evolving threats like side-channel and AI-powered attacks necessitate robust security measures. STM32Trust, with its focus on threat identification and mitigation, helps protect your assets. Visit STMicroelectronics storefront to learn more.

CLICK HERE

HOW TO DEVELOP EFFICIENT AND ACCURATE DRIVES FOR ROBOTIC APPLICATIONS

By **Frank Malik**,
Principal Engineer Solution Marketing,
Toshiba Electronics Europe GmbH

In the late twentieth century, robots were perceived as science fiction...

Primarily hidden in automotive manufacturing for tasks like welding car chassis. These machines boosted productivity and accuracy but required significant investment.

Recent advancements in motor control, simulation, and connectivity have transformed the robotics landscape, leading to substantial market growth over the past decade. Industrial robots still dominate sales, but collaborative robots and mobile robotics, such as Autonomous Mobile Robots (AMRs), are rapidly expanding . Human-robot hybrid technologies, like exoskeletons for heavy load manipulation, are also emerging.

Industry 4.0 initiatives and reduced costs of AI vision systems have expanded technological options for manufacturers while lowering investment costs. Consequently, lighter and adaptable robotic systems are becoming commercially viable for complex, mundane tasks traditionally performed by humans.

ROBOTIC CONTROL

The control system used to drive the servo motor, usually a brushless DC (BLDC) or stepper motor, in the joint of a robotic arm, can be broken down into three basic elements: a controller, an output stage and a feedback loop. A lot of today's designs integrate the control system with the servo motor into the robotic arm itself rather than connecting the two separate parts on-site during installation, making it more compact and reducing the likelihood of electromagnetic compatibility (EMC) issues. To assure speed and accuracy, these control systems need to be small and lightweight as well as highly efficient.

Within the control system, the microcontroller (MCU) needs to be powerful with plenty of memory and integrate complex peripherals to offload varying levels of control complexity from the processor. These requirements are essential for smooth, high-precision field-oriented control (FOC) based movement. Toshiba's TMPM4K motor control MCU, for instance, integrates a 160MHz Arm® Cortex®-M4 core with a built-in floating-point unit (FPU) and has memory protection units as well as up to 1MByte of code flash and 64KB of data flash. Alongside the advanced programmable motor driver (A-PMD) and vector engine plus (A-VE+) for vector control, the MCU can handle such compute intensive motor control algorithms like FOC.

The motor inverter, or output stage, needs power devices that feature a low on-resistance (RDS(ON)) to minimise losses. By using its U-MOSIX-H process with a low voltage trench structure, Toshiba's TPW3R70APL 100V power MOSFETs feature an RDS(ON) of 3.1mΩ (typ.) at a gate-to-source voltage (VGS) of 10V with a low output and gate switch charge.
This compact and lightweig device is housed in a therm enhanced double-side coo package (DSOP Advance), which features a top side cooling pad to help with he dissipation. These attribute combine to minimise the si of the joint, a key requirem for slimline collaborative robot arms, Selective Compliance Articulated Robot Arms (SCARA) and delta robot designs.

The final element of the co system is the feedback loo which is typically implemen in the software. Its primary is to determine the precise position of each axis of the robotic system derived from various types of sensor data, such as Hall-effect sensors, resolvers, or encoders. MCUs developed specifically for motor control applications, like the TMPM4K, offer a range of input peripherals that automatically decode this data and generate interrupt signals that can trigger actions in the software.

Designers need to effectively test each of these three elements to develop the optimal robotic control system. To support this test requirement, Toshiba has developed a highly configurable servo drive reference model that combines all the required pieces for multi-channel motor control (Figure 1).

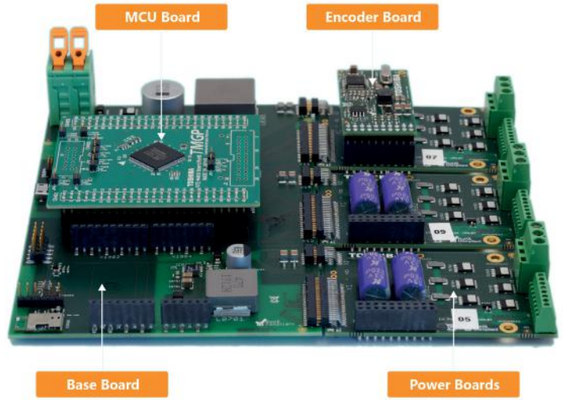


Figure 1 - Toshiba's servo drive reference model is highly modular, allowing a broad range of servo motor approaches to be trialled and implemented.

EASING ROBOTIC CONTROL DESIGN

The servo drive reference model platform comprises a baseboard that provides the necessary connectivity between the three functional elements of the motion control system. On top of this board sits an interchangeable MCU board, and, on the side, the designer can attach up to three power boards along with their optional encoder boards.

In addition to the MCU plug-in area, the baseboard also provides a connector for Arduino-compatible shields. This allows the integration of CAN, Ethernet, or other networking protocols. For ease of system analysis, a USB-to-UART converter, isolated from the MCU, is also provided while debugging is supported through an easily accessible JTAG connector. Power, polarity protection, and level shifters, where needed, including a TCR3DM33 low drop-out voltage regulator, round off the design (Figure 2)

The low-voltage power board provides power to the selected motor. It accepts an input voltage of up to 48 V and integrates a 3-phase inverter based upon Toshiba's TPW3R70APL power MOSFETs. This makes the board suitable for power dissipation of up to 10W and a heatsink can be fitted if required. Current measurement is also implemented in this board, with a TC75WxxFU comparator to provide a fault feedback signal to the base board - a temperature sensor adds further protection. The phase currents for the motor are also linked back to the base board for use by the MCU, where required.

The board features two further connectors: one is used for controlling a brake, connected to a GPIO pin through an SSM3K16 power MOSFET and a digital output optocoupler like the TLP2370. The other allows the connection of an encoder board, if required, for the feedback loop. Since this can take many forms, provision is made for both differential encoder and resolver boards, to simplify the integration of the sensors.

The servo drive reference model package is supported with firmware for the MCU based upon a real-time operating system (RTOS) with example code providing well-documented software application programming interfaces (APIs). A graphical user interface (GUI) helps during development by highlighting, in real-time, firmware status and parameters for each axis of the robot implementation (Figure 3).

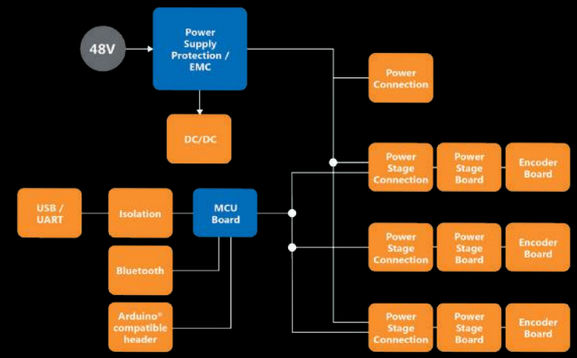


Figure 2 - The block diagram for Toshiba's servo drive reference model baseboard.

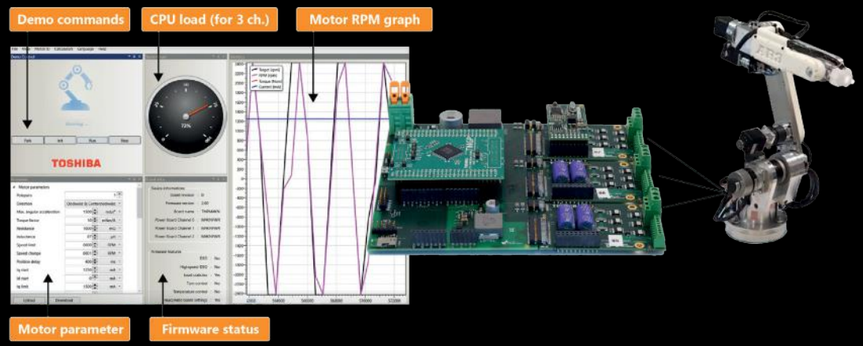


Figure 3 -z An AR3 robot arm has been converted to use BLDC motors with Hall sensor encoders. This provides a demonstration platform for the servo drive reference model GUI and firmware API.

CONCLUSION

Robotic control systems are getting more accurate, more efficient, and less expensive due to the development of highly integrated MCUs tailored to the demands of motor control as well as ongoing developments in power devices and packaging technology. These attributes support the increasing interest in collaborative robotic systems capable of performing difficult tasks that are tedious and taxing for humans. Moreover, they enable the development of AMRs used to transport workpieces and finished goods throughout factories and warehouses, and, even, make last-mile deliveries in our towns and cities. Flexible development platforms like the servo drive reference model platform make all this possible.

CLICK HERE

YAGEO GROUP

VISIT YAGEO

YAGEO X-SEMI MOSFETS: HIGH EFFICIENCY SOLUTIONS FOR **MODERN POWER APPLICATIONS**

In the realm of modern electronics, power management is crucial, and Metal-Oxide-Semiconductor Field-Effect Transistors (MOSFETs) play a pivotal role. YAGEO X-Semi, a prominent player in the semiconductor industry, offers a robust line of MOSFETs that are widely adopted for their efficiency, reliability, and cost-effectiveness. This article delves into the technical specifications, applications, and key features of YAGEO X-Semi MOSFETs, highlighting why they are the preferred choice for various power applications.

OVERVIEW OF MOSFETS

MOSFETs, or Metal-Oxide-Semiconductor Field-Effect Transistors, are essential components in electronic devices, primarily used as switches to control the flow of electrical power. Among the types of MOSFETs, the enhancement N-channel MOSFET is the most common due to its favorable performance characteristics.

KEY SPECIFICATIONS OF YAGEO X-SEMI MOSFETS

YAGEO X-Semi MOSFETs are designed with specific characteristics that make them suitable for a wide range of applications. Here are the critical specifications:

- Drain to Source Voltage: This parameter defines the maximum voltage that the MOSFET can withstand between the drain and source terminals. Exceeding this voltage can damage the device.
- Current / Continuous Drain: This indicates the maximum continuous current the MOSFET can handle at a temperature of 25°C. This value is subject to thermal limitations and must be carefully managed to prevent overheating.
- Drive Voltage: This is the gate-source voltage required to achieve specific on-state resistance characteristics. It is crucial for determining the efficiency and speed of the MOSFET.
- On-Resistance: The resistance between the drain and source terminals when the MOSFET is in the on-state. Lower values translate to lower conduction losses, enhancing overall efficiency.
- Gate Charge: This specifies the amount of electrical charge needed to switch the MOSFET on or off. Lower gate charge enables faster switching speeds and reduces power losses during transitions.
- Gate-Source Voltage: The maximum allowable voltage between the gate and source terminals. Exceeding this limit can lead to device failure.
- Power Dissipation: This parameter defines the maximum power the MOSFET can dissipate without exceeding its thermal limits. Proper thermal management is crucial to maintain reliability.
- Operating Temperature: The recommended temperature range within which the MOSFET can operate effectively. Exceeding these temperatures can degrade performance or damage the device.

SAFE OPERATING AREA (SOA)

Ensuring that the application stays within the MOSFET's Safe Operating Area (SOA) is critical for reliable operation. The SOA is defined by four key boundaries:

1. Maximum Operational Current: The limit of the current that the MOSFET can safely conduct.
2. On-Resistance: The resistance in the on-state, affecting conduction losses.
3. Power Dissipation Limit: The maximum power the MOSFET can dissipate without damage.
4. Maximum Operational Voltage: The highest voltage the MOSFET can handle without breaking down.

APPLICATIONS OF YAGEO X-SEMI MOSFETS

YAGEO X-Semi MOSFETs are versatile and find use in various high-power applications due to their efficiency and reliability. Some primary applications include:

- Adapters and Chargers: Efficient power management in consumer electronics.
- Electric Vehicle (EV) Chargers: Reliable power switching for fast and safe charging.
- Solar Inverters: Converting solar energy into usable electrical power with minimal losses.
- Industrial Power Tools: High-performance power control for robust industrial environments.
- Lighting: Efficient power regulation for LED and other lighting systems.

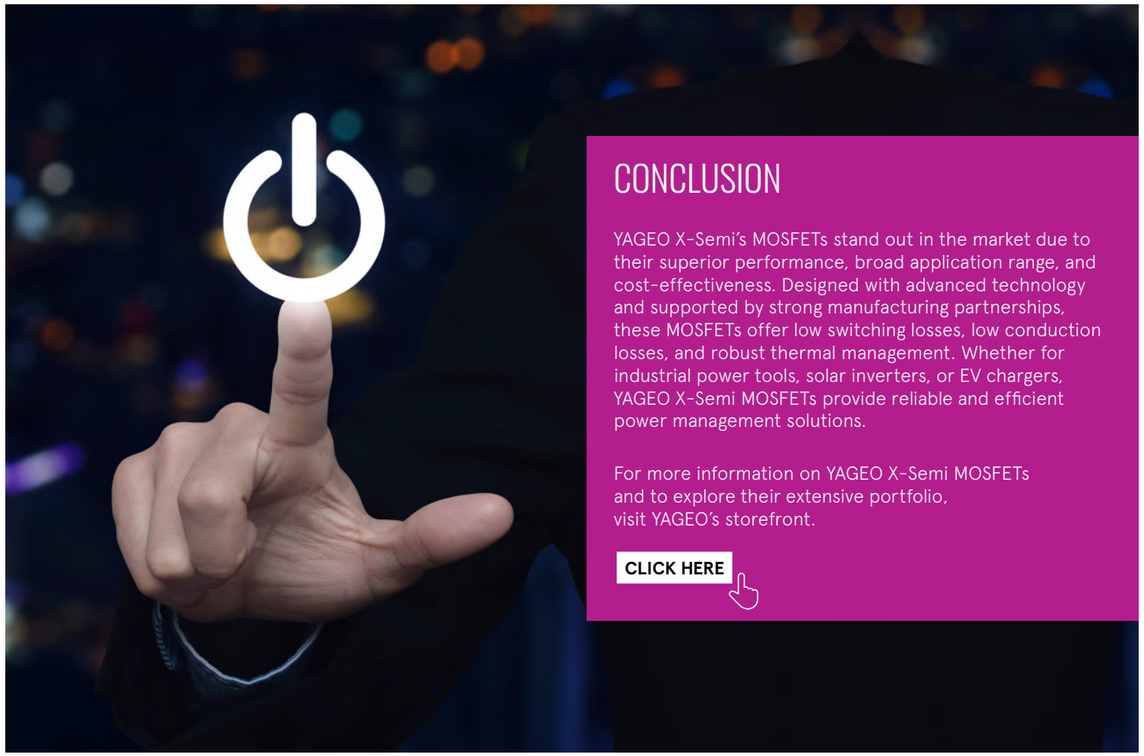
TARGET APPLICATIONS

- BLDC Motor Control: Precise and efficient control of brushless DC motors.
- Li-Ion Battery Management Systems (BMS): Safe and efficient management of lithium-ion batteries.

WHAT CUSTOMERS CARE ABOUT

When selecting MOSFETs, customers prioritize several key factors:

- Efficiency: Lower conduction and switching losses ensure minimal energy wastage.
- Reliability: Consistent performance under various operating conditions.
- Cost-Effectiveness: Competitive pricing without compromising on quality and performance.

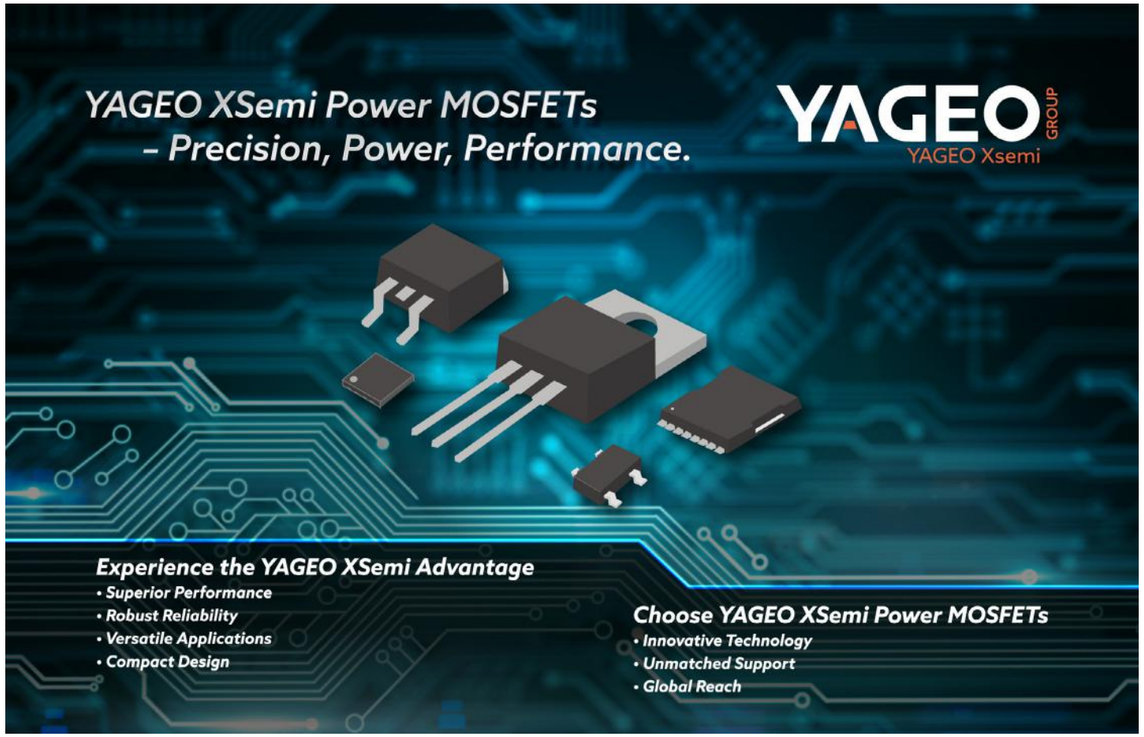


CONCLUSION

YAGEO X-Semi's MOSFETs stand out in the market due to their superior performance, broad application range, and cost-effectiveness. Designed with advanced technology and supported by strong manufacturing partnerships, these MOSFETs offer low switching losses, low conduction losses, and robust thermal management. Whether for industrial power tools, solar inverters, or EV chargers, YAGEO X-Semi MOSFETs provide reliable and efficient power management solutions.

For more information on YAGEO X-Semi MOSFETs and to explore their extensive portfolio, visit YAGEO's storefront.

CLICK HERE



TECHNICAL RESOURCES

Explore our well-curated library of whitepapers, technical articles, videos, training modules, tutorials, and more to support you in developing your designs, business, and career.