Brochure

MC-Edge: Security

Learn how MC-Edge can help keep your IoT data protected from cyber threats

MOTOROLA SOLUTIONS

The evolution of the edge

As the transition into the era of IoT and decentralized control continues, challenges evolve. Remote sites face limited public network infrastructure, the need for autonomous local response, and an escalating cyber threat landscape.

The MC-Edge™ isn't just a gateway; it is the culmination of long-standing field experience, engineered to solve these challenges with security by default.

The challenge	The MC-Edge solution
Response time and autonomy	Engineered for independent operation at the edge, allowing the system to react to events in real-time without total dependence on the control center.
Connectivity and continuous communication	Ensures operational continuity through redundant communication paths, keeping data flowing even if a primary link fails.
Remote infrastructure stability	Built to withstand the limitations of public and cellular networks in remote locations, providing a stable and reliable connection for national-level infrastructure.
The cyber threat landscape	Moves beyond simple data protection to prevent device manipulation and network-wide penetration. The MC-Edge hardens the device against both logical and physical attacks, so that the edge unit will not become a gateway for intruders.

How MC-Edge mitigates cyber threats

In critical infrastructure failure is not an option, edge security must be absolute. The MC-Edge mitigates security risks at remote sites through security-by-default engineering and layers of physical and logical security hardening including:

Data protection layer

Securing the unit's identity and sensitive information through physical and logical hardening.

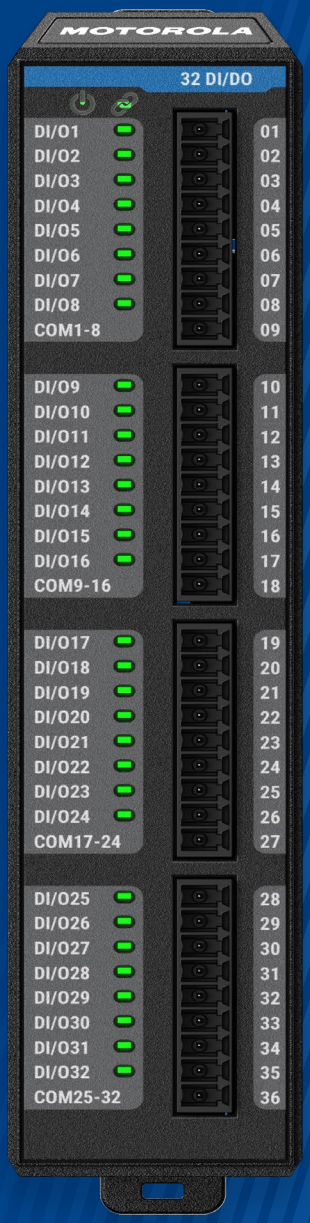
- **Hardware Security Module (HSM):** The MC-Edge supports the integration of a dedicated micro-HSM for MDLC communication and sensitive data at rest.
  - **Identity protection:** Features a physically hardened and isolated hardware chip dedicated to safeguarding the gateway's identity and cryptographic keys.
  - **Tamper events:** Removing or attempting to bypass the security immediately triggers a tamper event.
  - **Active data safeguard:** Prevents key theft through physical extraction; if storage removal is attempted, critical keys are automatically deleted or made unusable.
  - **Cryptographic agility:** Supports up to 5 algorithms simultaneously, including AES-256 (GCM), ECC (P-384 Curve), and RSA up to 4096-bit.
  - **FIPS 140-3 Level 3 compliance[1]:** The cryptographic module is built to meet Level 3 standards, ensuring cryptographic operations are protected from misuse.
- **Automated certificate management (PKI/SCEP):** Utilizes SCEP for automated initial enrollment (both automatic and asynchronous) with a Certificate Authority (CA).
  - **Lifecycle management:** Handles public key certificate renewal and Certificate Revocation List (CRL) updates automatically.
- **Software signing and verification:** Prevents unauthorized or malicious code execution through cryptographic signature verification for all firmware updates, user data, and edge applications.

Network and communiction layer

This layer focuses on isolating the device and establishing secure communication paths between the edge unit and the control center.

- **IPSec tunneling:** Provides secure remote access by protecting the entire original IP packet in "Tunnel Mode" over Ethernet and LTE interfaces.
- **Firewall protection:** Monitors and blocks unauthorized data transmissions to achieve network isolation.
- **Single Pair Ethernet (SPE) I/O modules:** The new SPE standard replaces legacy CAN BUS, offering native IP support for smart, secure module management and enhanced hardware-level security.
- **TLS V1.3 support:** Supports the latest TLS 1.3 protocol, delivering ultra-secure, low-latency MQTT, LoRaWAN® backhaul and HTTPS communication for mission-critical data.
- **SSH tunneling:** Secures legacy Modbus and DNP3 protocols through robust SSH tunneling, providing encrypted and cyber-hardened communications for critical infrastructure.

[1] Certification of FIPS 140-3 Level 3 is pending



SPE I/O module

Access management layer

Focuses on identity and gatekeeping, so that only authorized users and devices can interact with the MC-Edge.

- **IEEE 802.1x authentication:** Implements port-based network access control to block unauthorized physical entities from connecting to the device.
- **Allowlist:** Blocks Ethernet access except for network devices with an explicitly authorized MAC address.
- **USB restrictions:** Restricts USB interfacing to specific authorized vendor-IDs and product-IDs.
- **Console port control:** The console port can be deactivated via provisioning to prevent unauthorized local physical access.

Standards and certifications

Our commitment to cybersecurity is backed by industry-leading certifications and a standardized development process.

- Fully compliant with RED Article 3.3 (Cyber security certificate for Europe).
- Our product development is governed by an IEC 62443-4-1 Maturity Level 2 framework, ensuring that all security activities are systematically managed, documented, and repeatable throughout the product lifecycle.

To learn more, visit:
www.motorolasolutions.com/mcedge

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**