enigmedia

Enigmedia **MUGA**

Product Brochure

Protect OT implementing best-in-class Zero-Trust security designed in conformity with IEC-62443

Effortless network segmentation and micro-segmentation, masking legacy ICS and critical assets for unauthorized access and minimizing threat exposure under L3 in the Purdue Model

The Challenge

Digital transformation brings many benefits to industrial infrastructures.

Digitisation allows improved efficiencies, cost reduction, energy optimization, better supply chain integration, less environmental impact, and generation of new business models.

But digitisation brings new risks.

Traditionally, industrial infrastructures were “isolated”, and industrial networks and devices were not designed to be connected, presenting severe vulnerabilities that can be exploited by malicious attackers and provoke production downtime with big economic impact and even putting people’s safety at risk.

In this context, Industrial enterprises and critical infrastructures follow the recommendations of the latest industrial norms and standards, such as IEC-62443, when planning a robust cybersecurity strategy. IEC-62443 is based on “Defense-in-Depth” principles, providing a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems.

The Solution

MUGA is a Zero-Trust security platform for OT networks based on Enigmedia OS, our own operating system integrating advanced security features. MUGA software is embedded into rugged IoT and Industrial Gateways to deliver optimum security on site.

Designed in conformity with the IEC-62443 norm, MUGA delivers multiple cybersecurity features to protect digitisation projects and Industry 4.0 initiatives.

Fully compatible with existing devices and protocols, MUGA is deployed with zero-touch provisioning to avoid complex and costly process reengineering.

MUGA comprises 2 key elements: a security enhanced agent MUGA Node, and MUGA Orchestrator as a centralized management console including an intuitive user interface for Node onboarding and configuration.

Key Functionalities

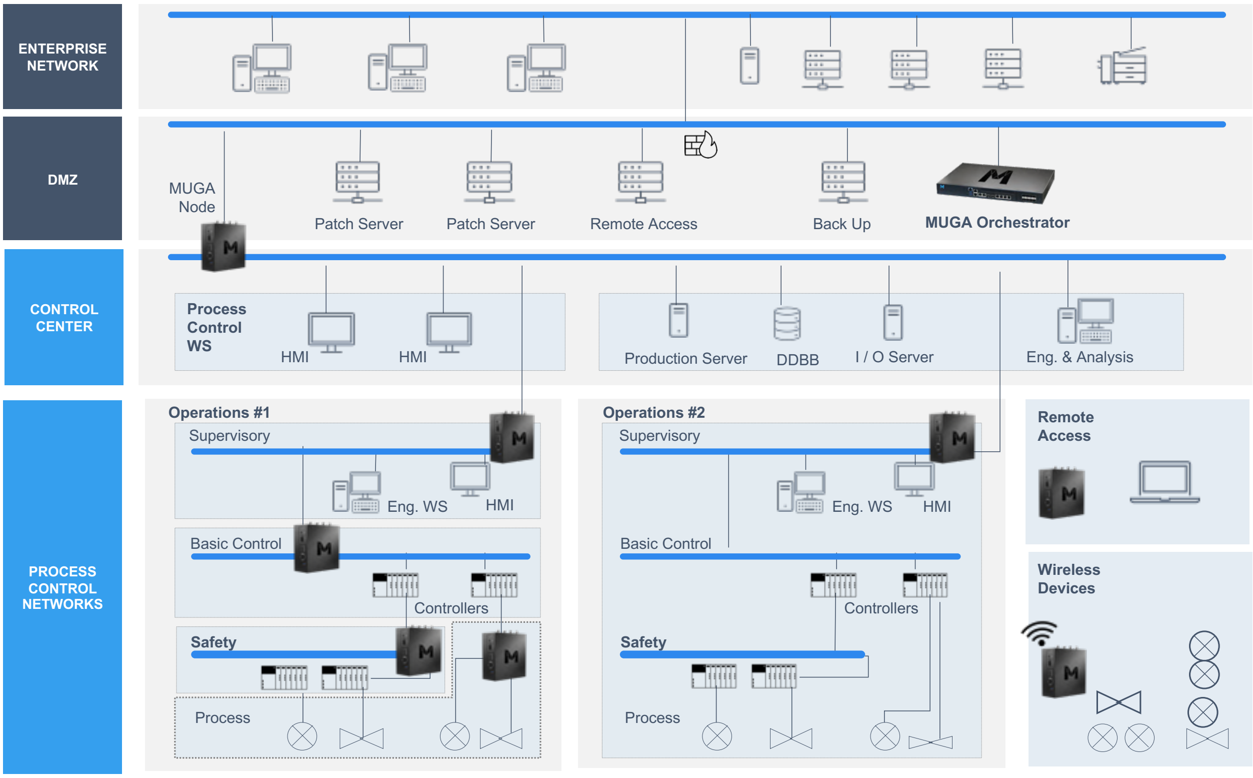
MUGA guides industrial enterprises along the norm roadmap by integrating advanced cybersecurity under L3 in OT networks, featuring:

- **Asset discovery**: Identify critical assets, connections and map the current state of OT networks
- **Segmentation & micro-segmentation**: Isolate legacy and critical assets into individual units with our express virtual zoning
- **Firewall and conduit definition**: Apply flexible firewall rules and defining conduits, crucial for advanced OT protection
- **Encryption & authentication**: Eliminate unauthorized access and protect data, masking the network to external threats
- **Host IDS & monitoring** Get alerts in your monitoring tool, and enjoy easy integrations.

Enigmedia OS

MUGA enjoys a hardened Enigmedia OS specifically designed for industrial network requirements, and considering “availability” as the main value to preserve. Among others, Enigmedia OS includes:

- Secure boot
- Full disk encryption
- Anti-tampering
- Host IDS
- OTA (over-the-air) signed firmware updates
- Hardware watchdog
- Alerts and logs management.



We want to hear from you

Visit us at: enigmedia.es

marketing@enigmedia.es
+34 603 462 937

About Enigmedia

Enigmedia builds cutting-edge industrial cybersecurity products to protect critical infrastructures and industrial companies in their digitisation journey. Enigmedia's products have been designed together with industrial CIOs and CISOs and in conformity with international norms, standards and best practices. Enigmedia helps to mitigate industrial threats with advanced cybersecurity features.