

Press Release

FOR IMMEDIATE RELEASE
2025

Contact Information

Bobbie Ferraro
VP, Marketing and Critical Infrastructure Partners
310.800.5252
Bobbie.Ferraro@psgglobal.net

Prometheus Security Group Awarded Patent for Groundbreaking Method to Secure Legacy Analog Sensor Systems

Revolutionary technology encrypts physical security sensors and controls at the edge—without replacing existing infrastructure

Austin, TX — June 19th, 2025 — Prometheus Security Group Global, a leader in Zero Trust physical security innovation, has been granted a U.S. patent for a novel method of securing legacy analog circuits in physical security systems, industrial control systems (SCADA), and premise access control applications. The patent (U.S. Publication No. 20220021545), titled “Novel Method of Securing Legacy Analog Sensor Circuits Used in Physical Security, Premise Access Control and Industrial SCADA Applications,” introduces a revolutionary approach to encrypt and authenticate analog sensors and facility controls transforming data at the edge—without the need for complete system replacement.

The patent covers the design and implementation of a **Universal Field Panel (UFP)** powered by a secure microcontroller that authenticates and encrypts both sensor inputs and control outputs. Leveraging a **Digital Encrypted Security Interface (DESI)**, the system modernizes analog infrastructure with authenticated digital cryptography, enabling secure communication between legacy devices and command systems.

“Most legacy intrusion detection and physical access control systems still rely on electronic techniques from the 1940s. This technology brings those systems into the modern age—featuring strong encryption, edge authentication, and seamless integration with today’s commercial platforms, while reusing the existing wiring plant,” said Jeremy Freeze-Skret, inventor and Chief Architect at Prometheus Security Group.

Key Innovations Include:

- **Drop-in compatibility** with existing analog sensor infrastructure (e.g., motion detectors, door contacts, relay outputs)
- **Edge authentication and encryption** using scalable public key infrastructure PKI cryptography
- **Tamper detection**, latching mechanisms, and watchdog timers to mitigate spoofing and replay attacks
- **Failover-ready architecture** with support for controlling redundancy and public-key lifecycle management

Unlike traditional physical security panels, the UFP with the DESI enables encrypted communication from sensor to server, eliminating blind spots and authentication gaps in security environments ranging from critical infrastructure and military bases to data centers and commercial applications.

About Prometheus Security Group (PSG)

Prometheus Security Group (PSG) delivers next-generation security solutions, bridging the gap from legacy analog to advanced digital systems in critical environments. Using Zero Trust principles, our ZTA Unified Solution, and its integrated technologies, ensure continuous authentication and verification across physical and digital domains, enhancing safety, situational awareness, and response. PSG seamlessly integrates with intrusion detection, access control, video and cyber-secure data platforms, protecting government agencies, critical infrastructure, and industrial operations.

High-security facilities rely on PSG for clean data to power AI-driven analytics, safeguard edge devices against threats, and enable cost-effective system integration. Backed by top federal certifications, PSG meets the most rigorous security standards. Headquartered in Austin, Texas, we operate globally, supporting defense, energy, and enterprise markets.

For more information, visit www.psgglobal.net or contact marketing@psgglobal.net.