PROMETHEUS™
SECURITY GROUP GLOBAL

P: (512) 247 3700
E: Sales@PSGGlobal.net
W: psgglobal.net

PREMISE CONTROL UNIT

Trusted Devices. Trusted Data. Trusted Decisions.

PRODUCT OVERVIEW

The **PSG Premise Control Unit (PCU)** is a complete **Zero Trust physical security platform** that combines intrusion detection, access control, embedded Command & Control (C2) software, and authenticated edge technology into a single integrated solution. Serving as the central management interface for PSG's Universal Field Panel (UFP), the PCU provides an HTML5 web application to configure the system, manage connected devices, and monitor security operations—all without the need for dedicated application servers or additional security software.

Built on PSG's Universal Field Panel (UFP) architecture, the PCU provides a modern physical security system for both **new construction and retrofit projects**. For retrofit projects, organizations can preserve existing wiring, sensors, readers, and door hardware while transitioning to Zero Trust at their own pace—**eliminating the need for costly rip-and-replace upgrades.**

Unlike traditional security systems that rely on **implicit trust** and **vulnerable end-of-line (EOL) resistor technology**, the PCU establishes **trust at the source**. When paired with PSG's Digital Encrypted Security Interface (DESI), connected field devices are **cryptographically authenticated**, communications are secured, and security events are verified before data enters enterprise systems, analytics platforms, or AI applications.

The result is a **cost-effective, easy-to-deploy platform** that delivers **trusted data, reduces cyber attack vulnerability,** and enables **more confident security decisions**.

KEY SYSTEM FEATURES

01. **COMPLETE SYSTEM IN A SINGLE ENCLOSURE**

02. **NO RIP-AND-REPLACE REQUIRED**
Preserve existing wiring, sensors, readers and door hardware while enabling a phased transition to Zero Trust.

03. **EMBEDDED C2 SOFTWARE**
No dedicated application server requirement.

04. **INTEGRATED INTRUSION DETECTION**
Supports scalable intrusion detection with up to 64 DESI devices per EM-16 panel.

05. **INTEGRATED ACCESS CONTROL**
Supports scalable OSDP reader deployments with up to 16 reader per EM-16 panel.

06. **HTML5 BROWSER-BASED MANAGEMENT**
No client software installation required.

07. **OPEN ARCHITECTURE DESIGN**
Supports integration with third-party security platforms.

08. **TAA/NDAA COMPLIANT**
Made in the USA.

DESI Zero Trust Capabilities

1. **REDUCES CYBER ATTACK VULNERABILITY**
   Eliminates implicit trust by authenticating devices, securing communications, and verifying data at the source.
2. **TRUSTED DATA FOR ANALYTICS & AI**
   Delivers authenticated, verified data for confident decisions.
3. **AUTHENTICATED DEVICE IDENTITY**
   Cryptographically authenticates the identity of connected field devices.
4. **AUTHENTICATED COMMUNICATIONS**
   Protects communications from the edge to enterprise systems.
5. **VERIFIED EVENT GENERATION**
   Validates alarms and events before they reach operators, automation, or AI.

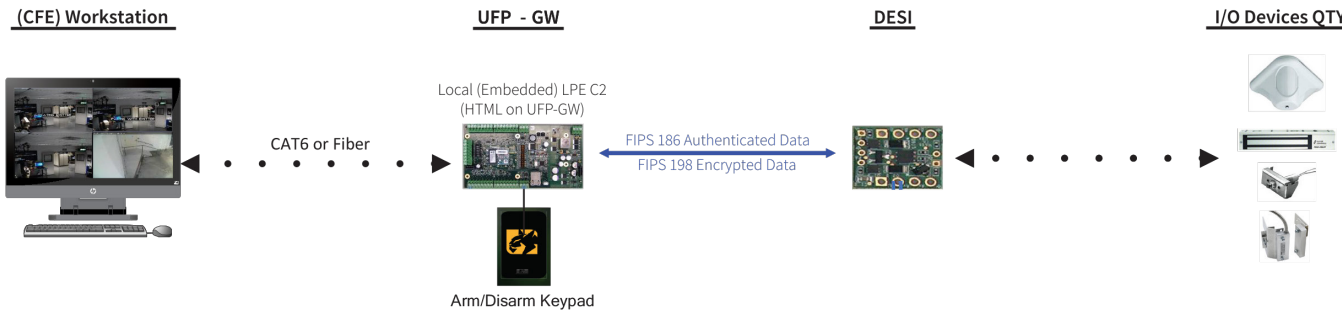
Proven in the Most Demanding Environments

Originally developed to meet the stringent security requirements of Sensitive Compartmented Information Facilities (SCIFs), the PSG Premise Control Unit brings the same high-assurance Zero Trust architecture to organizations that cannot afford to compromise security.

Ideal Applications

- Commercial Buildings
- Corporate Campuses
- Healthcare Facilities
- Schools and Universities
- Data Centers
- Warehouses and Distribution Centers
- SCIF and ICD-705 Environments
- Manufacturing Facilities
- Government Facilities
- Utilities
- Transportation Facilities
- Remote or Unmanned Sites

Premise Control Unit System Architecture



- Any PC can connect to access admin functions (no need for dedicated server)

Legend:
Blue: FIPS 186 Authenticated Data
Red: FIPS 198 Encrypted Data
Green: OSDP Secure Channel

UFP-GW
- 8 OSDP any combination up to 8 readers
- 16 inputs
- 32 DESI devices
-64 Encrypted I/O
- 8 unsupervised inputs (Encl, AC Fail, low Batt)
- 2 network interfaces 10/100/1000 BaseT
- 16 GB onboard storage for users rules, history

DESI Details
- DESI-R is a Form C Control Relay
- DESI-S is a Solid State Control Option (No)
- DESI-IN is a 2 input device
- Each DESI carries a unique identifier to provide supply chain traceability

Field Devices
- DESI Field Devices
- Sensors
- Door Hardware
- Readers

Premise Control Unit

Centralized Security Management

The PSG Premise Control Unit (PCU) provides centralized management of intrusion detection, access control, alarm monitoring, credential administration, device status, and system configuration through a modern HTML5 web interface. Operators can securely manage security operations from any standard web browser without installing specialized client software or dedicated application servers.

Powered by PSG's embedded Command & Control (C2) platform, the PCU delivers enterprise-grade security management capabilities proven in Department of Energy (DOE) and Department of Defense (DoD) environments while remaining cost-effective for commercial, industrial, critical infrastructure, and government applications.

Universal Field Panel (UFP) with DESI

PSG's Universal Field Panel (UFP) and Digital Encrypted Security Interface (DESI) establish **trust at the source** by authenticating connected field devices, securing communications, and verifying data before it enters enterprise systems.

DESI is equally effective for new construction and retrofit deployments. In existing facilities, **DESI replaces vulnerable end-of-line (EOL) resistors** in field devices, allowing organizations to modernize to Zero Trust while preserving existing wiring, sensors, readers, and door hardware.

Unlike traditional systems that rely on implicit trust, UFP and DESI authenticate and verify connected devices at the source.

The result is a Zero Trust architecture that reduces cyber attack vulnerability while delivering trusted data for faster, more confident security decisions.

Cyber Secure by Design

The PCU incorporates a comprehensive cybersecurity framework including:

- Trusted Platform Module (TPM 2.0)
- Secure Boot
- Secure Key Storage
- PKI-Based Authentication
- FIPS Encryption Support
- STIG-Aligned Security Controls
- Authenticated Device Communications
- Verified Data Integrity

These capabilities help organizations reduce cyber risk while supporting modern Zero Trust security strategies.

Open Architecture Platform

The PCU provides a flexible, open architecture designed to support evolving security and operational requirements.

Capabilities include:

- Containerized Application Support
- MQTT Communications
- Database Services
- Edge Computing Capabilities
- Third-Party COTS and GOTS Applications
- Enterprise and Cloud Integration

This enables organizations to deploy intrusion detection, access control, OT monitoring, analytics, automation, and other mission-critical applications on a common secure platform.

Trusted Security Starts at the Edge

The PSG Premise Control Unit delivers a modern alternative to legacy physical security systems by combining intrusion detection, access control, trusted device identity, authenticated communications, and verified data in a single platform.

Simply add a PC, connect field devices, and deploy a complete Zero Trust physical security solution that establishes trust at the edge—providing authenticated device identity and verified data from the source to enterprise systems, analytics, and AI. The result is higher-quality information, faster response, and more confident security decisions.

Specifications

PM-4 Specification	Description
Power input	[10 to 48 VDC]
Power Output (for expansion modules)	[12 VDC @ 4A]
Power Consumption	PM4 [20mA @ 12VDC, 15mA @24VDC]
# Serial Channels	1 RS-485 GW uplink* (1Mbit/s, 100m distance 2 Module to Module EM connectors
PM4 Used for power expansion or remote deployment of Ems away from GW	(*default at 1Mbit/s, 100m distance, can be set to 115k for 2000')

UFP Gateway Specification	Description
# of Gateways in a system	Unlimited
# of Ems under a single gateway	16
Communication	(2x) 1000Base Ethernet
Operating System	ubuntu [Core 22.04.5 LTS]
Open Architecture Integration Services	MQTT (Message Queuing Telemetry Transport) Open API & SDK available for 3rd party integrations
Open Architecture Database Services	PostgreSQL, TPM protected Secure Storage
Open Architecture Application Hosting	Docker container services for 3rd party edge applications
# of DESI Channels	UFP-GW [16 DESI Channels] supporting [64 DESI] any mix
# DESI Inputs/Outputs (Max)	UFP-GW [128] sensor inputs or [64] control relays
# of Field Serial Ports	[4x RS-485] with two field changeable to [RS232]
	[1x RS-485] for expansion modules downlink*
	(*default at 1Mbit/s, 100m distance, can be set to 115k for 2000')
# of OSDP Readers	4 per serial port
Power Input	[10 to 48 VDC]
Power Output (for Ems /Readers)	[12 VDC @ 4 A]
Power Consumption	UFP- GW + GW Embedded EM8's [450mA @ 12VDC, 5.4 Watts] UFP-GW + Embedded EM8's [350mA @ 24VDC, 4.2 Watts]
Cyber Security Features	TPM 2.0, Secure Boot, Secure Key Storage, Signed Firmware, Antivirus, Cyber Secured O/S (RMF STIG compliant)

UFP-EM-8/16 Specification	Description
# of Expansion Modules per GW	Up to 16, any mix 4A power from GW then PM-4 for expansion
# of DESI Channels	EM-8 [8 DESI Channels] supporting [32 DESI] any mix EM-16 [16 DESI Channels] supporting [64 DESI] any mix
# of DESI Inputs / Outputs	EM-8 [Max 64] sensor inputs or [Max 32] control relays EM-16 [Max 128] sensor inputs or [Max 64] control relays EM-8 supports 2/ EM-16 supports 4
# of Field Serial Ports	RS-485 with one port optionally RS-232 Serial channels are field configurable to support Wiegand EM-8 supports 4 / EM-16 supports 8 SPDT FORM C rated
# of Power Relays	[10 A at 120 VAC] / [8 A at 30 VDC] (Resistive) [5 at 120 VAC] / [4 A at 30 VDC] (Inductive)
# of Supervised Inputs	EM-8 supports 8 legacy inputs (in lieu of DESI per port) EM-16 supports 16 legacy inputs (in lieu of DESI per port) EM-16 supports 16 legacy inputs (in lieu of DESI per port)
Supervision Ranges	Option W [100 ohm to 50k ohm] Option F *contanct factory for OEM custon configurations
# of OSDP Readers	4 per serial port
# of Legacy Wiegand Readers	1 Wiegand Reader per serial port
Power Input	[12 VDC nominal] from UFO-GW or via PM-4
Power Consumption	EM-8 [350 mA/ 4.8 Watts] / EM-16 [500mA/ 6 Watts] @ 12VDC EM-* [250mA/ 3 Watts] / Em-16 [300mA/ 3.6 Watts] @ 24VDC

Common UFP Specification	Description
# of Unsupervised Inputs	4 per device GW/EM-8/EM-16 -40 to 70C, 10-90% humidity, non-condensing (GW*)
Environmental	-40 to 85C, 10-90% humidity, non-condensing (PM4, EM8, EM16) (*contact factory for heatsink options for GW to 85C applications) 265.50mm x 107.50mm [10.45” x 4.23”] (UFP-GW/EM-16)
Form Factor	139.50mm x 107.50mm [5.50" x 4.23"] (UFP- EM-8) 52.5mm x 107.50mm [2.067” x 4.23”] (PM-4)
Mounting	DIN-Rail TS-35 standard; Wall mount optional
Surge	IEC-61000-4-2, IEC-610004-5
Cryptography: All modules	FIPS 140-3 compliant TLS, FIPS-186 FIPS-198, NIST SP 800-90B, SHA-256 OTP, ECC-P256
Safety & Perfomance Standards	UL294, UL2610, UL62638, ROHS
Communication Standards	47 CFR FCC Part 15, sub part B, Class B
Readers Tested (in pass through mode)	HID, Verdit Stealth, Identiv, Cheetah, Bridgepoint (*contact factory for latest tested inpass through list)
Supply Chain Standards	Made in the USA, NDAA/TAA/BAA Secure supply chain via authenticated inventory

SCIF Deployment Example