PROMETHEUS™
SECURITY GROUP GLOBAL

PREMISE CONTROL UNIT (SCIF APPLICATION)

SAFE | SECURE | RELIABLE

Product Overview

Integrated Intrusion Detection and Access Control system solution - leverages PSG's Universal Field Panel (UFP) with Digital Electronic Security Interface (DESI) combined with PSG's Command & Control (C2) software. The system provides local (C2) management of sixty-four I/O devices and eight access control doors. Zone secure/access (SEC/ACC) control is provided with the included LINX™ arm/disarm LCD keypad. Optional 3rd party FIPS 140-2(3) encryption (VPN Tunnels, Modems, Network Switches) are available for SCIF applications.

Features	Benefits
Embedded C2 Software	No additional Application server required
Zero Trust security model	Replaces legacy field panels and old end-of-line resistors
UFP/DESI	Secure FIPS PKI Authenticated Data - Edge to Enterprise
SEC/ACC keypad with zone control	Simple text-based touch screen zone control
TAA/NDAA compliant	Made in the USA
3rd party FIPS 140-2(3) encryption	Meets ICD-705
Integrated stand alone Intrusion Detection System	Low cost per input field panel, scalable up to 64 alarm points
Integrated stand alone Access Control System	Up to eight doors

PSG (C2) Software

PSG offers its UFP/DESI Premise Control Unit with embedded C2 software. The included HTML5 based C2 provides intrusion detection alarm configuration, command and control along with access control user credential enrollment, and portal configuration management – all available to users through their client based web browsers. The PSG C2 provides users, US Dept. of Energy (DOE) /Dept. of Defense (DOD) nuclear asset approved security software at commercial low-cost pricing.

Universal Field Panel (UFP) with Digital Encrypted Security Interface (DESI)

UFP is a new generation of open architecture secure IoT devices that provide a solution for integrated data gathering and control from the edge to the enterprise. The UFP consists of a gateway and a mixture of optional expansion modules which implement the physical security mission. The solution combines intrusion detection, access control and industrial data gathering controls into an cost-effective footprint. The UFP, combined with DESI, provides users Zero Trust FIPS level PKI encryption & authentication of data between UFP and edge devices (analog dry contact input/output) to their enterprise.

CONVERGING PHYSICAL SECURITY & ZERO TRUST

Cyber Secure
The UFP/DESI is designed with a Cyber Security mindset and delivers a rich set of current security tools including but not limited to support for Security Technical Implementation Guide (STIG), Trusted Platform Module (TPM 2.0), Secure Boot, Secure Key Storage for communications and a rich FIPS encryption (PKI) and authentication stack.

Cost Effective Event Processing and I/O Device
The UFP also brings an Open Architecture platform concept to the edge computing needs of the any security mission solution. In addition to the LPE C2 software included with the UFP, the UFP is truly open, providing database, computing and container services allowing hosting of third-party applications, both commercial-off-the-shelf (COTS) and/or government-off-the-shelf (GOTS) via MQTT communications protocol. With an already secure computing environment, the UFP enables modernization of sensing and control applications for Intrusion Detection, Access Control, and more.

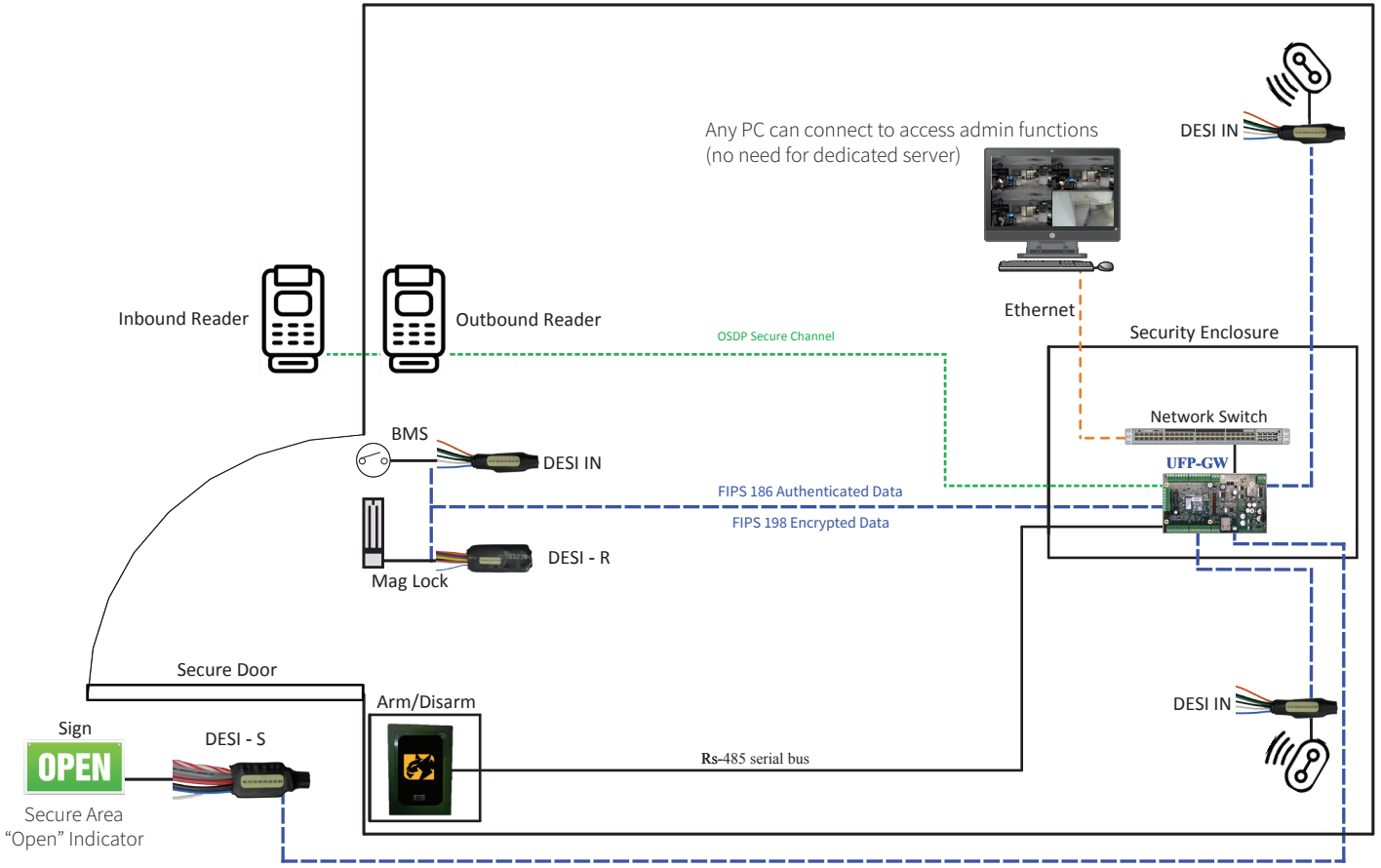
UL 2050 Commercial Central Stations
PSG's Premise Control Unit can be configured to output its data in a variety of SIA Standard internet protocols allowing for seamless ICD 705 compliant integration. Thus making it possible for the benefits of UFP/DESI to be leveraged by the operators of UL2050 central stations.

Specification	Description
# of Gateways in a system	Unlimited
Form factor	227.5mm x 104mm [9" x 4.1"]
Communications	(2x) 1000BaseT Ethernet
Operating system	Ubuntu [Core 20.10]
Open architecture database services	PostgresSQL
Open architecture database services	Docker container services for 3rd party edge applications
# of DESI ports	UFP-GW (16 DESI Ports) supporting (64 DESI) any mix
# of DESI Inputs/Outputs (max)	UFP-GW [128] sensors inputs or (64) control relays
# of field serial channels	[2x RS-485] with one field changeable to [RS-232]
# of OSDP readers	2 per serial channels are field configurable to support Wiegand
# of legacy Wiegand readers	1 Wiegand reader per serial channel
Power input	[10 to 48 VDC]
Power output	[12 VDC @ 4 A] (for EMs)
Power consumption	6 Watts (exclusive of expansion modules)
Cyber security features	TPM 2.0, secure boot, secure key storage, signed firmware, cyber secured O/S (RMF STIG compliant

Certifications and Approvals	
Environmental	-40 to 85 C, 10-90% Humidity
Surge Suppression	IEC-61000-4-2
Cryptography; All modules	FIPS 140 compliant TLS, FIPS-186, FIPS-198, NIST SP 800-90B, SHA-256, ECC-P256, TLS
Safety	UL294, UL1076, UL60950, ROHS
Communication	47 CFR FCC part 15, sub part B, class B
Supply chain	Made in USA, TAA/BAA: Secure supply chain via authenticated inventory

General Specifications	
# of unsupervised inputs	4 per device GW/EM-8/ EM-16
Mounting	DIN-Rail TS-35 standard; wall mount optional

NOTIONAL SCIF PSG BLOCK DIAGRAM



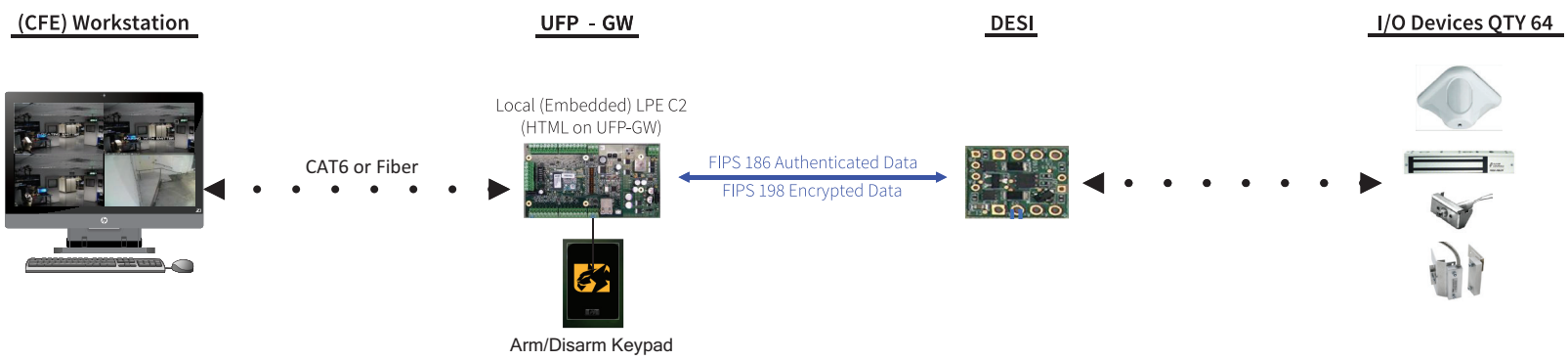
Legend:

Blue: FIPS 186 Authenticated Data

Red: FIPS 198 Encrypted Data

Green: OSDP Secure Channel

PREMISE CONTROL UNIT (PCU)



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

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

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

Filename: Scene Authentication Flow Diagram 5-25-21 CS TT.vsdx