PROMETHEUS®
SECURITY GROUP GLOBAL

GOVERNMENT SOLUTION (SCIF)

SAFE | SECURE | RELIABLE

Product Overview

PSG's Universal Field Panel (UFP) is designed to be the keystone for physical security operations of highly secure SCIF's for permanent buildings and temporary modular structures. 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 extremely cost-effective footprint. The UFP leads the way to the cloud with Zero Trust authenticated and encrypted data.

Cyber Secure

The UFP product line 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 provides a rich FIPS encryption (PKI) and authentication stack. When combined with The Digital Encrypted Security Interface (DESI) a revolutionary approach for upgrading current security and control interfaces for gathering authenticated, confidential data from the edge.

Cost Effective SCIF Event Processing and I/O Device

The UFP also brings an Open Architecture platform concept to the edge computing needs of any security mission. Instead of proprietary field panels, the UFP is truly open, providing database, computing and container services allowing hosting of third-party applications (COTS/GOTS). With an already secure computing environment, the UFP enables modernization of sensing and control applications for SCIF related Intrusion Detection, Access Control, and more.

Features

- **Meets ICD-705**
- **Secure FIPS PKI Authenticated Data from the Edge to Enterprise**
- **COTS low cost per input field panel**
- **Zero Trust security model**
- **Replaces legacy field panels and 80-year-old end-of-line resistors**
- **TAA/NDAA compliant**

Any Command and Control (C2)

PSG offers its UPF/DESI C2 API, to any C2 system manufacturer allowing them to easily develop their own interface to UFP allowing for direct two-way command, control, and communications between UFP and their own C2 system. In this way, C2 manufacturers can benefit from the power and low-cost benefits of PSG's UFP allowing for FIPS level PKI encrypted data from edge devices including motion sensors, door sensors, secure access devices and access control readers to their enterprise.

UL 2050 Commercial Central Stations

PSG's UFP can be configured to output its data in a variety of SIA Standard internet protocols allowing for seamless ICD 705 compliant integration with UL2050 central stations making it possible for the benefits of UFP to be leveraged by the operators of UL2050 central stations.

PROMETHEUS®
SECURITY GROUP GLOBAL

Specifications	Discription
# 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 complient

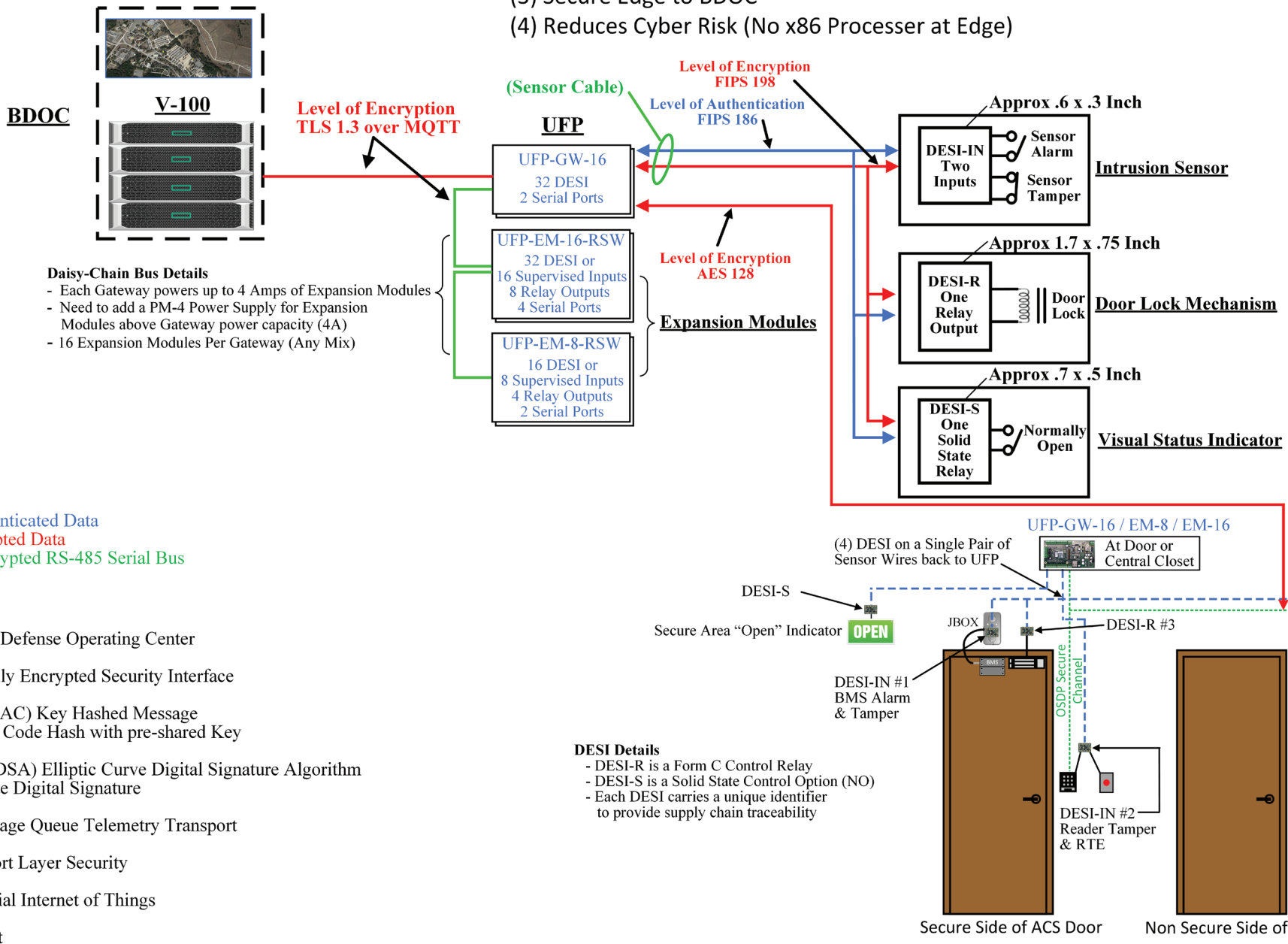
Certifications and Approvals	
Environmental	-40 to 85 C, 10-90% Humidity
Surge Suppression	IEC-61000-4-2
Cryptography; All modules	FIPS 140 compliant TLS FIPS-186 FIPS-198 NIST SP 800-90B SHA-256 ECC-P256 TLS
Safety	UL294 UL1076 UL60950 ROHS
Communication	47 CFR FCC part 15, sub part B, class B
Supply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

DESI Authentication and Encryption from the Edge Flow Diagram

DESI Ensures Authenticated and Confidential Data from the Edge Sensors and to Control Outputs

(1) Open Architecture IIOT
(2) Authenticated and Confidential
(3) Secure Edge to BDOC
(4) Reduces Cyber Risk (No x86 Processer at Edge)



Acronyms:

- BDOC – Base Defense Operating Center
- DESI – Digitally Encrypted Security Interface
- FIPS 198 (HMAC) Key Hashed Message Authentication Code Hash with pre-shared Key
- FIPS 186 (ECDSA) Elliptic Curve Digital Signature Algorithm used to generate Digital Signature
- MQTT – Message Queue Telemetry Transport
- TLS – Transport Layer Security
- IIOT – Industrial Internet of Things
- RTE – Request

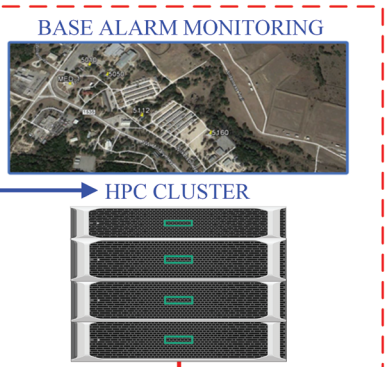
NOTIONAL SCIF PSG BLOCK DIAGRAM

HPC Hosts GOTS/COTS Virtualized Solutions:

- Any C2: PICARD, JIGSAW, ARES AVERT/VIDSYS, Vindicator, LPE, Advantor, etc.
- Any Sensor/IDS/ACS/Cameras: WISP, FLIR, Ghost Robotics, Digital Force Technologies, Drones, Software House, Identiv, etc.

Features:

- ATO, Cyber RMF, Inv. & Mgmnt.
- High Performance Computing (HPC)
- Elastic Stack Computing
- HOT - Low Cost Sensing the Base
- VICADS VMS V100 - "All Things Video"
- BDOC, Local Secure Data Lake
- AI/ML Processing
- 3rd Party Analytics/Data Mining



UL 2050 Compliant
Not Required but Meets Standards

FIPS 140-3 Device

VLAN

UnTrusted

FIPS 140-3 Device

FIPS 140-3 Device

Outside SCIF

***ANY* VIDEO**
Scene Authentication (as desired)

Any Camera

ANY C2

SCIF

UFP

UFP-GW-16
32 DESI
2 Serial Ports

UFP-EM-16-RSW
32 DESI or
16 Supervised Inputs
8 Relay Outputs
4 Serial Ports

UFP-EM-8-RSW
16 DESI or
8 Supervised Inputs
4 Relay Outputs
2 Serial Ports

Expansion Modules

UFP-GW-16 / EM-8 / EM-16

At Door or Central Closet

(4) DESI on a Single Pair of Sensor Wires back to UFP

DESI-S

Secure Area "Open" Indicator

OPEN

JBOX

DESI-R #3

DESI-IN #1
BMS Alarm
& Tamper

OSDP Secure Channel

OSDP Secure Channel

DESI-IN #2
Reader Tamper
& RTE

DESI-IN #4
Reader
Tamper

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

Secure Side of ACS Door

Non Secure Side of ACS Door

Legend
Blue = Advanced Technologies
Red = Authenticated Data - Edge to Enterprise, (DESI & Scene Authentication)
Black = Current Technologies/Infrastructure

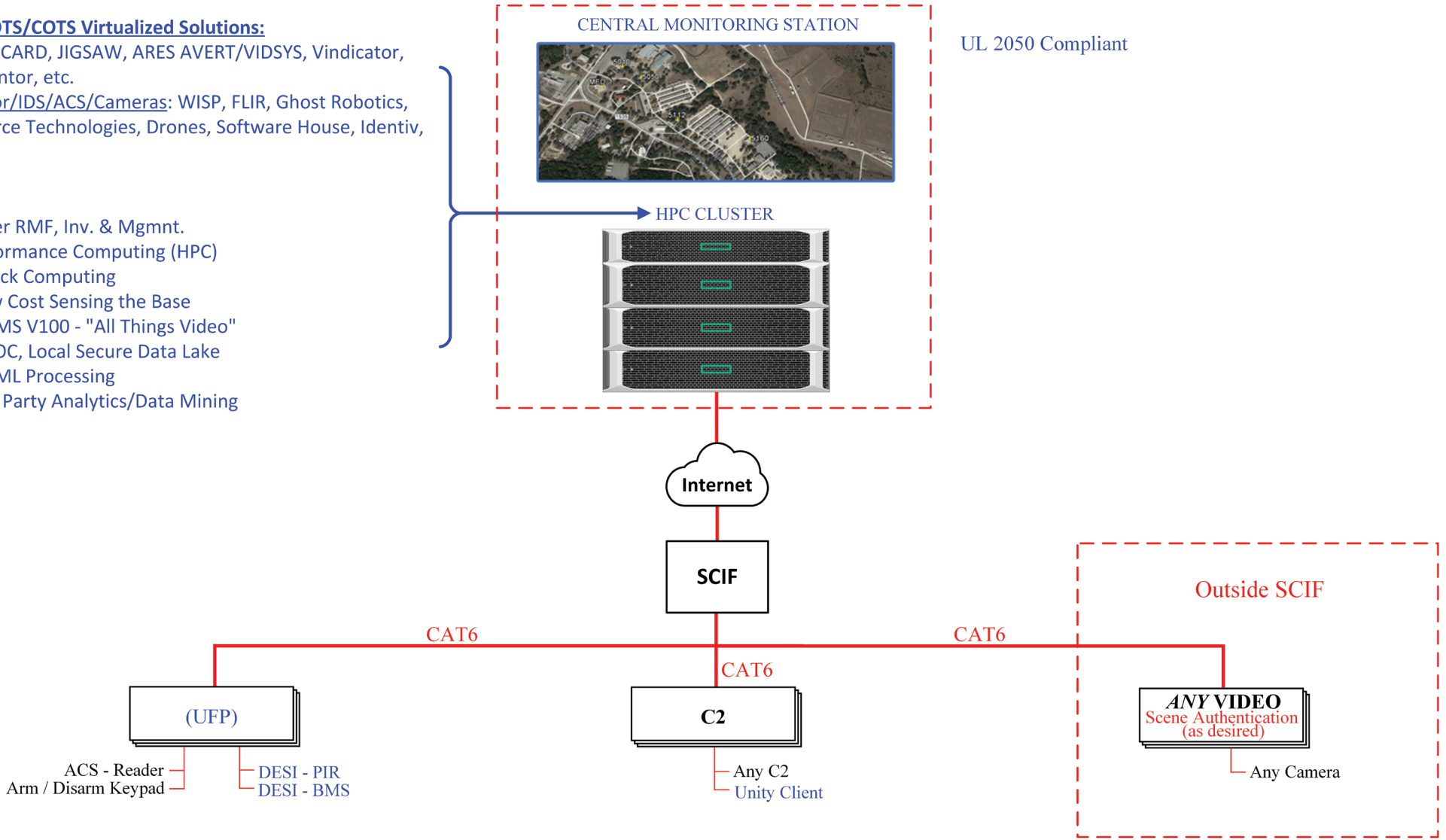
NOTIONAL COMMERCIAL PSG BLOCK DIAGRAM

HPC Hosts GOTS/COTS Virtualized Solutions:

- Any C2: PICARD, JIGSAW, ARES AVERT/VIDSYS, Vindicator, LPE, Advantor, etc.
- Any Sensor/IDS/ACS/Cameras: WISP, FLIR, Ghost Robotics, Digital Force Technologies, Drones, Software House, Identiv, etc.

Features:

- ATO, Cyber RMF, Inv. & Mgmnt.
- High Performance Computing (HPC)
- Elastic Stack Computing
- HOT - Low Cost Sensing the Base
- VICADS VMS V100 - "All Things Video"
  - BDOC, Local Secure Data Lake
  - AI/ML Processing
  - 3rd Party Analytics/Data Mining



Legend

Blue = Advanced Technologies
Red = Authenticated Data - Edge to Enterprise, (DESI & Scene Authentication)
Black = Current Technologies/Infrastructure