



OWL Cyber
Defense

Defending the Tip of the Spear: On-Base OT Cybersecurity

Dr. James Taylor

Defending On-Base Operational Technology

On-base Operational Technology (OT) is under unprecedented attack from multiple vectors.

This includes attacks on the bases, facilities, equipment, etc. which can reduce and/or cripple our operational capabilities.

Nation state level threats are actively probing and infiltrating these OT networks.



Infrastructure Truths

There is a general acknowledgment in the Air Force today that the air base itself is a “weapons system.”

As former Secretary of the Air Force Dr. Heather Wilson stated with the release of the Infrastructure Investment Strategy (I2S), “in the Air Force, we fight from our bases... the places we call home are also the platforms from which we project combat power.”

INFRASTRUCTURE TRUTHS

- 1. Infrastructure is an integral component of air, space, and cyber operations.**
Based on the lessons of history and the guidance of current doctrine, physical infrastructure inside and outside the air base fence-line is an integral component of success in air, space, and cyberspace.
- 2. Quality infrastructure requires investment.**
Quality infrastructure that enables the mission requires time and money to build, maintain, and protect.
- 3. Critical infrastructure systems must be sustainable and resilient.**
Infrastructure is a network of systems that must be sustainable and resilient, as problems at one node of the system can cause cascading effects elsewhere.
- 4. Neglecting infrastructure puts the mission at risk.**
If the infrastructure fails, the mission fails...and costs to repair and maintain physical infrastructure only compound with time.
- 5. Infrastructure is for all leaders.**
All leaders must be aware of the status and capabilities of infrastructure systems within their span of control, from military family housing to runways, maintenance facilities, and operations centers.

Source - Infrastructure Truths for Air, Space, and Cyberspace
Air & Space Power Journal



On-base Operational Technology (OT) Infrastructure

- Communications
- Command & Control Signals
- Logistics
- Power Infrastructure
- Aircraft Maintenance Equipment
- Building Systems & other Facilities-Related Control Systems (FRCS)

For example: Cyber and remotely piloted Infrastructure aircraft (RPA) operations require facilities with resilient and reliable building systems (e.g., air conditioning to keep servers from overheating and reliable backup power)



Power plant operations at Eielson AFB, Alaska



Identifying Points of OT Cyber Vulnerability

Focus on Network Edge:

Exposed endpoints and infrastructure

- Supply chain & 3rd party attacks
- Denial of Service (DoS/DDoS)
- Zero-day & Advanced Persistent Threats (APT)
- Electronic Warfare (EW)



CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications



Securing the Edge

Secure the network edge, you can control what's coming in and ensure you can continue to operate in the face of an attack.

Methods of OT Cybersecurity:

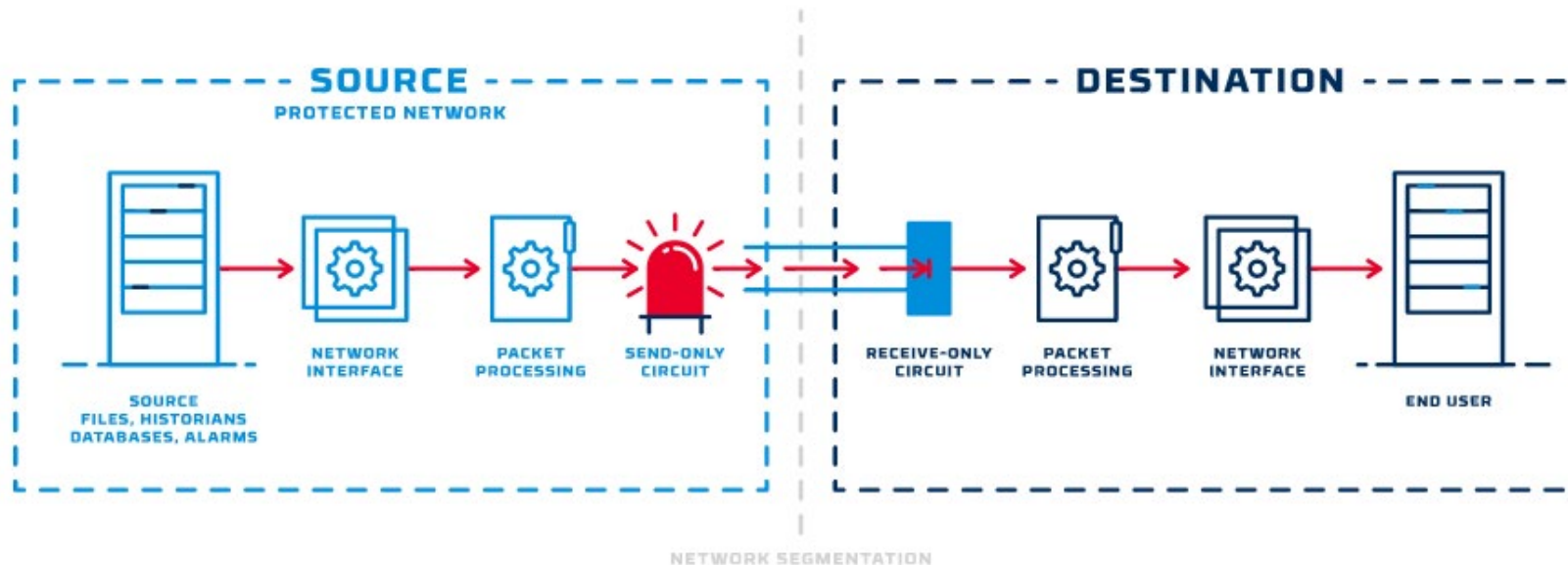
- Firewall / Industrial Firewall
 - Zero Trust Authentication
- } *Software-based Security*
-
- Air Gap
 - Data Diodes & OWT
- } *Hardware-based Security*
-
- Cross Domain Solutions
- *Software & Hardware-based Security*



What is a Data Diode?

A **diode** is an electronic component that physically only allows current to flow in one direction.

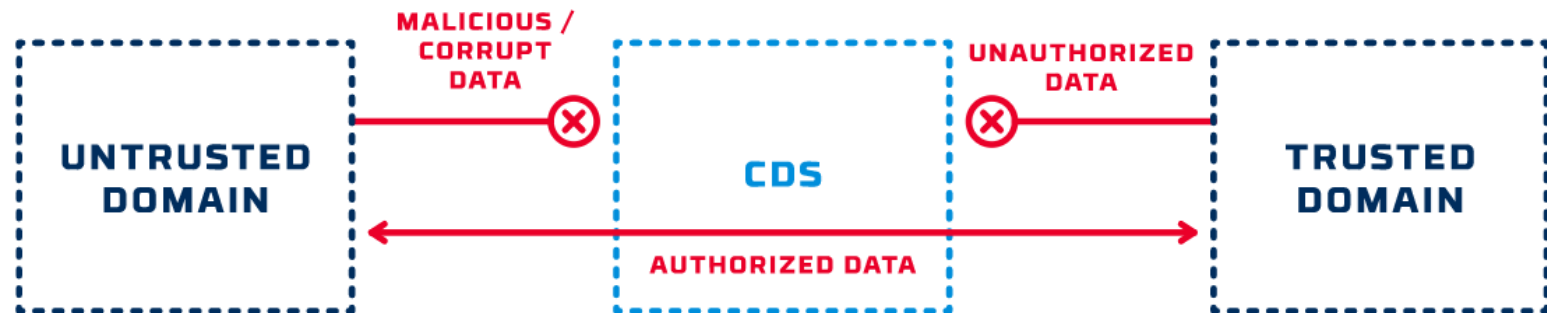
A **data diode** is a hardware-based electronic device, designed with two separate circuits – one send-only and one receive-only – which physically constrains the transfer of data to one direction only, forming an "air gap" between the source and destination networks.



What is a Cross Domain Solution?

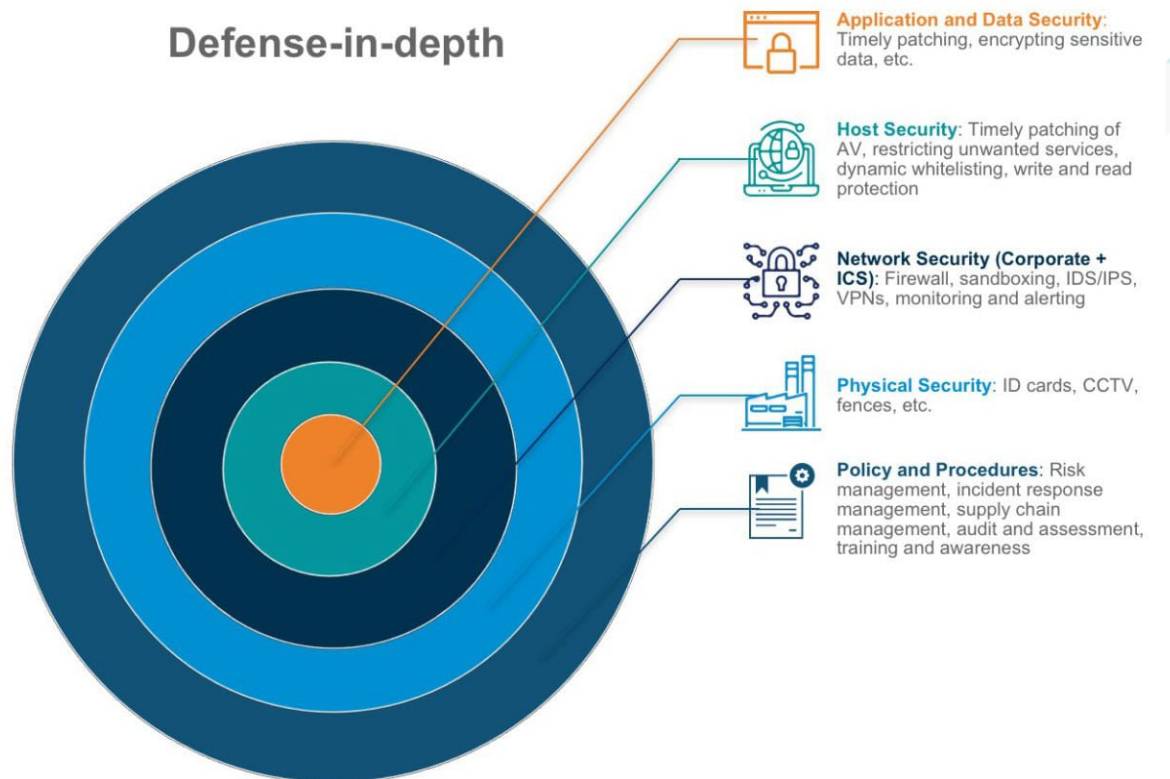
- Content Inspection & Sanitization
- Redundant, Independent Filtering
- HWE Separation & Protocol Break
- Trusted Operating System (TOS)
- Separate Transfer & Management
- Mandatory Access Control (MAC)
- Logging & Quarantine (SIEM/DCO)
- User Identification & Authentication
- Self-Protection Mechanisms
- Secure Failure

A controlled interface with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. Provides the ability to manually and/or automatically access and/or transfer information between different security domains



Defense in Depth

- Defendable Environment
- Edge Security
- Policy & Configuration
- Patch Management
- Application Whitelisting
- Authentication / Zero-Trust
- Security Monitoring & Defensive Cyber Operations
- Data Encryption & Tokenization



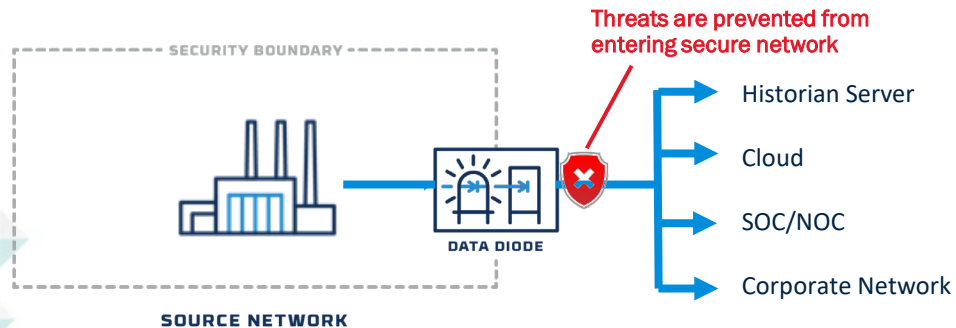
Source – POWER Magazine



Critical Infrastructure Use Cases

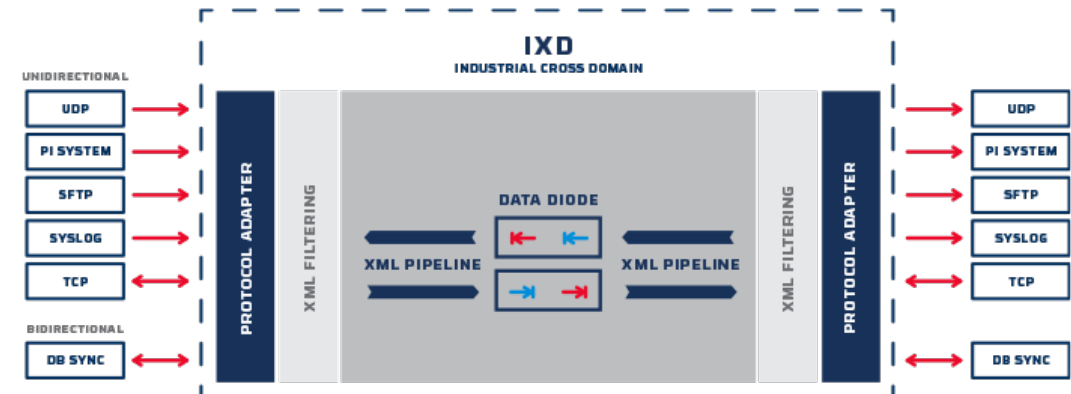
Secure Remote Monitoring

- One-way data transfers into or out of a secure network

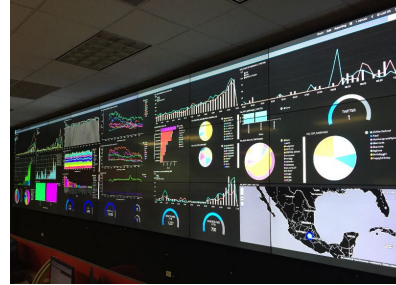


Secure Command & Control

- One-way and bidirectional connections between two domains at differing security levels



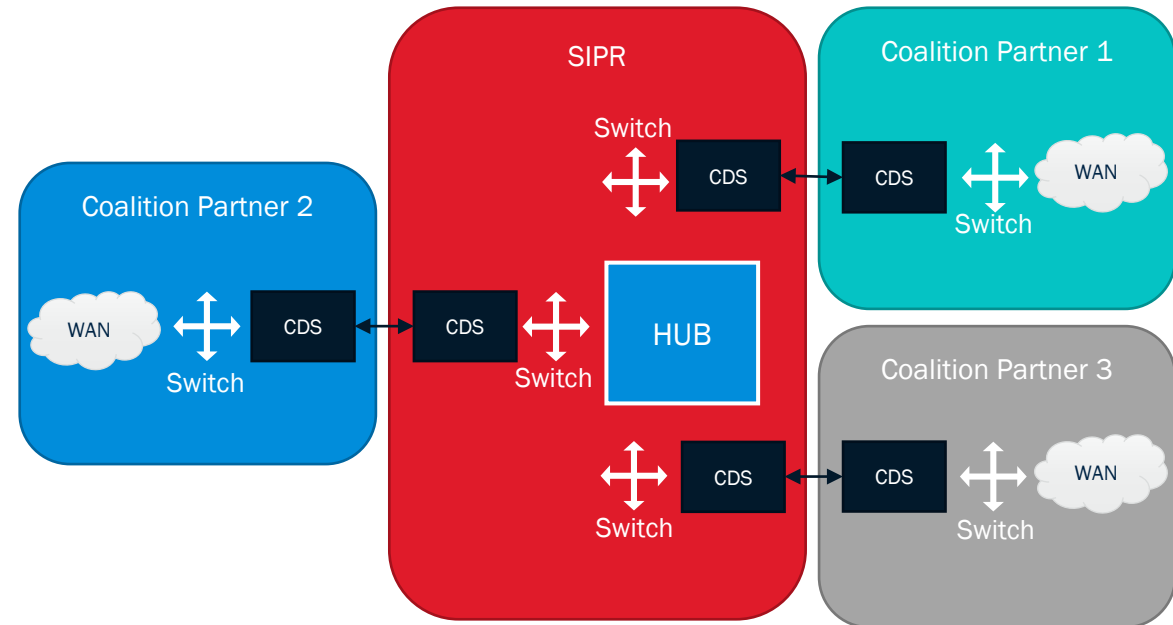
Critical Tactical Communications Network



Strategic Tactical Communications Network

Real-time coalition voice and video collaboration network for operational communications and command.

- Enabled secure voice and video telecommunication across multiple coalition partner networks.
- Provided advanced voice and video data filtering, dramatically lowering risk to classified network.
- Single implementation significantly lowered costs compared to previous copper infrastructure.
- Eliminates the need to manage multiple networks across the site(s) and require multiple endpoints at each desk.



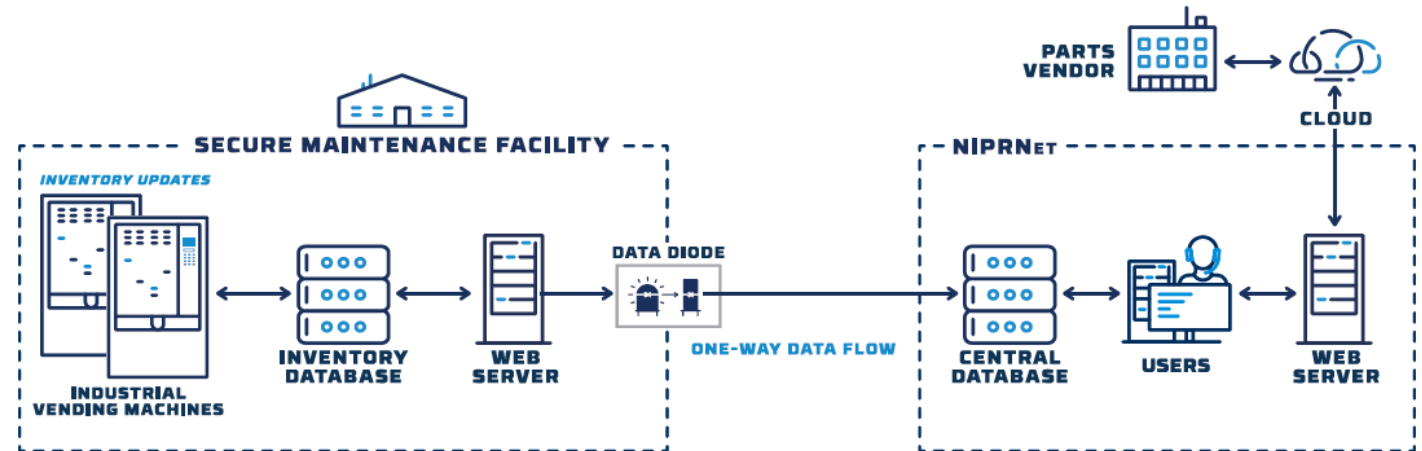
Air Base Maintenance Vending Machines

- Replaced inefficient manual processes for inventory management and communication with secure, automated parts inventory unidirectional data transfer to 3rd party vendors via data diodes.
- Resulting solution greatly increased efficiency of inventory management and decreased time to repair and maintain aircraft without increasing risk to the AFB facility network.
- Preserved effective “closed” architecture at the maintenance facility network boundary.



United States Air Force Base

Manager for the maintenance of a wide range of aircraft, engines, missiles, software and avionics and accessories components.

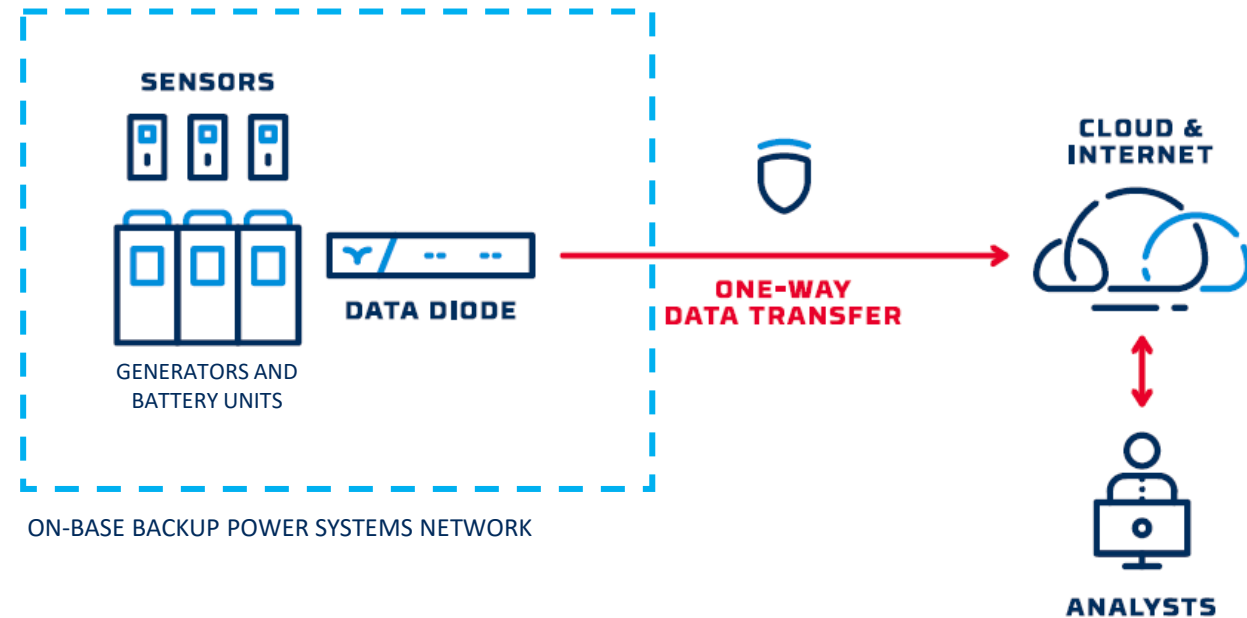


Backup Power Systems - 3rd Party Monitoring

- Timely, actionable data availability enabled real-time grid performance optimization and energy trading
- Effective network segmentation helped to ensure absolute cyber threat protection for the battery units
- Cloud analytics on IIoT monitoring and sensor data provided increased battery longevity and reliability
- Minimal maintenance requirements dramatically reduced upkeep time and costs



Transmission System Operator
Regional electric reliability authority responsible for power distribution and load balancing



Thank you!



Questions?

