Why Consider Data Diodes for Substations?

(a utility perspective)

Jodi A. Jensen

MRO 2021 Security Training – 10-4-2021

Western Area Power Administration

Objective: Get Valuable Substation Data
(Without External Routable Connectivity)

1) Substation data is unavailable in at many substations
   - Synchrophasor data
   - OT cyber monitoring data
   - Fault data

2) External Routable Connectivity (ERC)
   1) Currently many of WAPA's substations do not have ERC
   2) ERC would add 37 new NERC CIP requirements to these OT devices
   3) ERC would add new attack paths into the OT environment

WAPA Substation Data Diode Pilot

- Pilot Data Diode Technology
  - Fault Distance Use Case
    - Considering initial pilot in a lab
    - Then in substation
  - Synchrophasor and OT Cyber Monitoring Use Cases
    - Two substations
    - Different regions of WAPA - to glean feedback from multiple teams
  - Re-evaluate Substations that have ERC
    - Could we eliminate the ERC and retain desired functionality?
    - Bidirectional Diodes

Electric Sector Interest

- EPRI is considering a lab implementation of data diodes
  - looking for affordable solutions that are scalable
- NATF OT Network Practices Group Discussion
  - 13 responding entities had substations with no ERC
  - 4 responding entities have implemented a diode in a substation
  - 10 responding entities had interested in diodes for substations

Industry Trends to Consider

- FERC NOI – Potential Enhancements to the Critical Infrastructure Protection
  - Identified Gap in addressing Attack Containment
  - Data Diodes can enable Containment Strategies
- Consequence Driven Cyber Informed Engineering
  - Identify Strategies to reduce the Consequence of an Attack
  - Data Diodes can enable Containment Strategies
- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
  - Draft DHS Response mentions data diodes
- DOE/DHS Recommended Cybersecurity Practices for Industrial Control Systems
  - Includes the use of data diodes as a recommended practice whenever possible
  - https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

Understanding the Cybersecurity Role of Data Diodes in Providing Non-routable Substation Connectivity and Protection

OWL
Cyber Defense

Agenda:

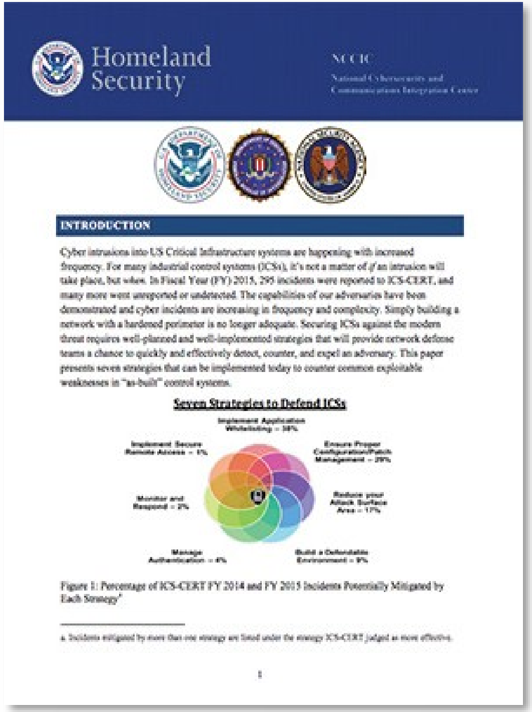
1. Data diodes – how they work
    1. creating the airgap
    2. Protocol breaks
2. Use Cases
3. Future of data diodes – why hardware cybersecurity is importnat
    1. Smaller, faster, cheaper
    2. Better security through protocol verification & content inspection
4. Scalability and pricing – from single device to the whole perimeter
    1. Form factor
    2. Scalability
    3. Licensing
    4. Pricing

Addressing 7 Common Myths:

1. **Data Diodes are expensive**
2. **Complicated to deploy**
3. **Data diodes are limited to one-way use cases**
4. **Data diodes consist of multiple boxes and flanking servers**
5. **Data diodes only support a single flow or data protocol at once**
6. **Firewalls can operate as a one-way data diode**
7. **Data diodes are hard/expensive to maintain**

Implementing DHS Recommendations

- Reduce/Eliminate Connections in/out of the Network
- Convert Two-Way Connections to One-Way out of the Plant
- Convert Two-Way Connections to One-Way into the Plant
- Secure Remaining Two-Way Connections


Homeland Security

NCCIC

National Cybersecurity and Communications Integration Center

INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

Seven Strategies to Defend ICSs

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as most effective.

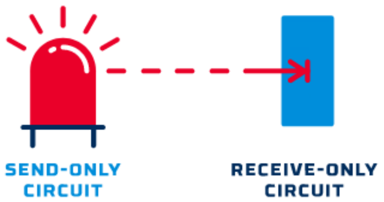
1

The air gap

- **Hardware enforced one-way data path**
- **Transmitter sends but cannot receive**

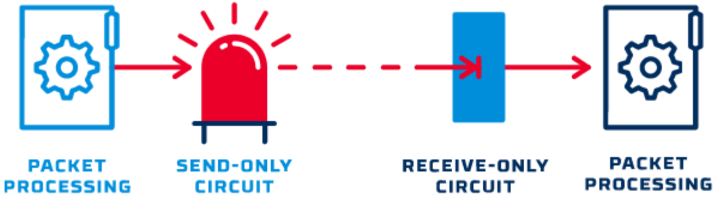
The air gap

- **Receiver has no ability to send data**
- **Data cannot flow “backward”**



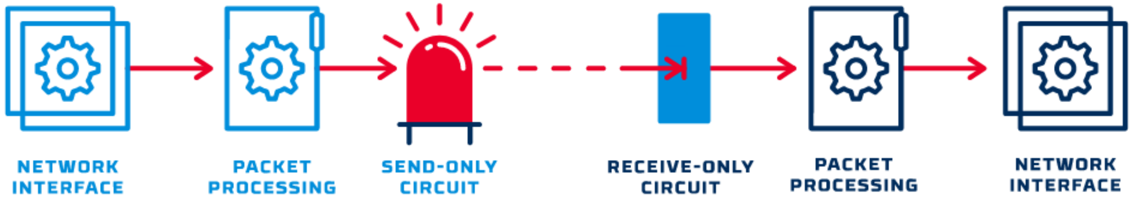
The protocol break

- Packet headers removed before sending
- Only packet payloads pass across air gap
- Packets rebuilt with new headers
- No send-side routable information
- Double-blind transfers
- ERC
- IRA



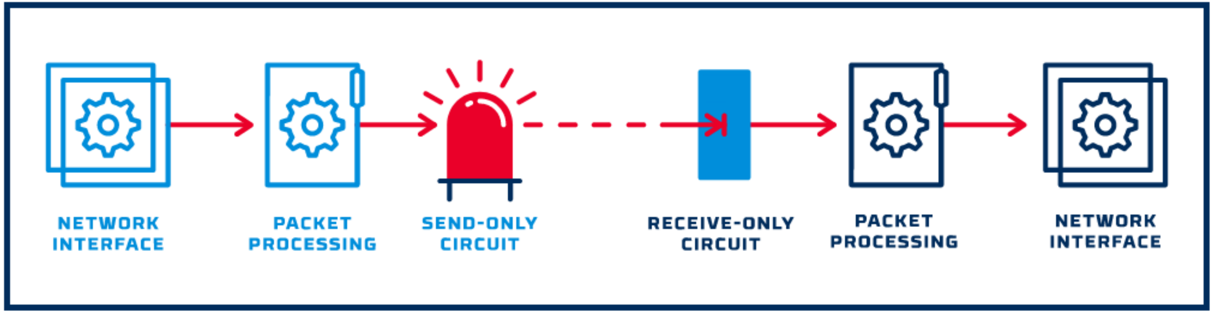
The network interface

- **Source-side proxy validates incoming data then translates data for transmission across air gap**
- **Receive-side proxy reverses the process and initiates new session with downstream resources**
- **Enables support for protocols (like MQTT) that are inherently two-way**



The secure environment

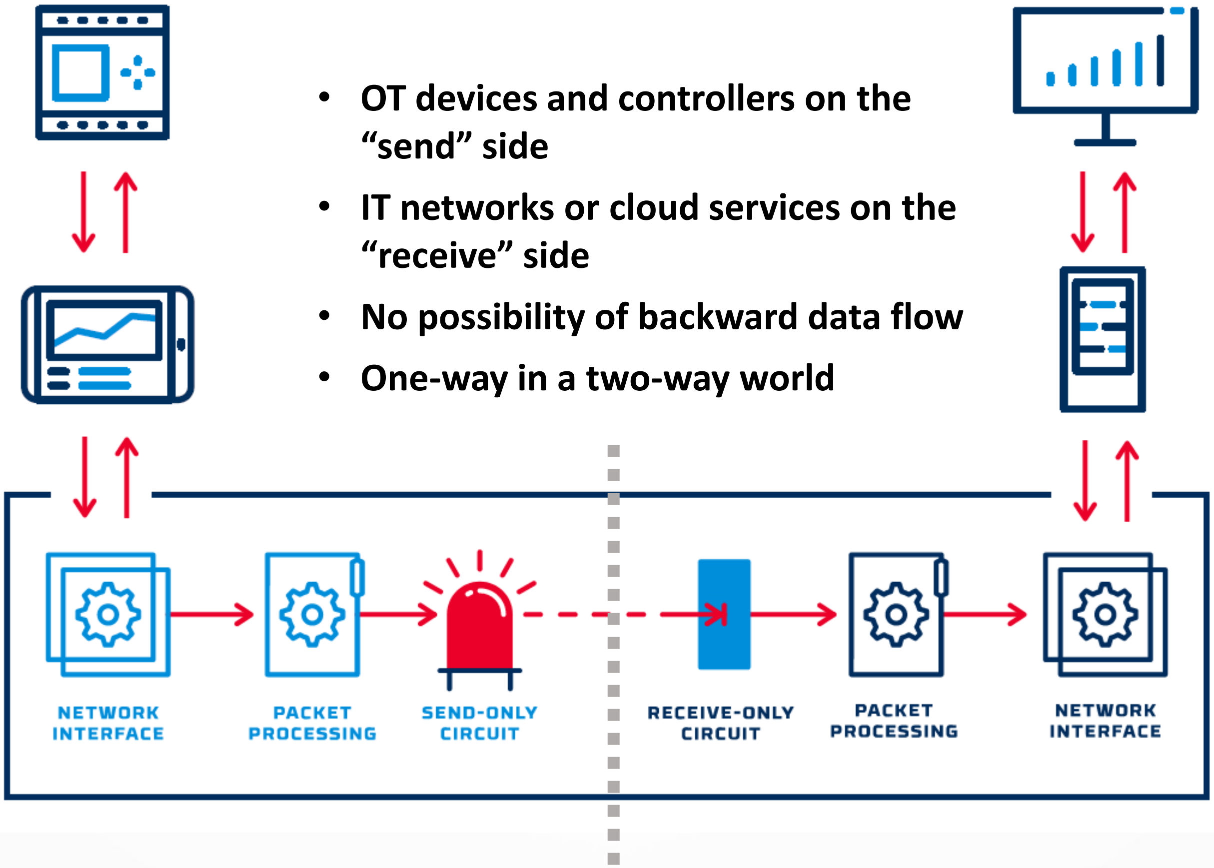
- Diodes are deployed in secure, high-performance appliances
- Secure operating systems
- Little to no maintenance required
- Often run for 10+ years continuously



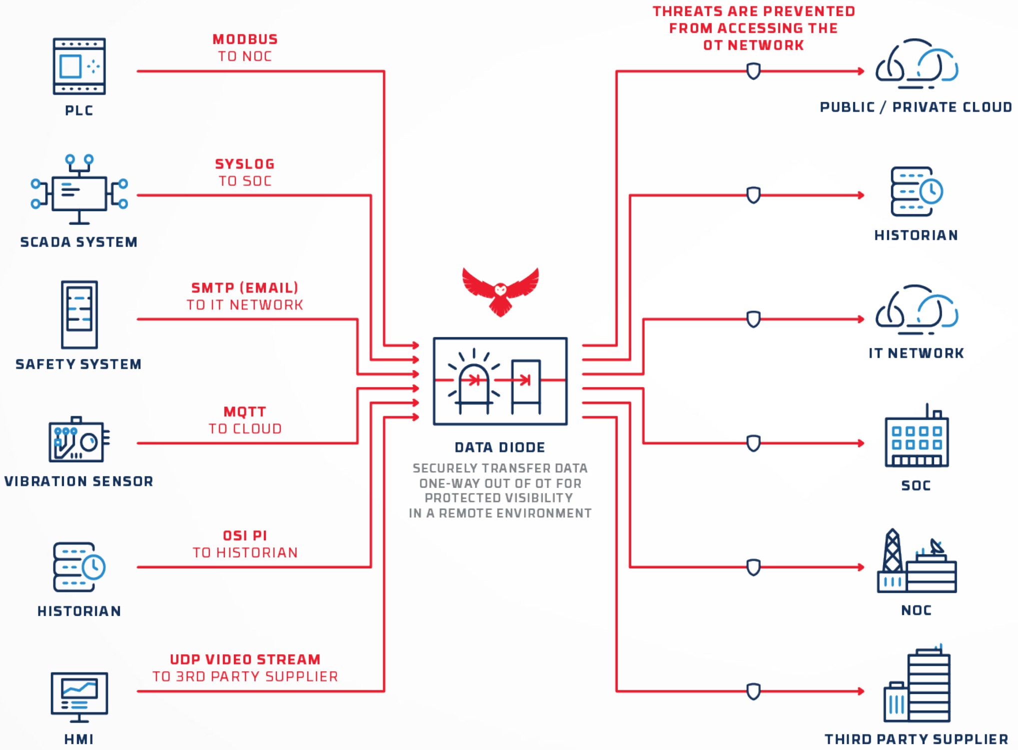
OWL Cyber Defense

The data diode in action

- OT devices and controllers on the “send” side
- IT networks or cloud services on the “receive” side
- No possibility of backward data flow
- One-way in a two-way world



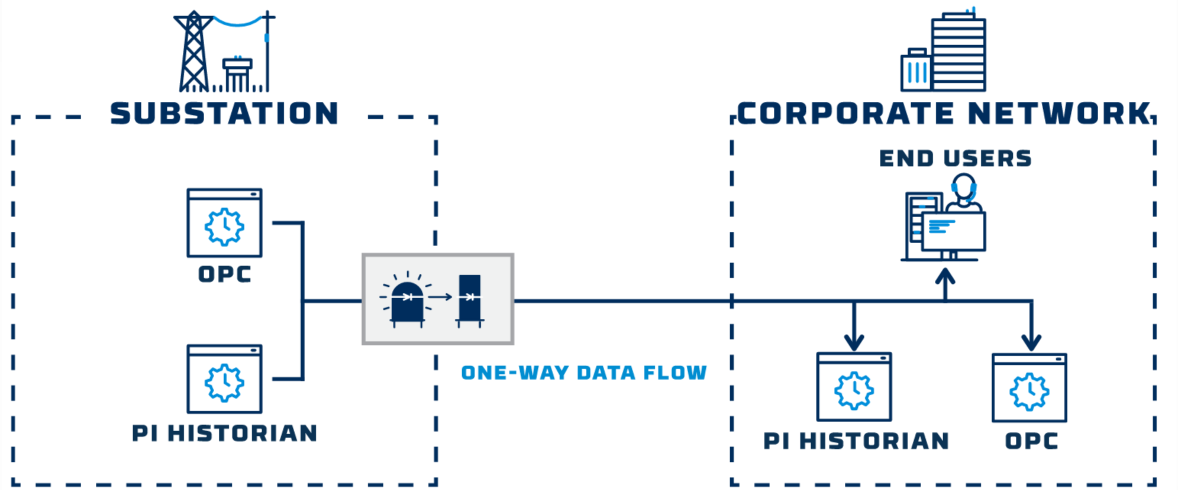
Data diode use cases



- **Deployed widely in the Bulk Electric System (100+ Owl implementations)**
- **Protect operator assets and exclude them from being categorized as Critical Cyber Assets**
- **Transfer multiple data types– historian, syslog, performance, alarms, events, remote HMI**

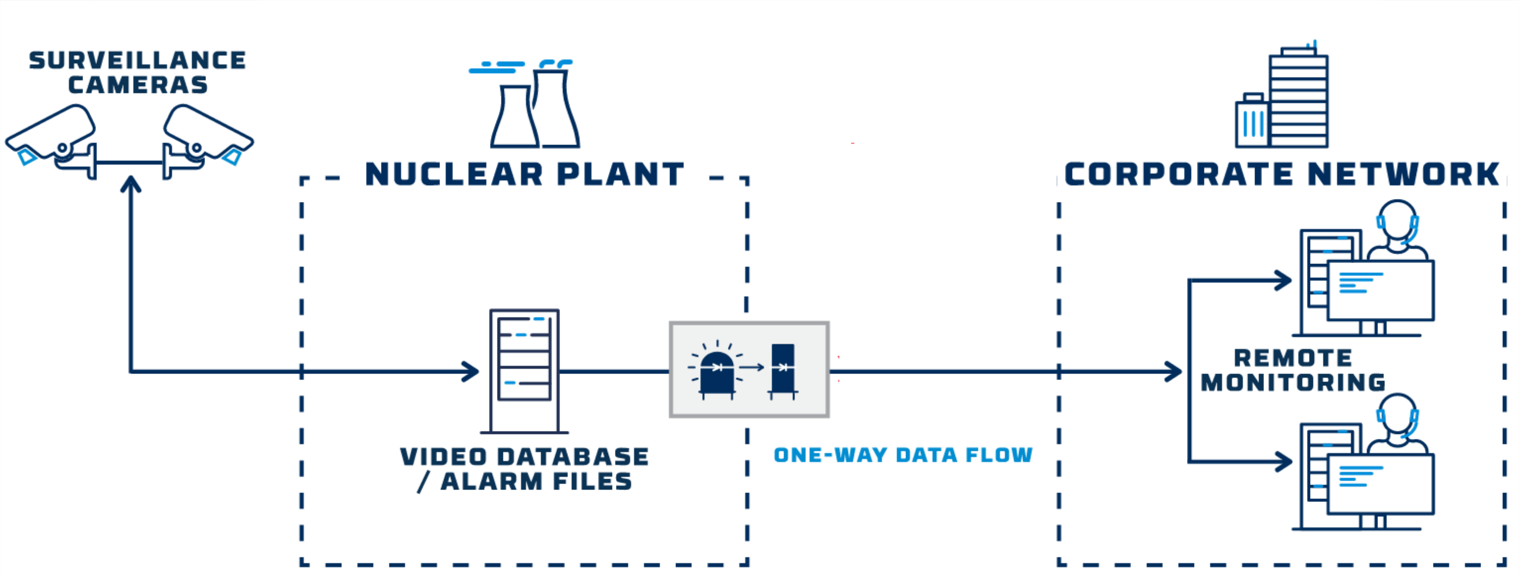
OWL Cyber Defense

Use Case: Historian Replication



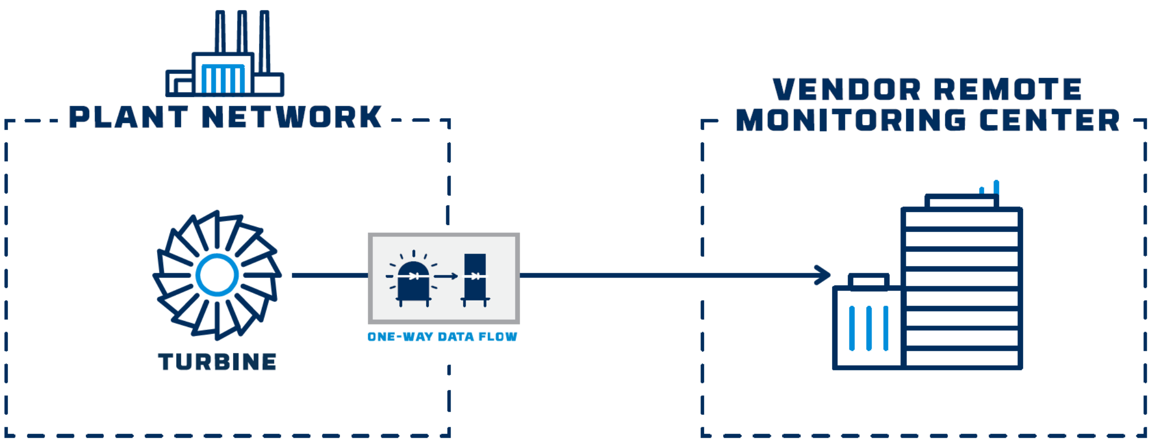
- NERC CIP prohibits external connectivity into substation OT network
- Corporate network users need access to the OT performance data
- Replication of historian data from OT to IT/cloud quickly and safely unlocks performance gains

Use Case: Security Monitoring



- **Surveillance and alarm data is needed at remote monitoring center to ensure physical security**
- **NRC Regulatory Guide 5.71 prohibits external connectivity into nuclear plant OT network**
- **Data diodes transfer camera and alarm data without creating inbound connection**

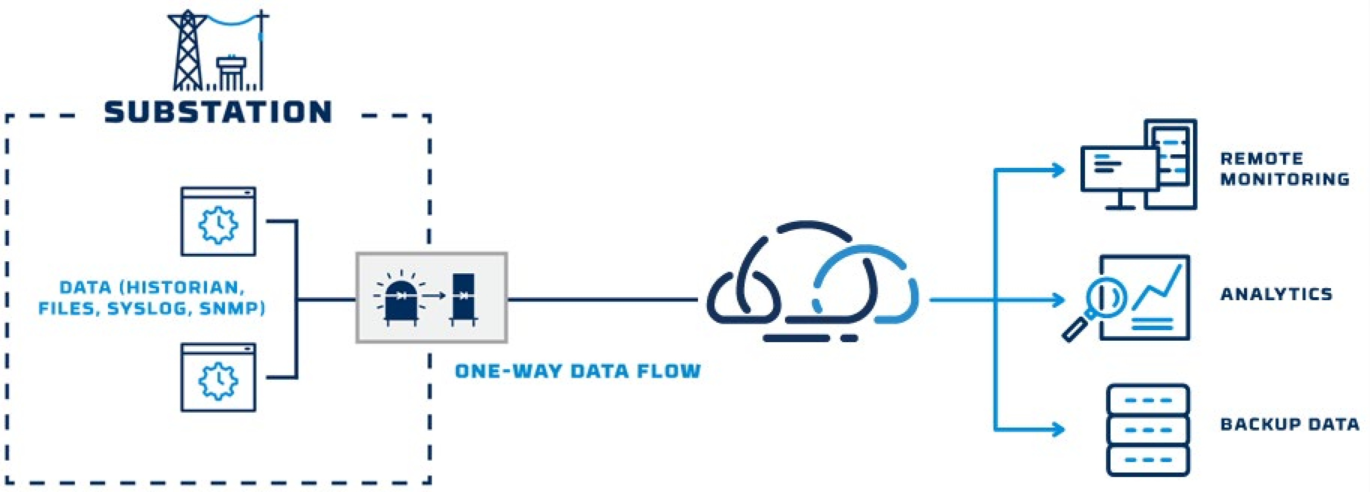
Use Case: Vendor Remote Monitoring



- **Many OT vendors offer enhanced services that depend on remote asset monitoring**
- **Plant and substation operators must maintain air-gapped protection**
- **Data diodes transfer condition and performance data without creating inbound connection**

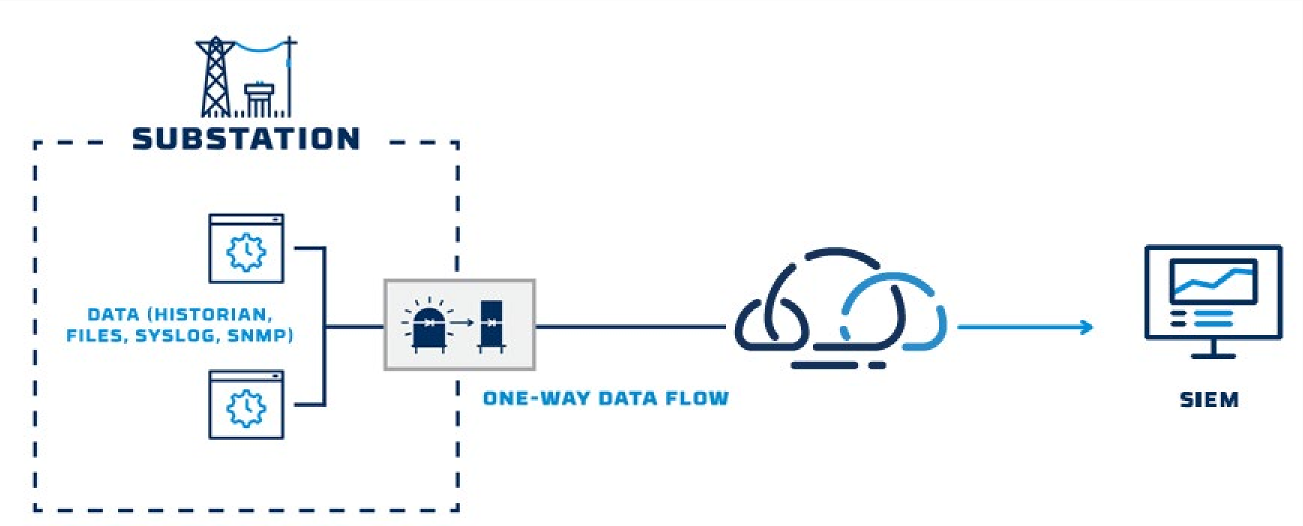
OWL Cyber Defense

Use Case: Cloud Enablement



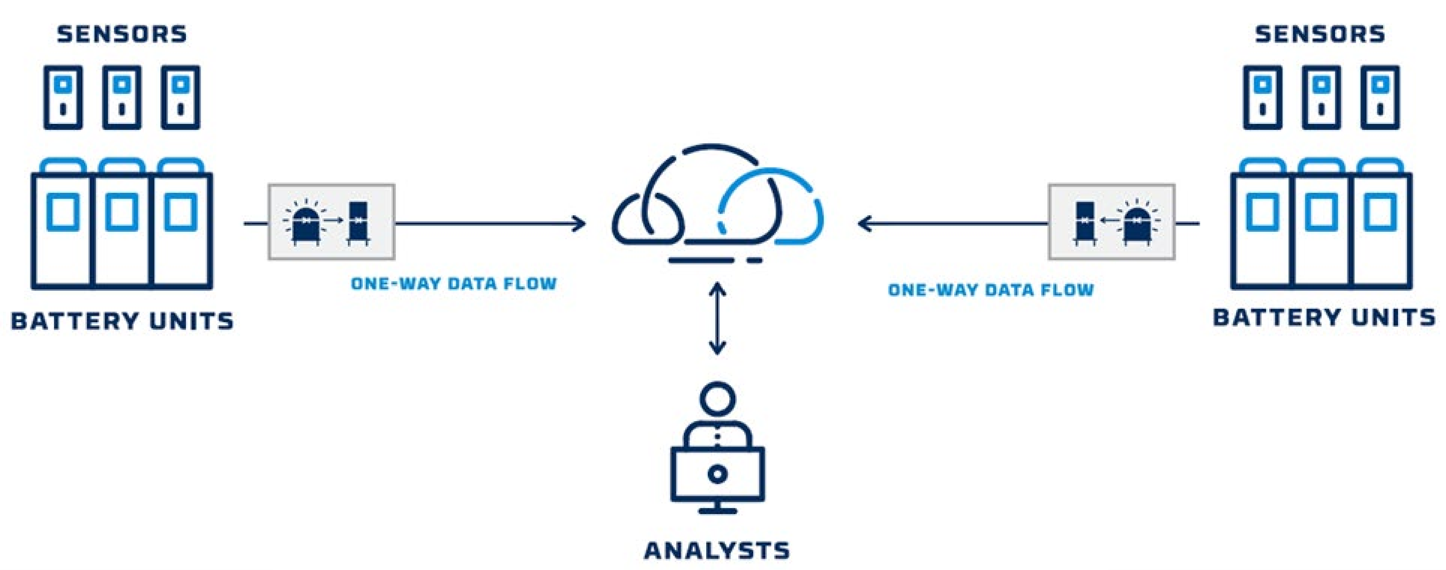
- **Cloud connectivity helps operators optimize operations and take advantage of new capabilities**
- **Applications include predictive maintenance, OEM analytics, digital twins, and operational performance**
- **Integrations available for many data types/protocols including MQTT, FTP/SFTP, Modbus, OPC DA, OPC UA, AMQP, raw network packet**

Use Case: Threat Hunting



- Proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools
- Diodes transfer data to the IT data store, SOC/NOC or cloud for monitoring and analysis
- Data types include syslog, log files, SNMP, and network raw packet data flows

Use Case: Battery Monitoring

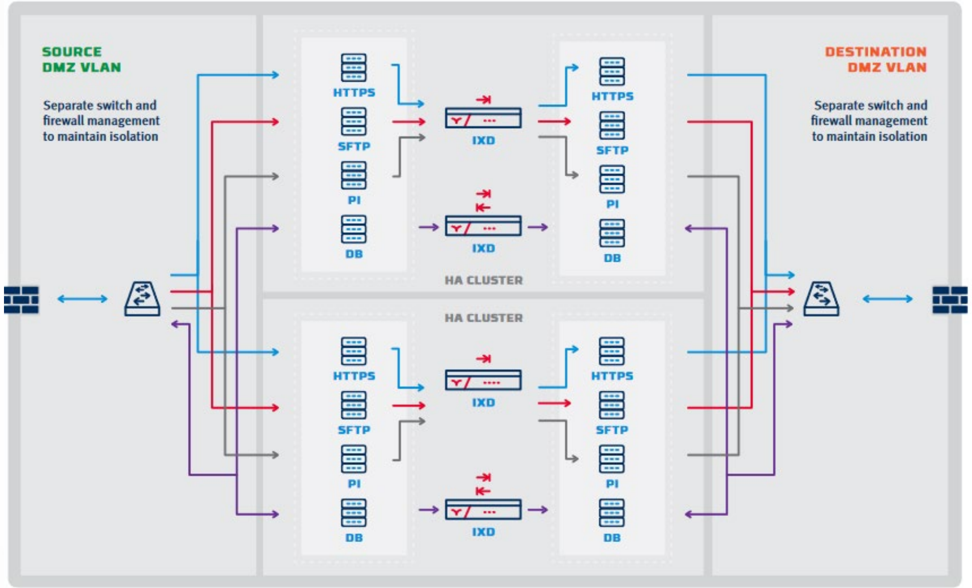


- **Status, performance, and environmental data monitoring is needed to enable energy sales and grid connectivity from distributed battery-based power banks**
- **Periodic VPN-based data transfer does not meet operational needs**
- **Data diodes enable real-time secure data transfer with minimal maintenance requirements**

Use Case: IEC104/DNP3 monitoring

- **Power transmission and distribution operators have a need to secure communications between master control stations and their slaves**
- **However, IEC 104 and DNP3 protocols are inherently unsecure, and software-based firewalls can introduce new vulnerabilities**
- **Combining IEC 104 or DNP3 with a hardware-enforced data diode secures remote monitoring communications**

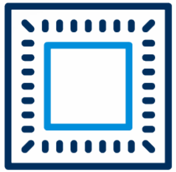
Use Case: Security Enhancement



- **Large, NERC CIP-compliant energy provider sought increased protection for critical assets**
- **Deployment included data diode transfer of ICCP, SFTP, HTTPS, SQL database, and historian data across multiple clusters and locations**
- **Enabled secure external data flow without altering NERC CIP compliance status**

The future of data diodes: FPGA technology

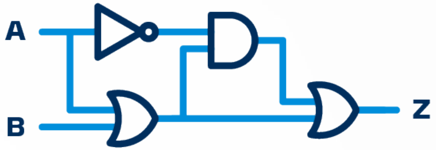
CPU



Turing Machine
General Purpose, programmable
Virtually unlimited states are possible

VS.

FPGA



Non-Turing Machine
Highly restricted functionality
Finite number of states, verifiable

Expanding Hardware-Enforced Security

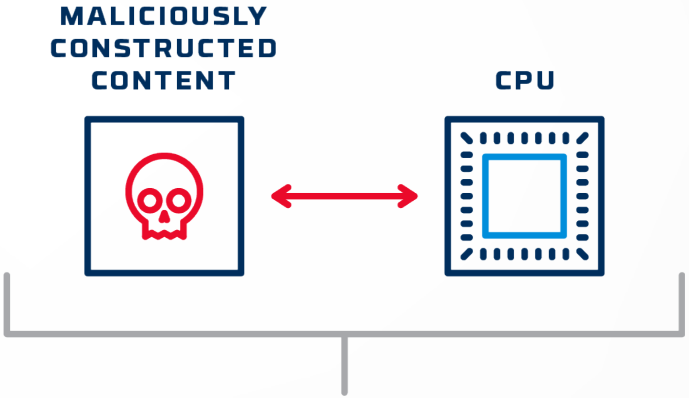
A data diode is just one example of hardware-enforced data security.

- Why focus on hardware security?
- What else can be done to protect systems in hardware?
- Can that be done at scale?

Owl Cyber Defense

Motivation for Hardware-Based Security

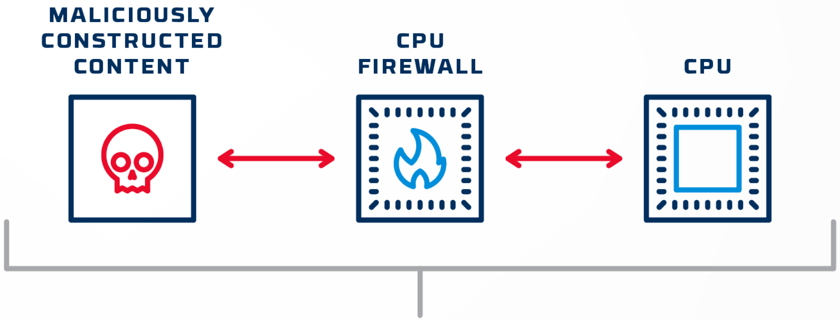
The goal of many network-based cyber-attacks is to cause a remote CPU to execute new code and/or override data and application boundaries.



Trigger a fault or unexpected condition
Override system controls
Execute new code

Motivation for Hardware-Based Security

- Typical solution is to protect the critical system with another CPU acting as a firewall or gateway
- Modern firewalls use advanced techniques to protect themselves, but fundamentally they are just a CPU running code

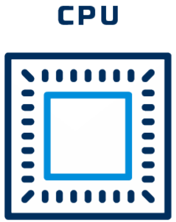


Chain of conventional systems makes an attack much more difficult, but it does not prevent an attack - Once successful, the attack pattern is repeatable

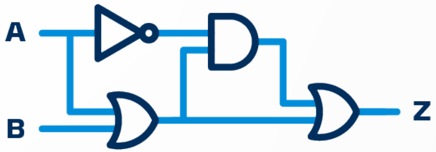
For truly critical applications, start by assuming any CPU will be compromised

Non-Turing Security

- **A CPU is powerful because it can be programmed to do anything – with a large amount of storage it can implement any arbitrarily complex function**
  - Not practical to test every input/output combination
- **A dedicated circuit is different, it can have a large but well-defined set of input/output paths**
  - Can be extensively tested and validated



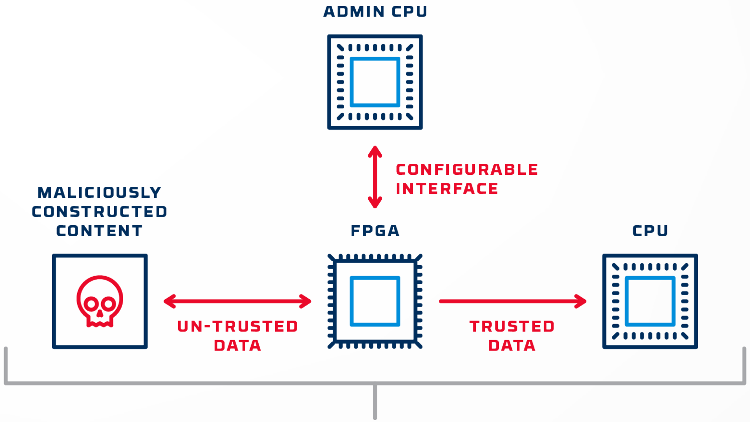
Turing Machine
General Purpose, programmable
Virtually unlimited states are possible



Non-Turing Machine
Highly restricted functionality
Finite number of states, verifiable

FPGA-Based Cybersecurity

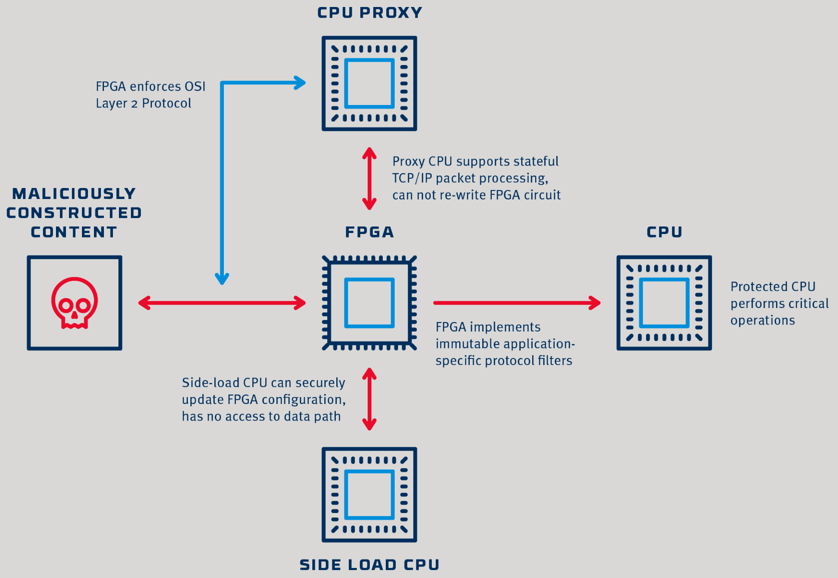
- **Field Programmable Gate Array (FPGA) technology can implement large-scale, complex circuits**
  - Circuit can be extensively tested and validated
  - FPGA configuration can only be updated through independent data path



FPGA logic filters content that is presented to CPU
Only valid patterns are passed by the FPGA
Limited number of states – can be tested and analyzed

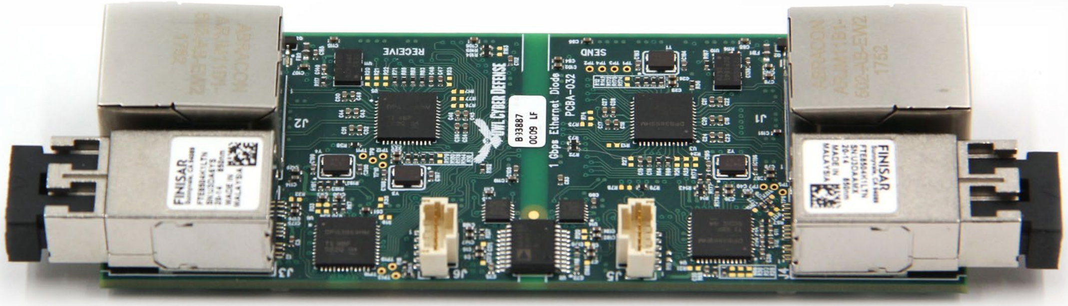
FPGA-Based Cybersecurity

- **FPGAs are not good at handling complex, stateful protocols**
- **Use a proxy CPU to support protocol management**
  - FPGA enforces strict application-specific data filtering
  - Proxy CPU supports TLS/DTLS and stateful protocols
  - Optional side-load CPU allows for configuration updates



The future of data diodes: smaller, cheaper, faster

- **Miniaturized technology allows diode capabilities to be embedded inside industrial devices**
- **Radically lower size, weight, and power requirements allow large-scale deployment to protect hundreds of devices per facility**
- **As with standard-size diode solutions, ongoing maintenance costs are negligible compared to software-based firewalls**
- **High throughput potential enables data filtering with very low latency (microseconds)**



Scalability

- **Single purpose devices**
  - Device level protection or micro-segmentation
  - Single data protocol
  - Limited bandwidth/capacity

- **Multi-purpose devices**
  - Multiple protocols
  - Multiple data types
  - Multiple sources and destinations
  - 10Mb -> 1Gb

- **Cards and Embedded**
  - DIY solutions
  - Cards installed in servers – 10Gb and higher
  - Designed into a device – inherent part of the device

OWL Cyber Defense

Q & A

Cyber Defense