

NS22 - Owl Computing Technologies

Cybersecurity for the Information Enabled Industrial Internet of Things

Dennis Lanahan
Director World Wide Channel Partnerships & International Sales
June, 2016

PUBLIC



Allen-Bradley • Rockwell Software

**Rockwell
Automation**

- Introduction to Owl
- The Industrial Internet of Things and the Connected Enterprise
- DHS Industrial Control Cybersecurity Recommendations
 - “Use Data Diodes”
- What is a Data Diode
- Applying Data Diodes to Protect SCADA, PLCs, Historians, etc.
- Data Diode Use Cases
- Demonstrations here at TechEd



US owned and operated

- US supply chain
- US R&D & manufacturing
- US based Technical Support & Service
- US Secret and Top Secret Clearances
- Self-funded Development



Experience

- Exclusive focus on cybersecurity for 17 years
- Over **2000 deployments globally**
- Global Sales and Service
- Accreditation Services
- Configuration Management Services



Multi-Market Solutions

- Government Cross Domain Solutions
- DoD & Intelligence Agencies
- USDSMO Baseline listed

- Critical Infrastructure Network Defense
- Utilities: Nuclear, Electric, Gas, Water
- Energy: Oil & Gas, Petrochemical
- Telecommunications
- Financial Services



Technology Innovator

- Single 1U, all-in-one solution
- Server based Communication Card Systems
- 24 technology patents
- Deterministic one-way transfers
- EAL Certified
- Unified Cross Domain Services Management
- Office Approved Cyber Baseline

What is the IIoT?

Smart Machines,
Software,
Sensors,
&
Network Connectivity

That

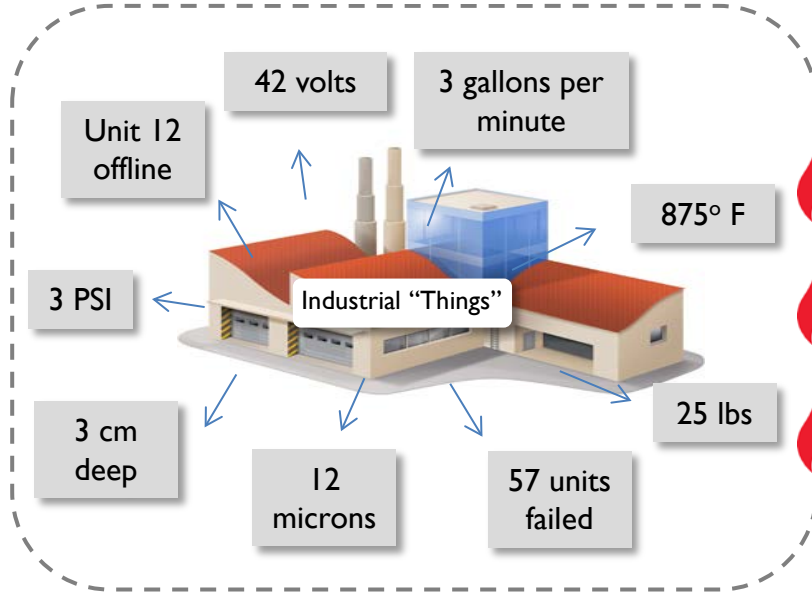
Collect
And
Exchange Data

Generating Operational Information in the Plant, at HQ
or in the Cloud

And by the way, it needs to be *secure*.

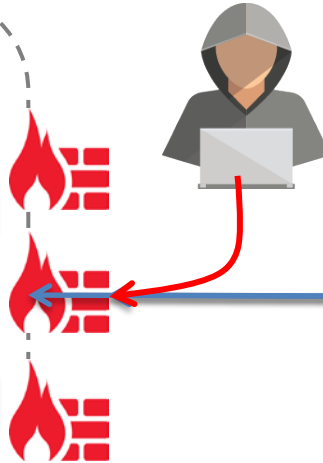
Remote Access of IIoT data – Is it Secure?

OT Network

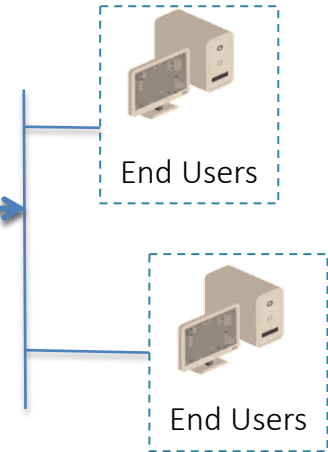


Security Boundary

But is it secure?

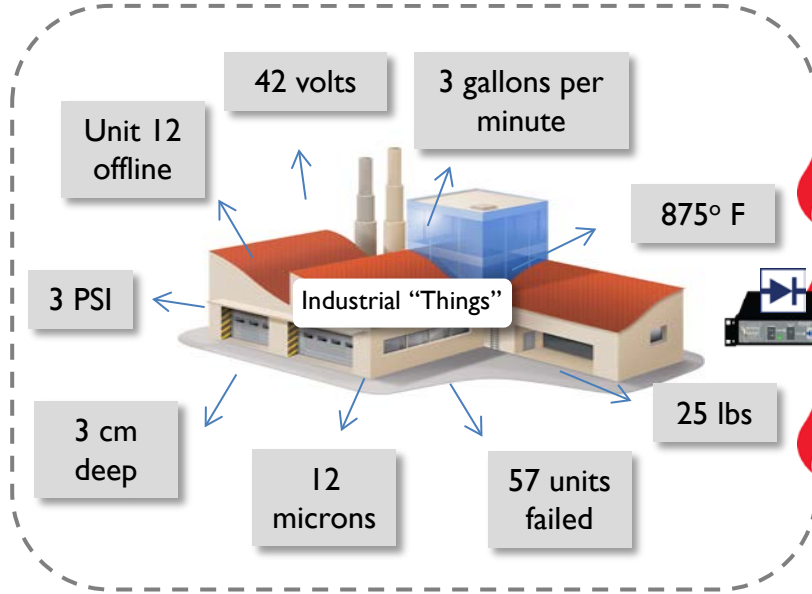


Remote Monitoring With Remote Access



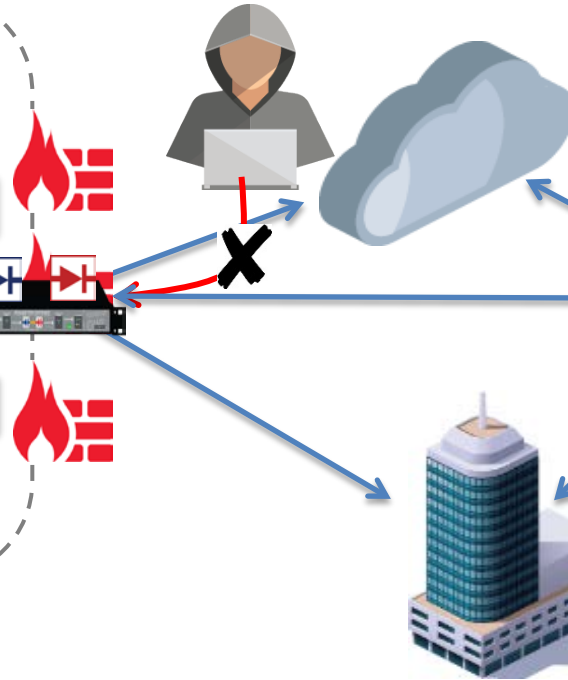
Change the Paradigm – Monitoring without Access

OT Network

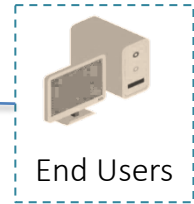
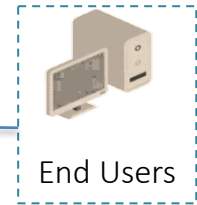



Security Boundary

But is it secure?






Remote Monitoring Without Remote Access





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, 294 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.

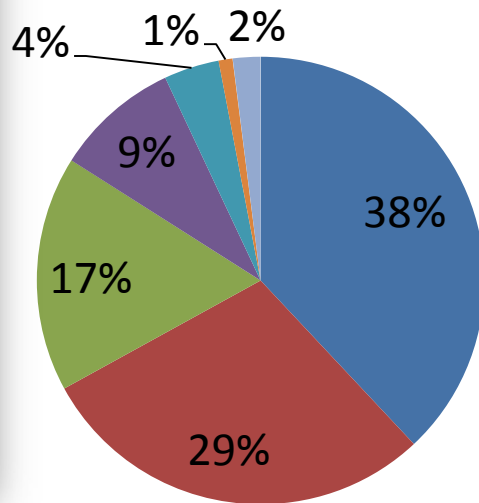
Seven Strategies to Defend ICSs

Strategy	Percentage
Implement Secure Remote Access	1%
Monitor and Respond	3%
Manage Authentication	4%
Implement Application Whitelisting	38%
Ensure Proper Configuration/ Patch Management	29%
Reduce your Attack Surface Area	17%
Build a Defensible Environment	9%

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 more effective.

Cyber Threats Against Industrial Controls



- Execution of Malware
- Unpatched Systems
- Open Connections
- Perimeter Breaches
- Compromised Credentials
- Exploit Back doors
- Miscellaneous exploits

DHS Seven Strategies for Defeating Threats

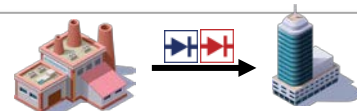
1. Application Whitelisting
2. Configuration/Patch Management
3. Reduce Attack Surface
4. Defendable Environment
5. Manage Authentication
6. Implement Secure Remote Access
7. Monitor & Respond

Data Diodes Support
all Seven Strategies



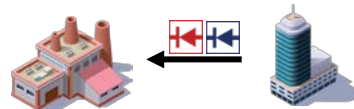
These strategies could have ***prevented 98%*** of attacks in 2014 and 2015

- **One-Way Communications Path Out of the Plant**



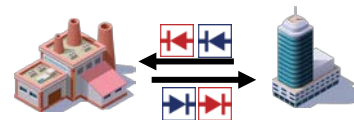
- Build a Defendable Environment : Segment networks and restrict host-to-host paths to prevent and contain the spread of infection
- Reduce Attack Surface Area: use a **data diode** to provide network segmentation
- Implement Secure Remote Access: Implement monitoring only solution with access enforced by **data diodes**

- **One-Way Communications Path Into the Plant**



- Configuration/Patch Management: provide secure configuration/patch management program centered on safe importation of trusted patch updates

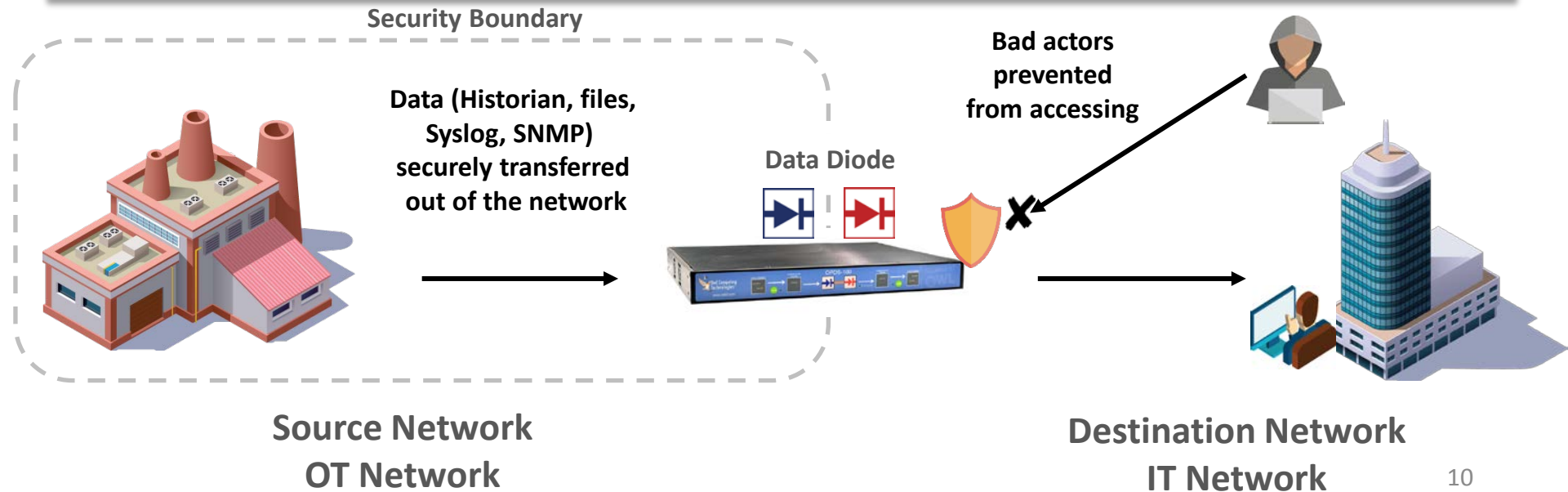
- **Two-way Communications Path With the Plant**



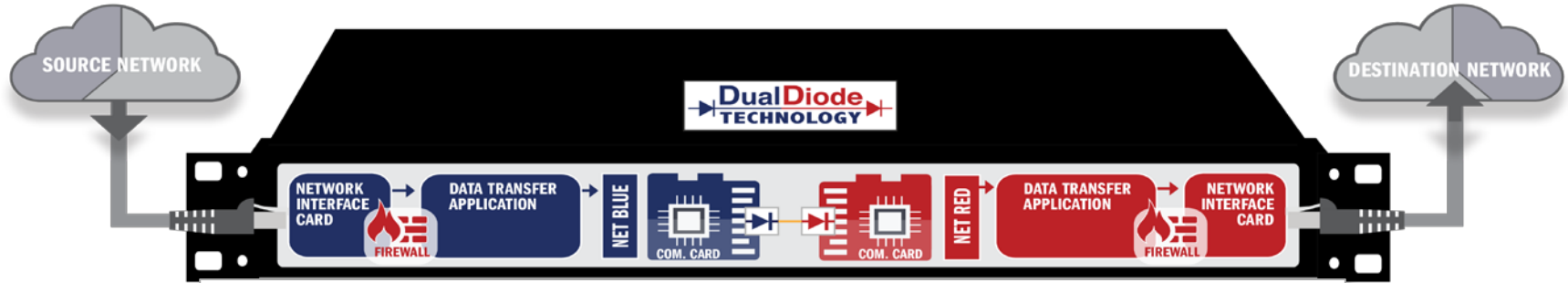
- Reduce Attack Surface Area: If bidirectional communication is needed use a single port over a restricted path

What is a Data Diode?

- Hardware based cybersecurity *designed* to be one-way
- Impervious to software changes or attacks (hardware cannot change)
- Defends the perimeter of the source network (prevents all external attacks)
- Transfers data across network security boundaries (without creating attack vector)



DualDiode Features - Benefits



Owl data diodes are proven, deterministic one-way only network security products

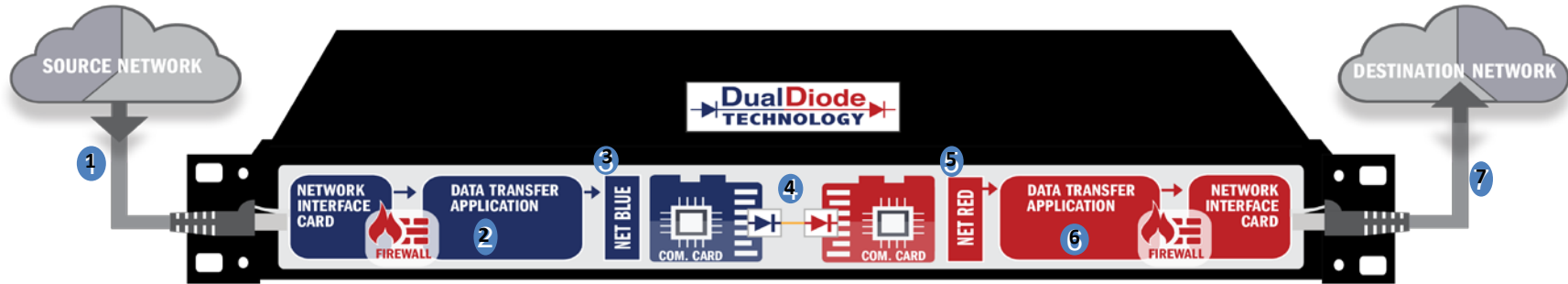
Features:

- Optical “air gap”, enforces one-way network segmentation
- Proxies terminate/initiate communication with end points
- ATM protocol to transport data across DualDiode.
- Only payload is transferred, no routable information crosses DualDiode
- ATM High bandwidth, low latency, high reliability protocol
- Single box solution, no flanking servers
- Simultaneous transfer of multiple data flows and multiple data types
- Software connectors - Files, databases, historians, video surveillance, syslog messages, events, alarms, UDP/IP, TCP/IP, email, HMI replication, etc., plus vendor specific applications

Benefits:

- 100% Network Confidentiality
- Standard Network Protocols (TCP, UDP, File transfer)
- Protocol break - meets regulatory requirements
- 100% Network Confidentiality
- Very high quality of service, Availability and Integrity
- Easy installation, lower SWaP and cost of ownership
- Multi-use security product
- Industry Applications you can use today

DualDiode Data Flow



1. IIoT data is generated on Source network and sent to data diode
2. Blue - Data transfer application proxies terminate connection(s) (UDP, TCP, files) with Source network
3. Net Blue prepares data packet payloads for transfer across ATM channel
4. Core DualDiode transfers data payload using ATM across network boundaries through air gap
5. Net Red pulls payload off of ATM channel
6. Red – Data transfer application places payload in new packets (UDP, File, TCP)
7. Connection established with Destination using original transport protocols and data is delivered

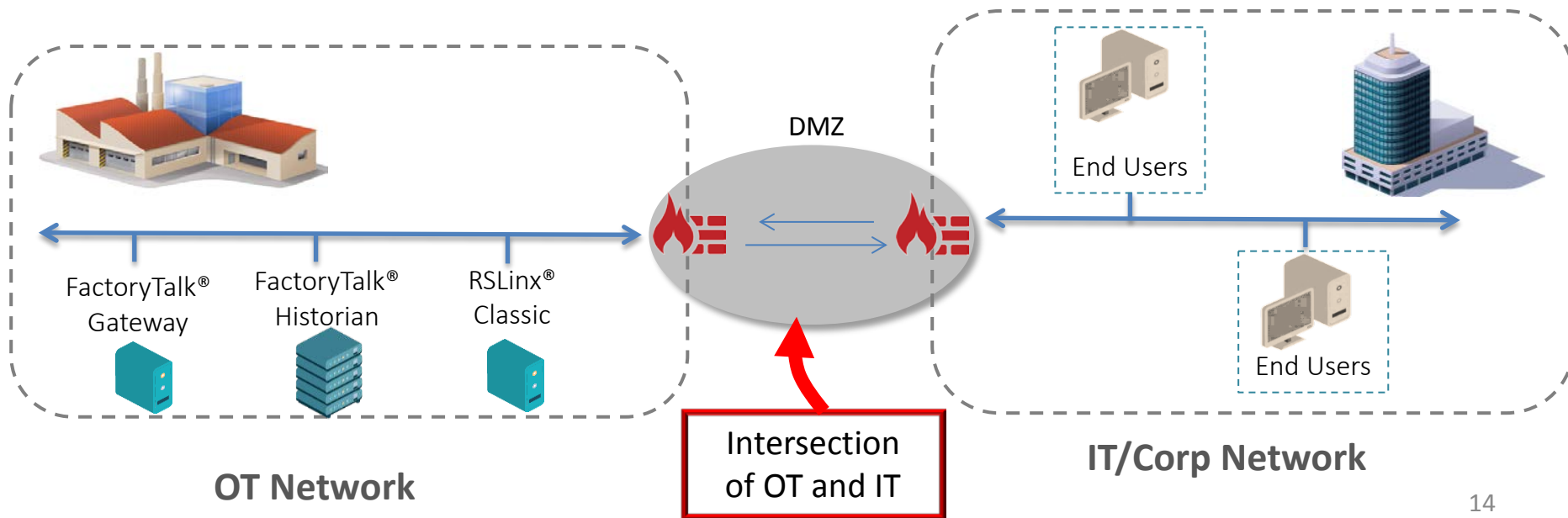
Data Diodes, more secure than Firewalls



According to recent third party analysts, data diodes are the highest level of network security next to physical separation (air gap)

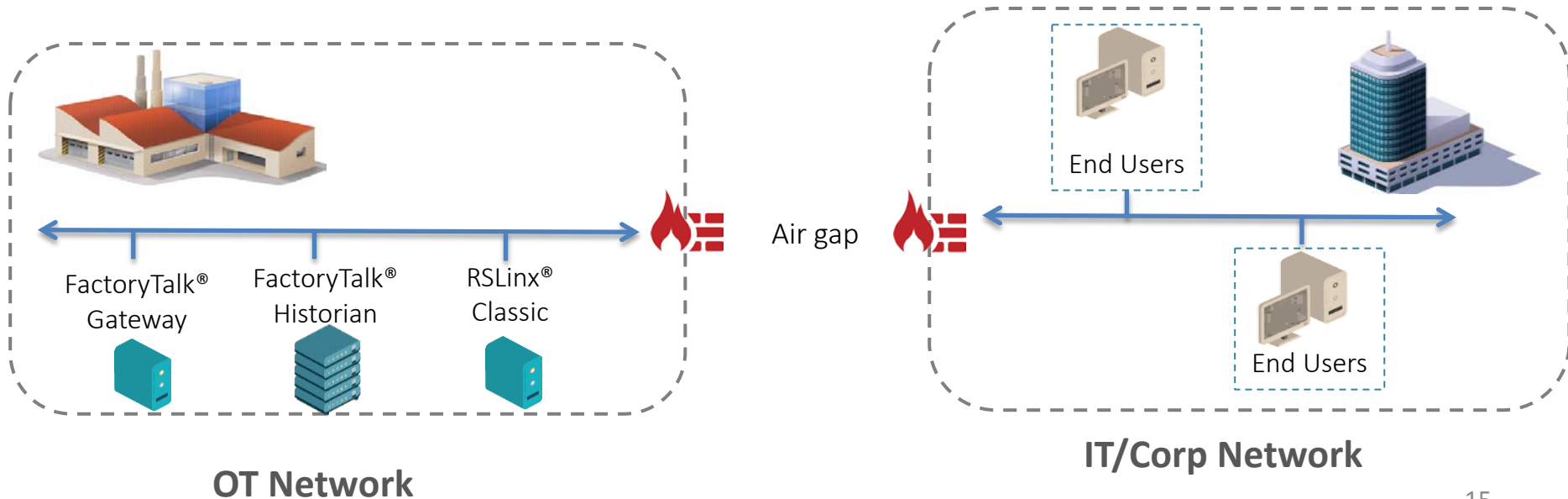
Firewall Network Security

- EXCELLENT BUSINESS CONTINUITY
- *LIMITED CYBERSECURITY*

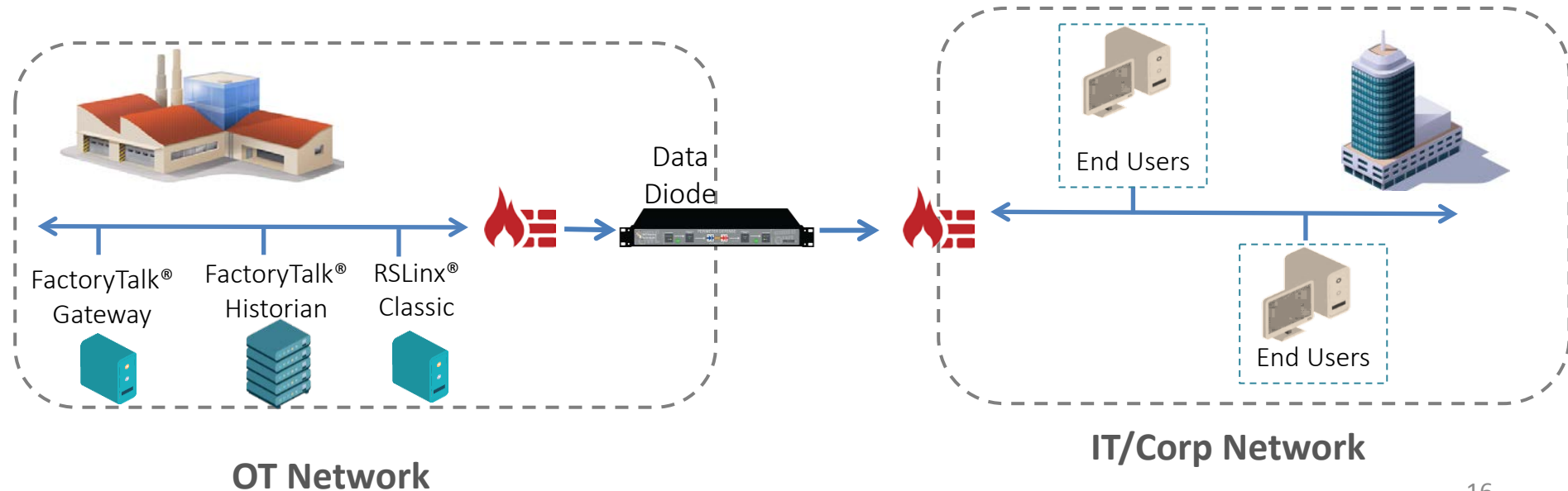


Air gap network security

- EXCELLENT CYBERSECURITY
- *LIMITED OR NO BUSINESS CONTINUITY*



- EXCELLENT CYBERSECURITY
- RESTORED BUSINESS CONTINUITY



How One-Way Works in a Two-Way World

Existing



OT Network



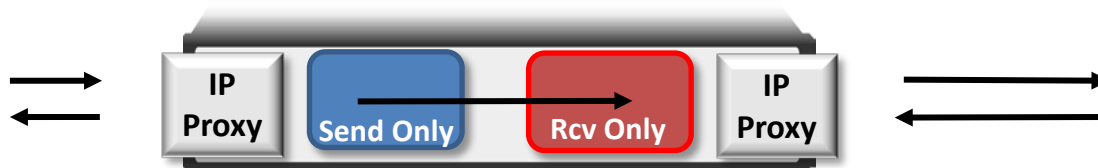
IT Network



One-way Transfer Established



OT Network

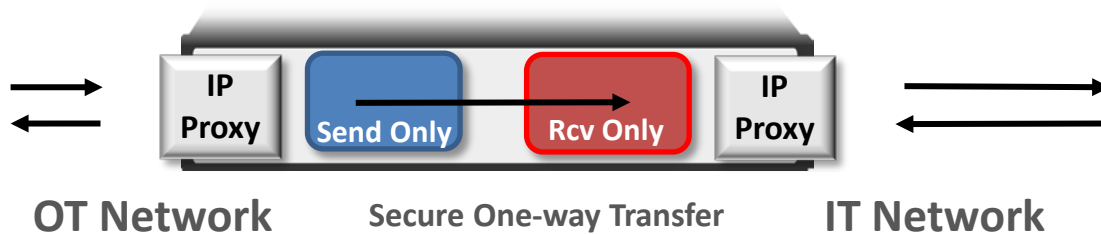


Secure One-way Transfer

IT Network

One-way Out & One-way In

One-way Out



One-way In

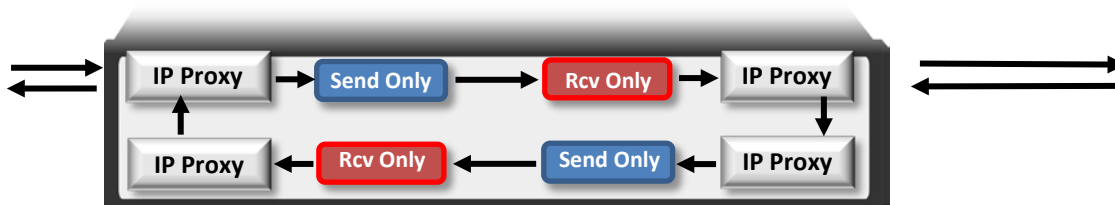


DHS Strategy #3: Reduce Your Attack Surface Area -

“If *Bidirectional communication is necessary*, then use a single open port over a restricted network path.”



OT Network

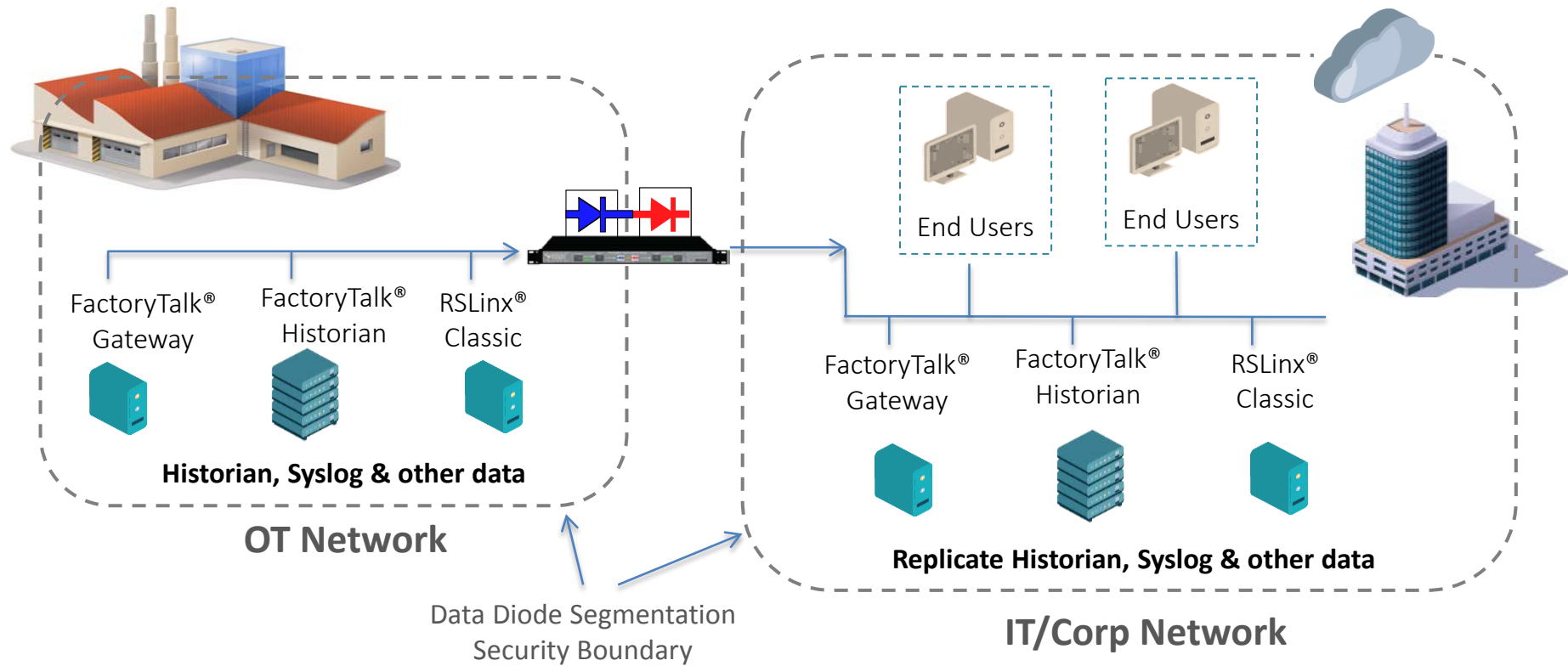


IT Network

Owl Bilateral Communication System (OBCS):

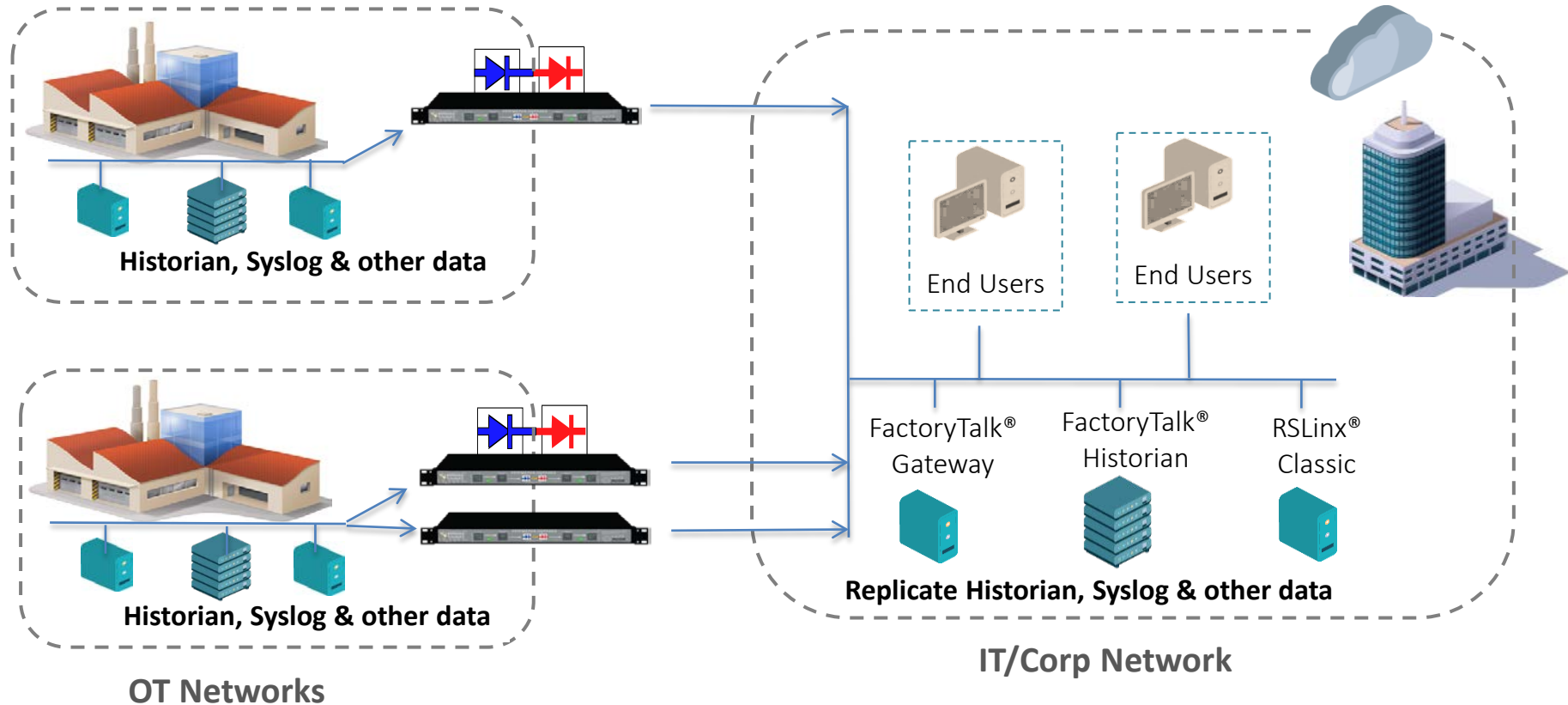
- Single port with restricted path
- Supports TCP/IP Applications that cannot be one way
- Pair of Secure One-way Transfers with in 1U enclosure
- Non Routable ATM protocol breaks
- TCP/IP proxies that break and join single whitelisted session

Small Enterprise Architecture



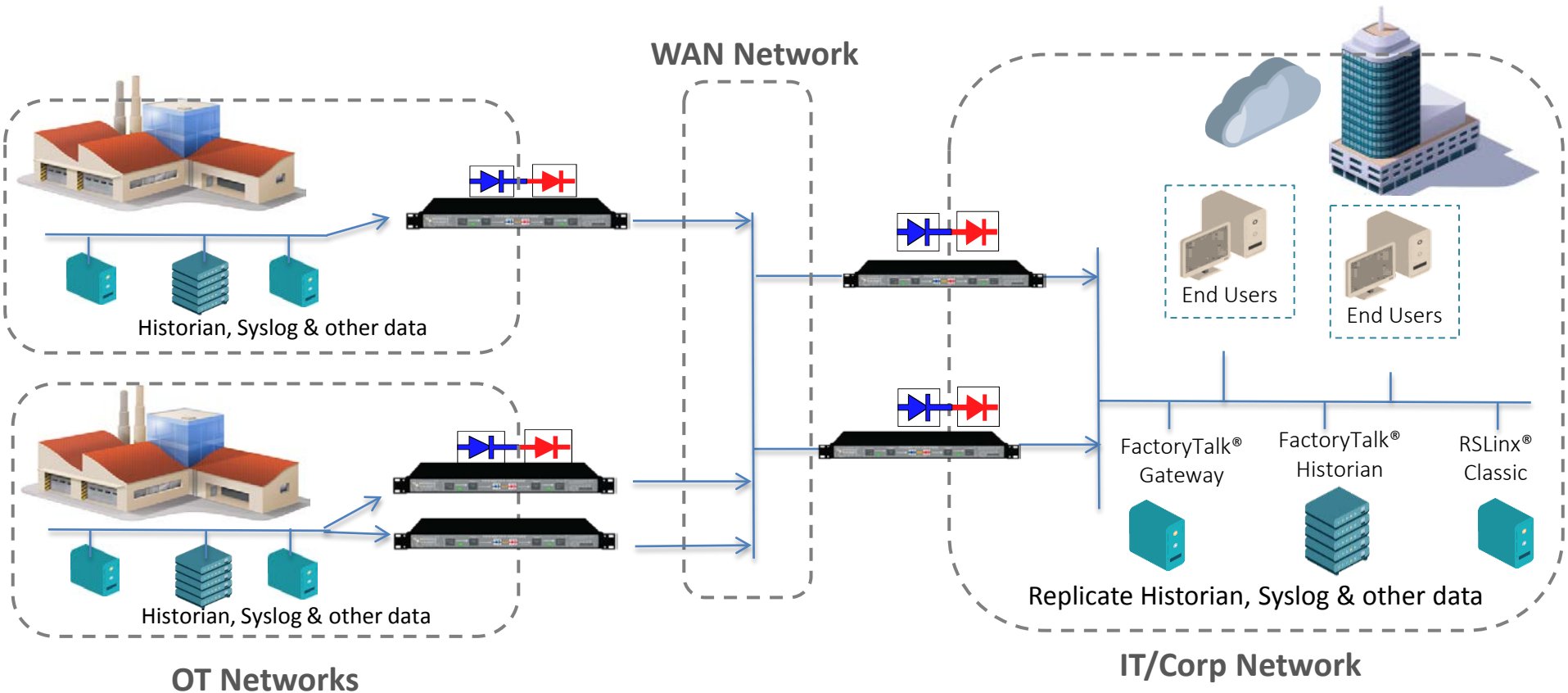
Supports simple and easy security and established data replication flows

Medium Enterprise Architecture



Meets the needs of any midsize company security and data needs

Large Enterprise Architecture



Supports largest enterprise needs with failover, redundancy and load balancing

- **Owl Supports other Transfer Applications**
 - Historian replication
 - OSISoft PI, Rockwell FactoryTalk Historian, others
 - Syslog, SNMP transfer
 - Email (SMTP) Alerts and events
 - RA Asset Center
 - Remote HMI Screen replication
 - SQL Database replication - MS SQL, Oracle 10g, 11g
 - UDP, multicast, broadcast, unicast (video surveillance)
 - TCP/IP transfers
 - Remote File Transfer for Reporting, Alarms, Events, any file
 - OPC Foundation certified, supporting DA, A&E, UA
 - Modbus
 - Others...
- Software and Patch Updates, whitelisted inbound file transfers, with AV content inspections, and file hash code validations (SHA 256)



- **Power Generation, Substations, T&D**

- Turbine, Nuclear, Fossil, Hydro plant performance data
- Historian replication
- Secure remote monitoring – syslog, alarms, events
- Compliance reporting



- **Manufacturing and Mining**

- Secure monitoring of system alarms, events, syslog messages
- Transfer of Files, email, security video



- **Oil and Gas**

- Transfer of historian data, alarms, events
- Interfaces: MODBUS, OPC,



- **Water, Wastewater**

- Windows HMI Screen replication
- Historian data



- **Financial and Banking**

- Data transfer between secure and less secure locations
- Financial transactions

17 Illustrated Use Cases

- **Oil & Gas Industry**
 - **Oil company** – plant isolation and replication of OSIsoft historians from plants to a centralized corporate facility
 - **LNG company** – plant isolation, replication of OSIsoft historian, transfer of alarm information to centralized NOC
 - **Natural Gas co** – isolation of gas turbines & remote support/monitoring of turbines by OEM
- **Petrochemical**
 - **Chemical producer** – isolation of plants & OPC interface for real-time transfer of plant data and alarm & event information, OSIsoft historian replication from plants to corporate facility
- **Water/Wastewater**
 - **Utility** – plant isolation, transfer of operations management reports to corporate facility. Remote HMI screens.
- **Power Generation**
 - **Nuclear Utilities** – plant isolation per NRC regulatory requirements. Replication of OSIsoft historians, ModBus data replication and remote monitoring data all transferred out of the plants
 - **Coal power** – plant isolation per North American Electric Reliability Corporation (NERC) CIP 5 regulations. OSIsoft historian replication. OPC data replication. Transfer of compliance reporting files
 - **Gas turbine** – turbine isolation, operations/performance data sent to remote monitoring facility of vendor
 - **Federal nuclear, fossil, hydro facility** – NRC and NERC compliance, isolation of plants/OT networks, fleet-wide replication of historians, transfer of management reports to HQ

- **Power Transmission and Distribution**
 - **Utilities** – isolation of substations to meet NERC CIP v5 regulatory guidance, replication of OSIsoft historian, OPC data transfer, transfer of compliance reporting files, HMI screen replication to remote facilities
- **Financial services**
 - **Banking (ATM transactions)** - transfer of ATM transaction data and surveillance data into a secure repository. No remote access to repository, no way to remove data from repository.
 - **Credit Union (remote backup)** – periodic transfer of backup data files from branches to offsite backup repository. No way to remove data from repository or create a back channel into the branches from repository
 - **Banking (data center, 24x7 operations)** – isolate the center, transfer performance and monitoring data to remote IT staff responsible for running the data center
 - **Banking (capture forensics data)** – transfer digital copies of compromised computer assets to a forensic analysis lab. Isolation of lab, no way for forensic data to be manipulated or any malware to escape
- **Transportation**
 - **Rail** – isolation of sensors deployed in railyard, transfer of sensor data to cellular communications center for wireless transmission to remote centralized monitoring center
- **Rare Earth Mining**
 - **Mining company** – plant isolation against foreign attacks, historian replicated from plant to corporate

1. The IIoT generates data for a range of end-users
2. Data Diodes protect the plant and those elements of the IIoT within it
3. Data passes through the data diode to reach data-store outside of the plant
4. External users have access to the data to get their work done
5. External users do NOT have access into the plants
6. Plant Security Enabled for the Rockwell Connected Enterprise and IIoT

Secure Plants With Access to IIoT Generated Data

1. OPDS-100D Replication of data out of the plant
 1. Rockwell FT Historian ME to SE replication
 2. RS Linx and RS View OPC server replication
 3. HMI Screen replication (UDP connection)
 4. File Transfer (TCP/IP connection)
2. OPDS-100 Secure Update Service
 1. Secure file transfer into the plant
 2. With Secure SHA hash code validation



1. Industrial Control Systems (SCADA, PLCs, etc.) are an inherent part of IIoT
2. DHS has made recommendations for defending Industrial Control Systems
 - Highlight the use of data diodes
3. Data Diodes
 - Proven more secure than firewalls
 - Work in a variety of scenarios
 - Support a range of protocols/data types
 - Are deployed across many industries






Owl Computing Technologies, Inc

**Ridgefield, CT
+1 203-894-9342
www.owlcti.com**

We care what **YOU** think!

**Rockwell
Automation**

Please take a quick session survey on our mobile app to tell us how we're doing.

- Locate session using Schedule  or Agenda 
- Click on the  icon on the lower right corner of session detail
- Complete Survey & Submit



Thank you!