LISTEN.
THINK.
SOLVE.

T44 – Owl Computing Technologies

Data Diodes Implement DHS Strategies for Industrial Control System Cybersecurity

Dennis Lanahan
Director of Worldwide Channel Partnerships & International Sales
November, 2016

PUBLIC

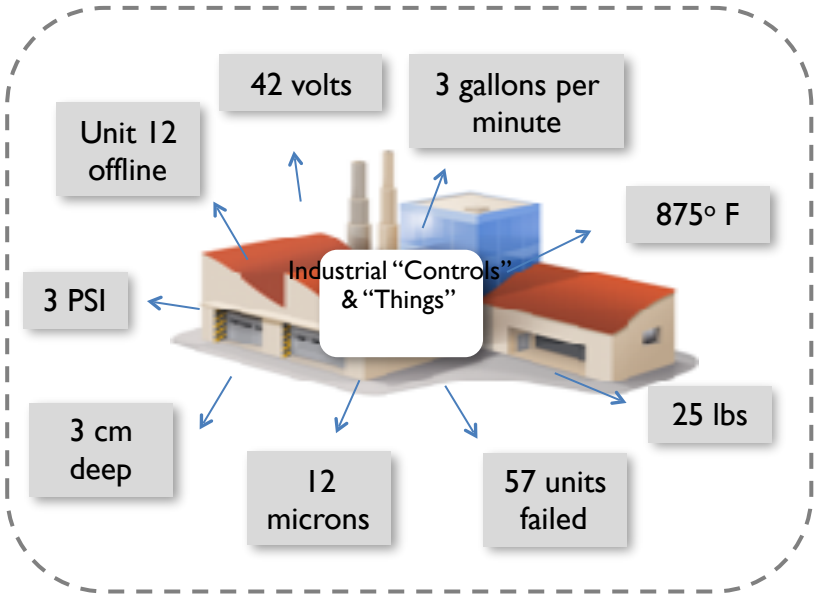
Allen-Bradley • Rockwell Software

Rockwell Automation

Operations Technology (OT) – ICS and IIoT

Industrial Control Systems (ICS), Industrial Internet of Things (IIoT)

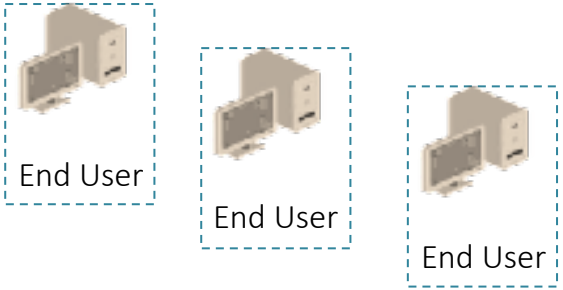
OT Network



Security Boundary

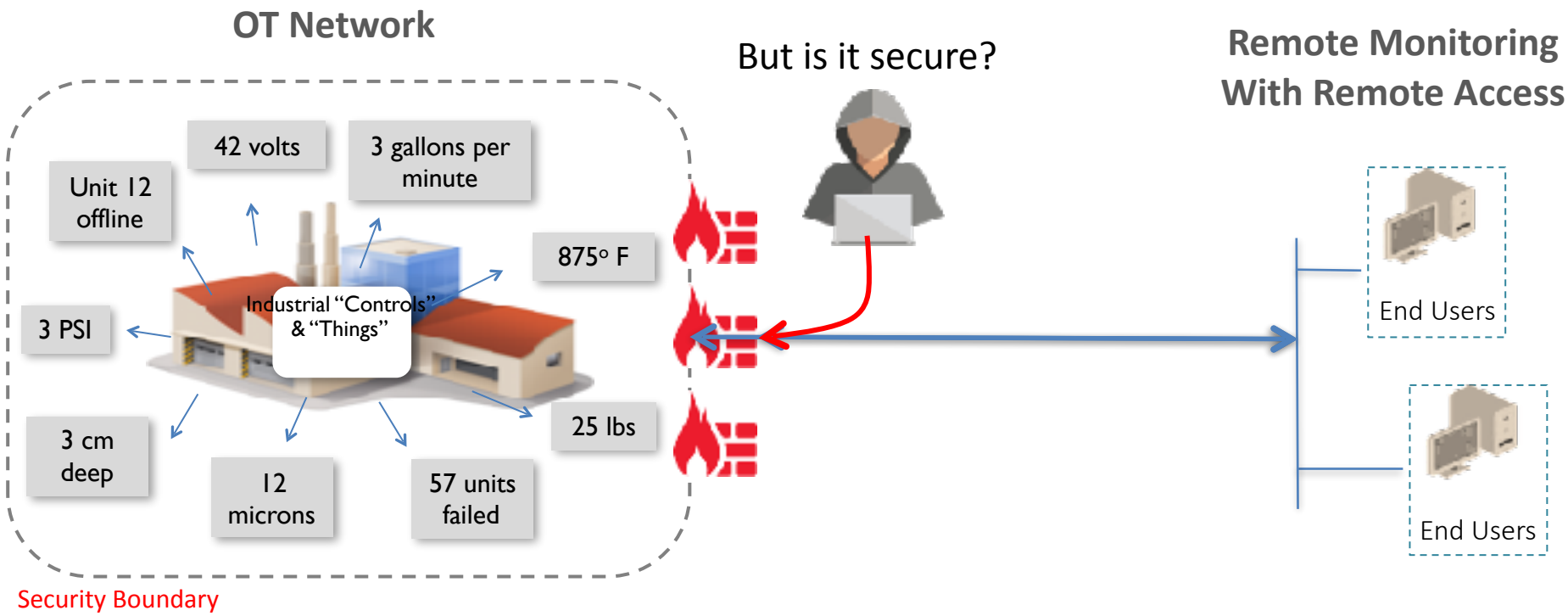
Information Creators

IT Network



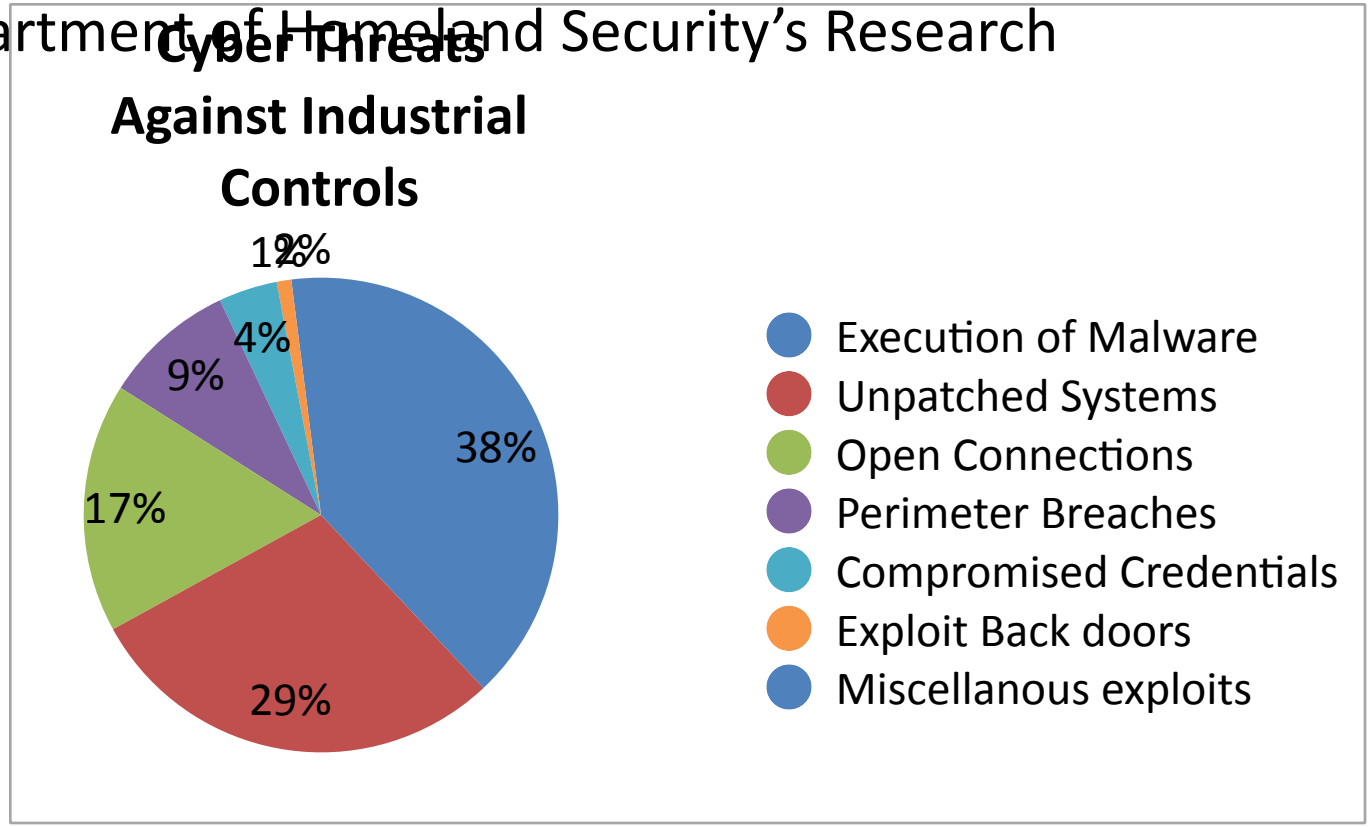
Information Consumers

Remote Access of Data – Is it Secure?



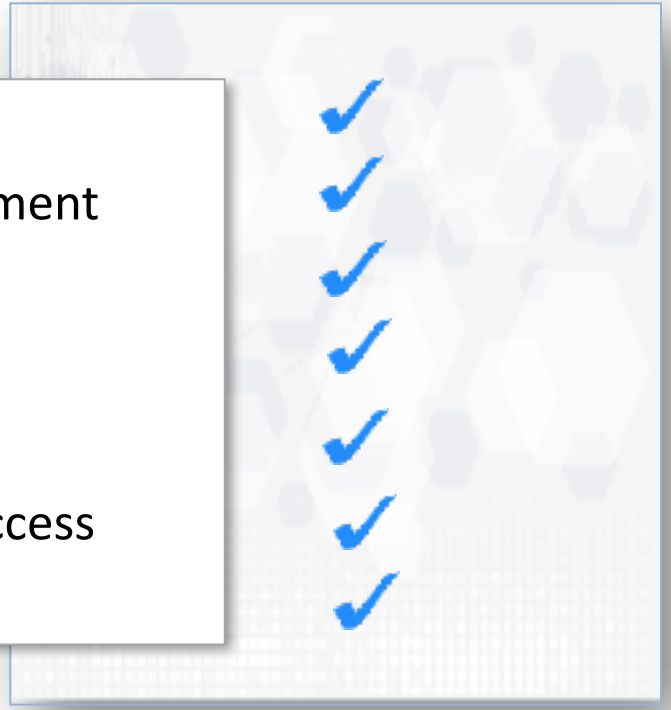
DHS, FBI, NSA Risk Assessment for ICS

US Department of Homeland Security's Research



Published December 2015, https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

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



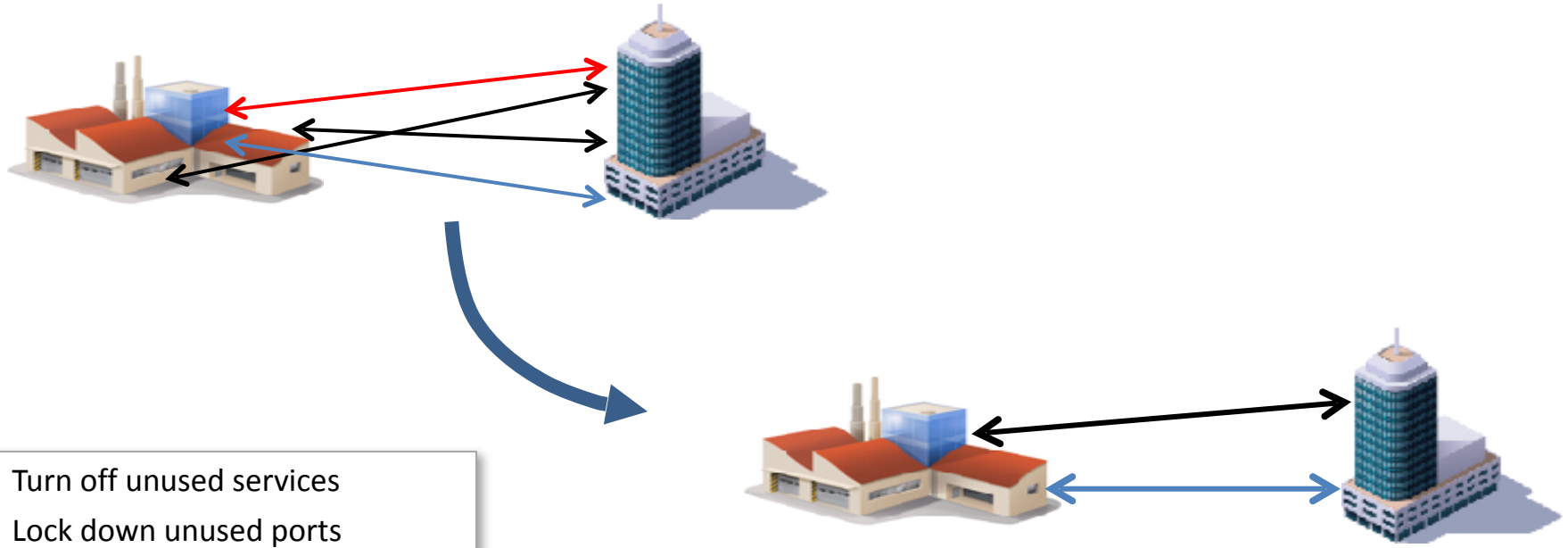
These strategies could have ***prevented 98%*** of attacks in 2014 and 2015

Highlights from DHS Seven Strategies Whitepaper

- **Application Whitelisting**: Only allow pre-designated applications to run
- **Configuration and Patch Management:** safe import of trusted patches
- **Reduce Attack Surface Area**: Isolate industrial control system (ICS) networks ●lock down unused services and ports ●use a ***data diode*** to provide network segmentation
  - if bidirectional communication is needed use a single port over a restricted path.
- **Build a Defendable Environment**: Use optical separation ("data diode") to:
  ●segment networks ●restrict host-to-host paths ●prevent and contain the spread of infection
- **Implement Secure Remote Access:** Remove back doors and modem access ●implement monitoring only with access enforced by ***data diodes*** ● do not rely on "read only" software configurations ● don't allow persistent remote connections

Bottom Line – Reduce Open Access

1. Eliminate connections that aren't necessary

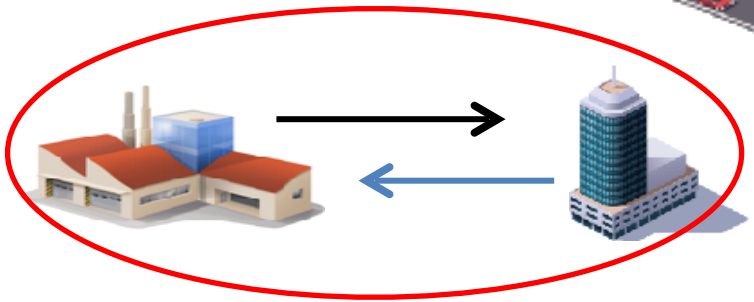


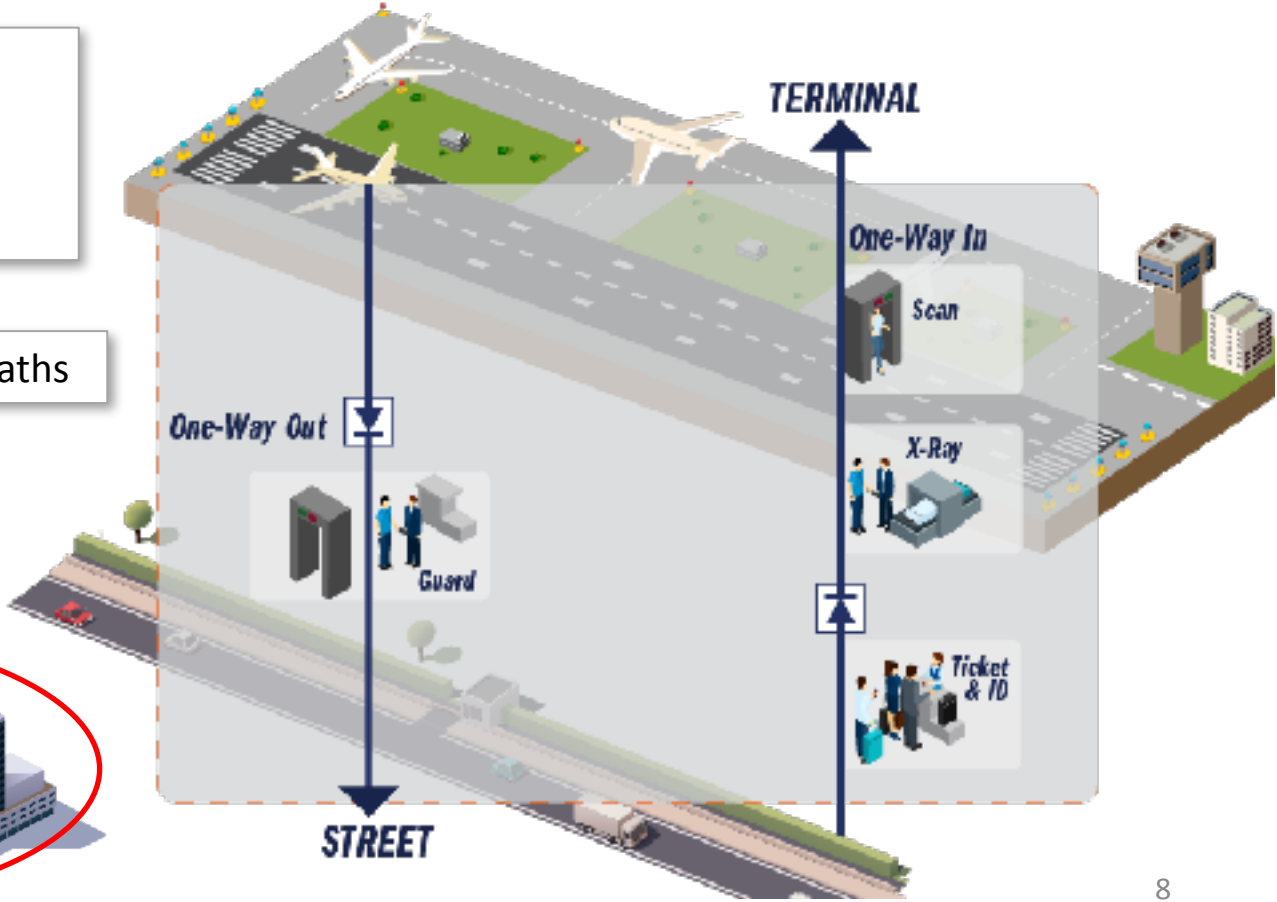
- Turn off unused services
- Lock down unused ports
- Eliminate modem connections
- Consolidate access points

Bottom Line – Reduce Open Access

2. Convert data paths to:
   - One-way in
   - One-way out

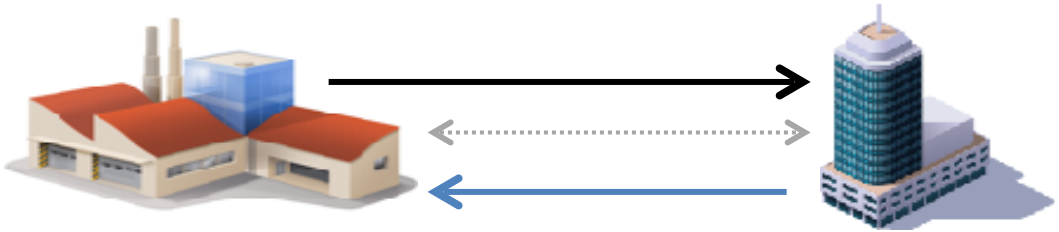
Analogy: Physical airport security paths



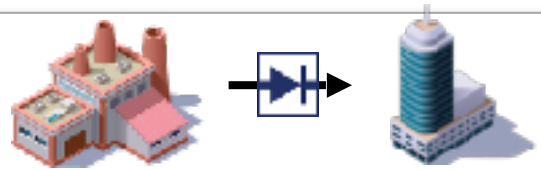


Bottom Line – Reduce Open Access

3. Any remaining two-way connections for external command and control, requires risk assessment
   - DHS recommendation:
     - "if bidirectional communication is needed use a single port over a restricted path"
     - Transient connections (NERC-CIP terminology)
       - Short term, single purpose connection – only connected while in-use
       - VPN, physical Ethernet switch, restricted firewalls, etc.
     - Owl data diode Bi-Lateral solution (More about this later)

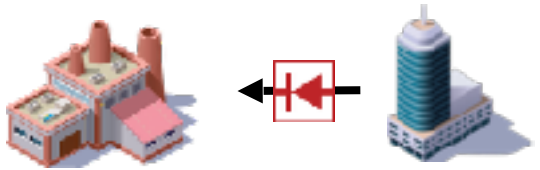


Implementing DHS Guidance



#1 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***



#2 One-Way Communications Path into the Plant

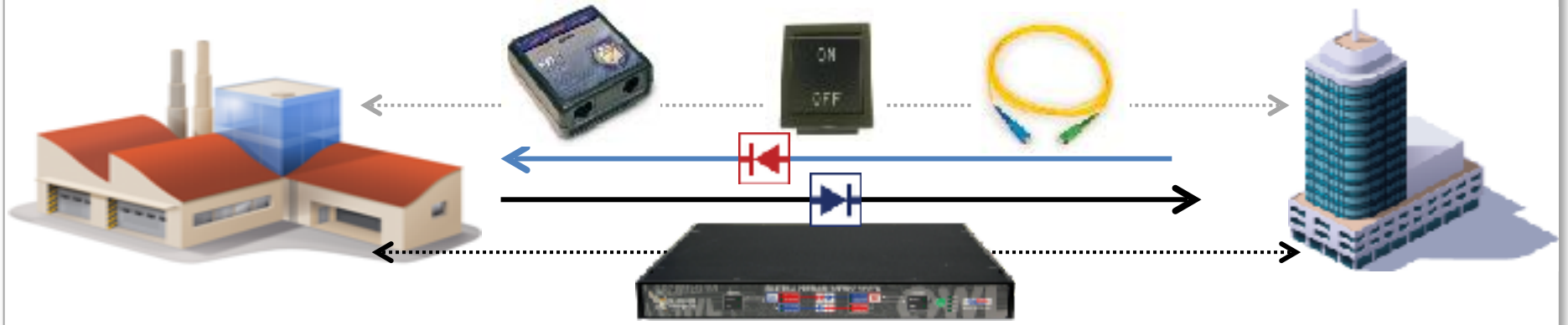
- Configuration/Patch Management: Provide secure configuration/patch management program centered on safe importation of trusted patch updates

Two-Way Communications Path with the Plant

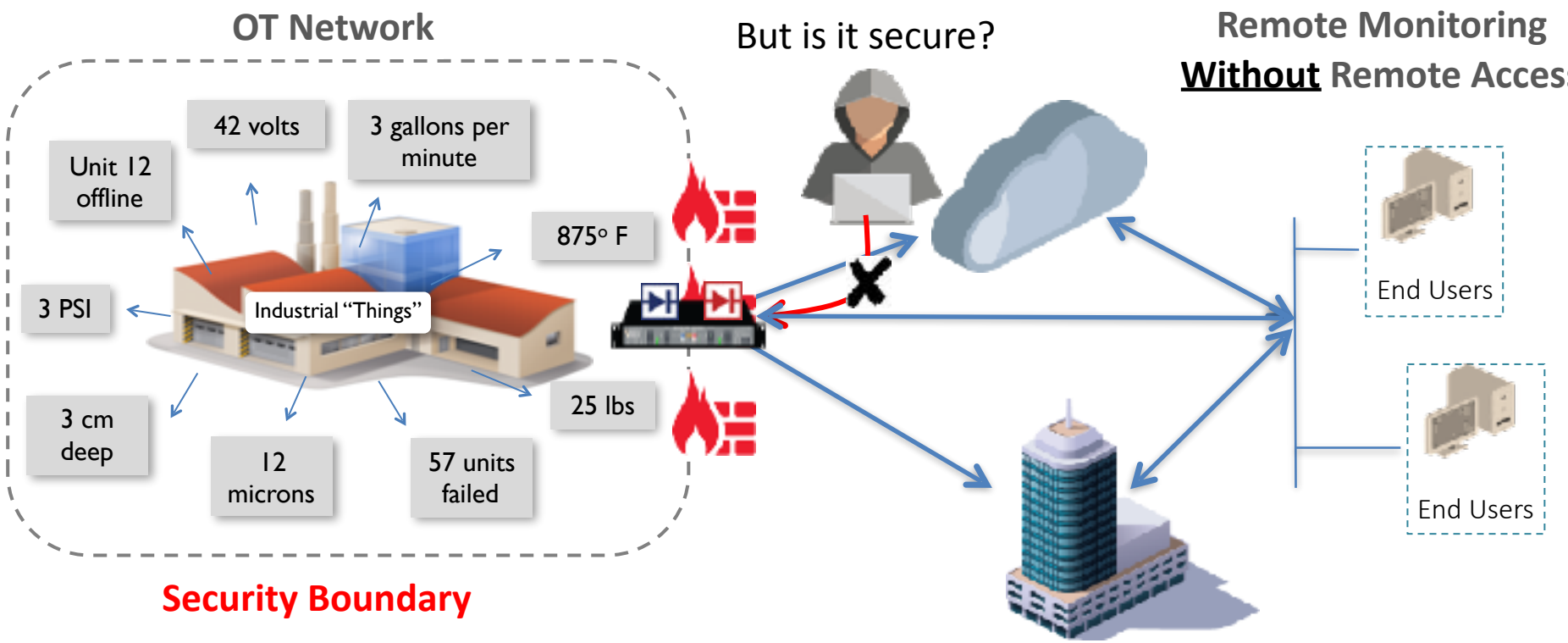
- Reduce Attack Surface Area: If bidirectional communication is needed use a single port over a restricted path
- Bi-Lateral data diode solution

By-pass alternative

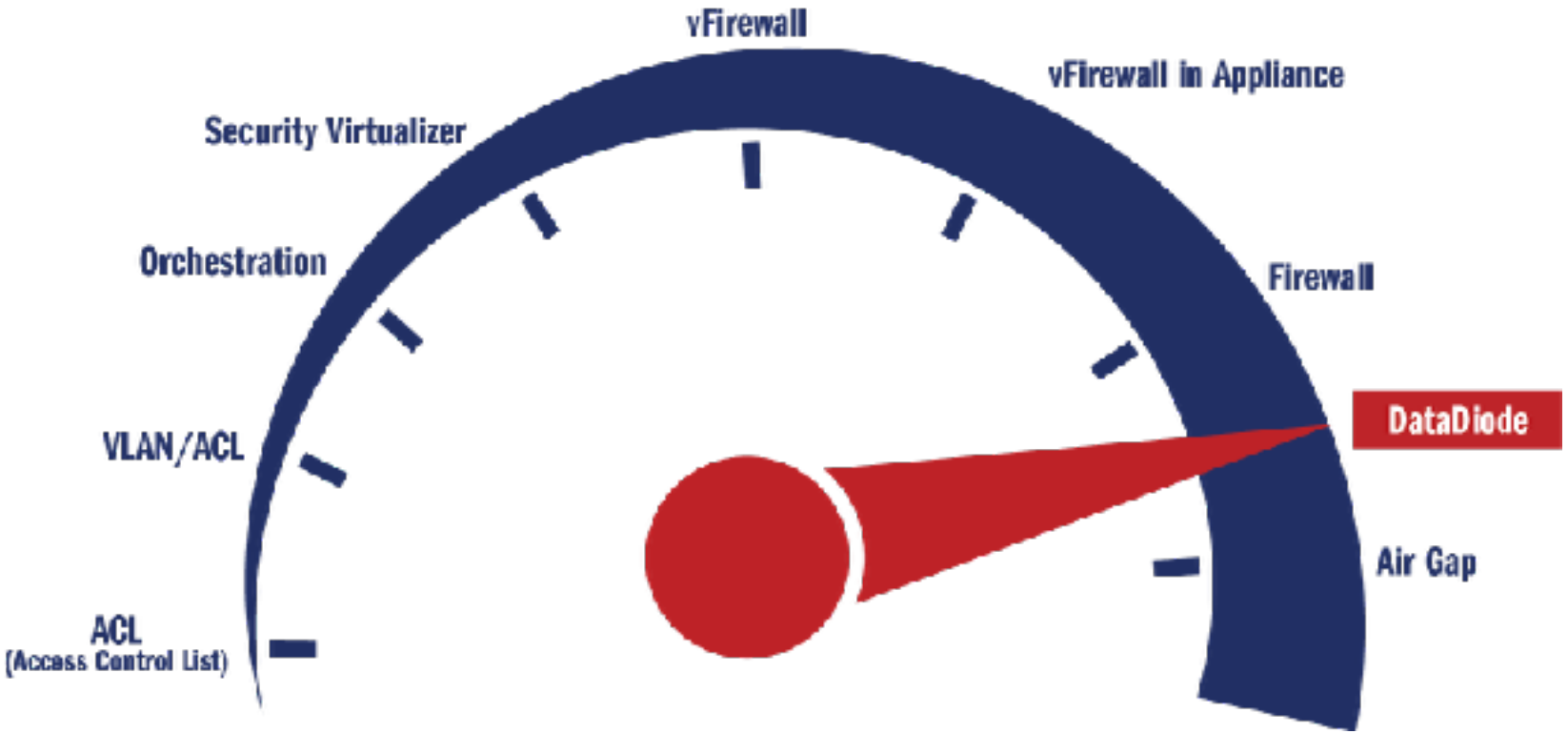
- Permanent infrastructure used for temporary connections
  - Ethernet on/off switch, dedicated patch cable



Change the Paradigm – Monitoring without Access

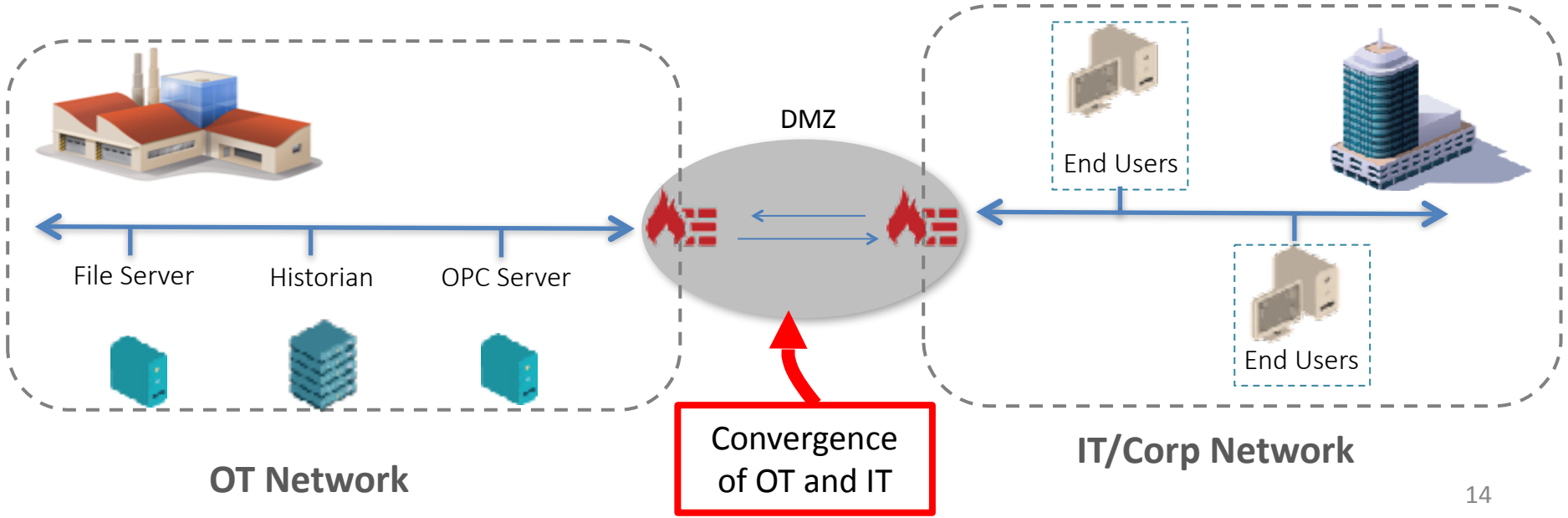


Effectiveness of Cybersecurity Technologies



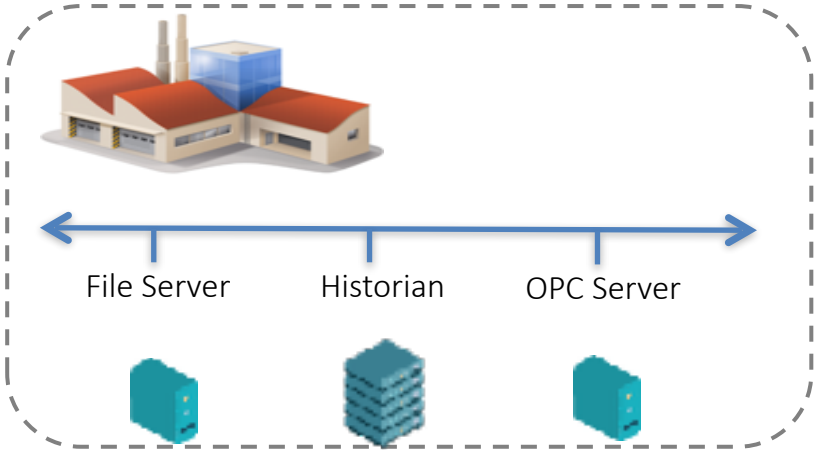
Firewall Network Security

- EXCELLENT BUSINESS CONTINUITY
- *LIMITED CYBERSECURITY*



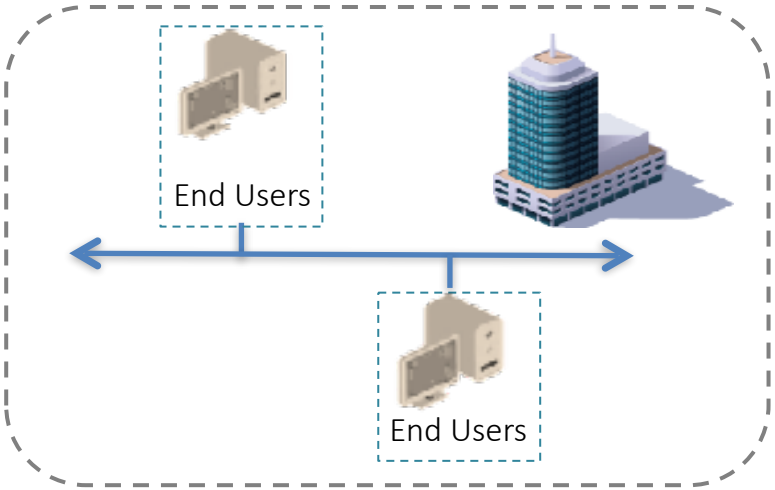
Air Gap Network Segmentation

- EXCELLENT CYBERSECURITY
- *LIMITED OR NO BUSINESS CONTINUITY*



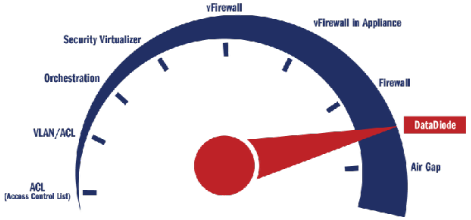
OT Network

Air gap

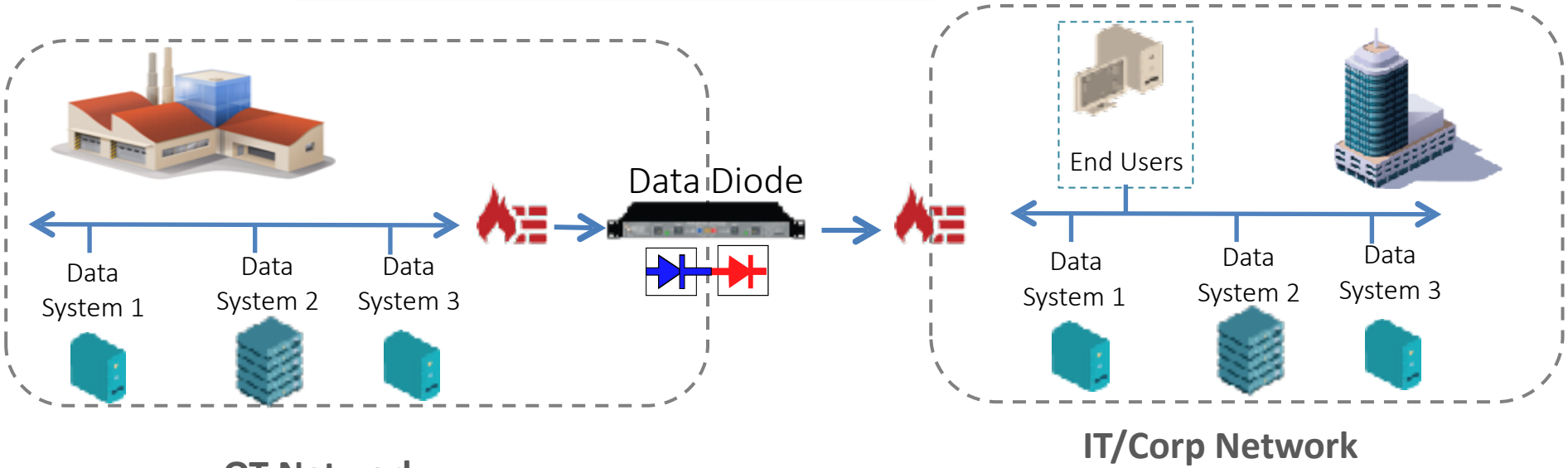


IT/Corp Network

Data Diode Network Security

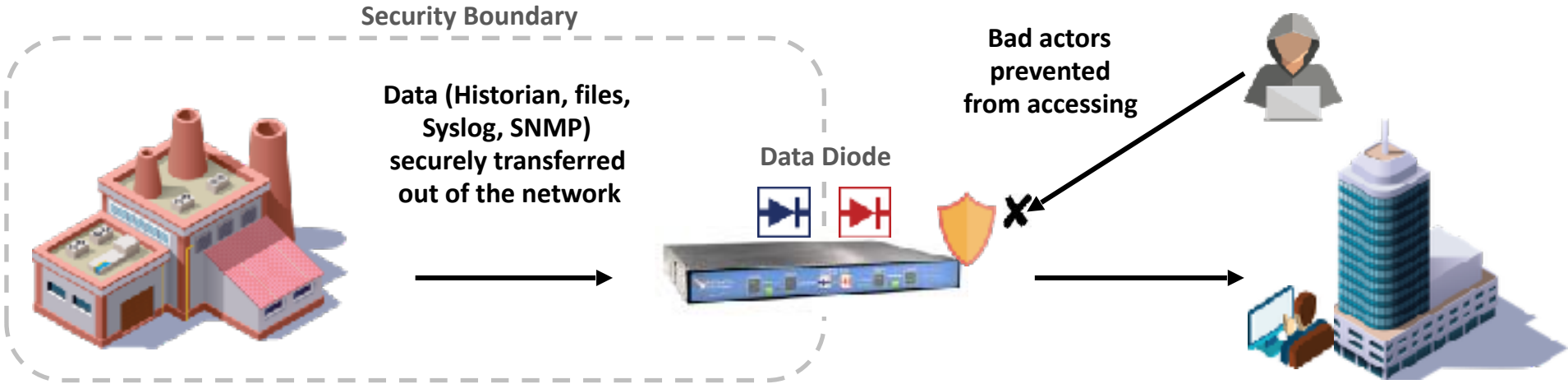


- EXCELLENT CYBERSECURITY
- ENABLES BUSINESS CONTINUITY



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)



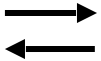
How One-Way Works in a Two-Way World

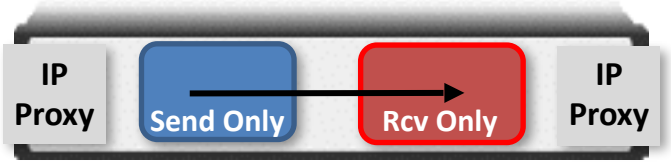
Existing

OT Network

IT Network

One-way Transfer Established





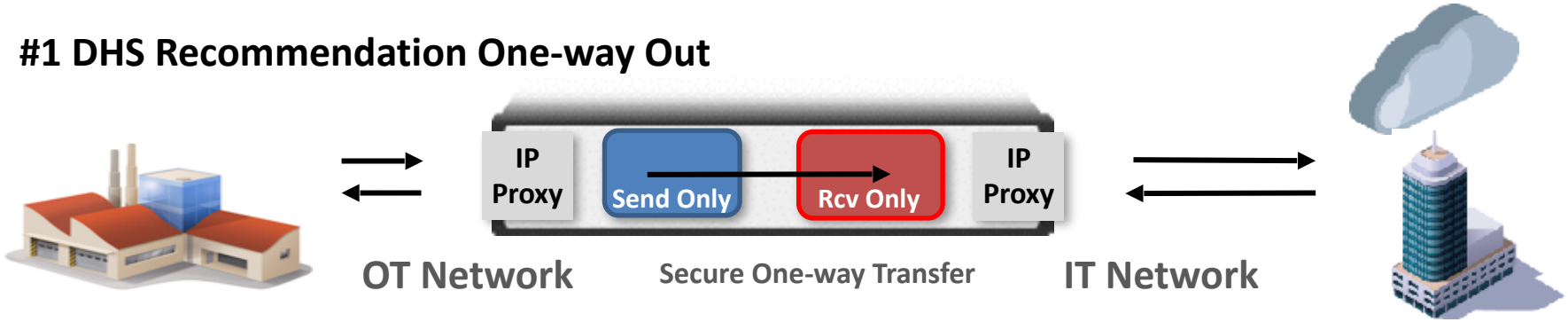
Secure One-way Transfer

OT Network

IT Network

One-Way out & One-Way in

#1 DHS Recommendation One-way Out



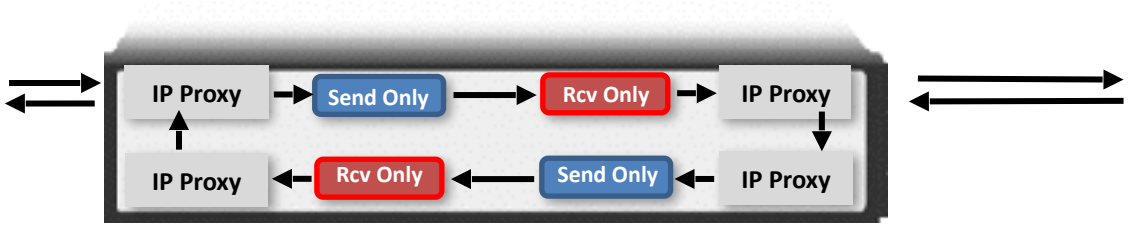
#2 DHS Recommendation One-way In

Data Content Filter with Antivirus
Data Content Inspection with Hash Code Validation
Whitelist File Types and File Names

Bi-Lateral for Remote Command and Control

DHS Strategy #3: Reduce Your Attack Surface Area -

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



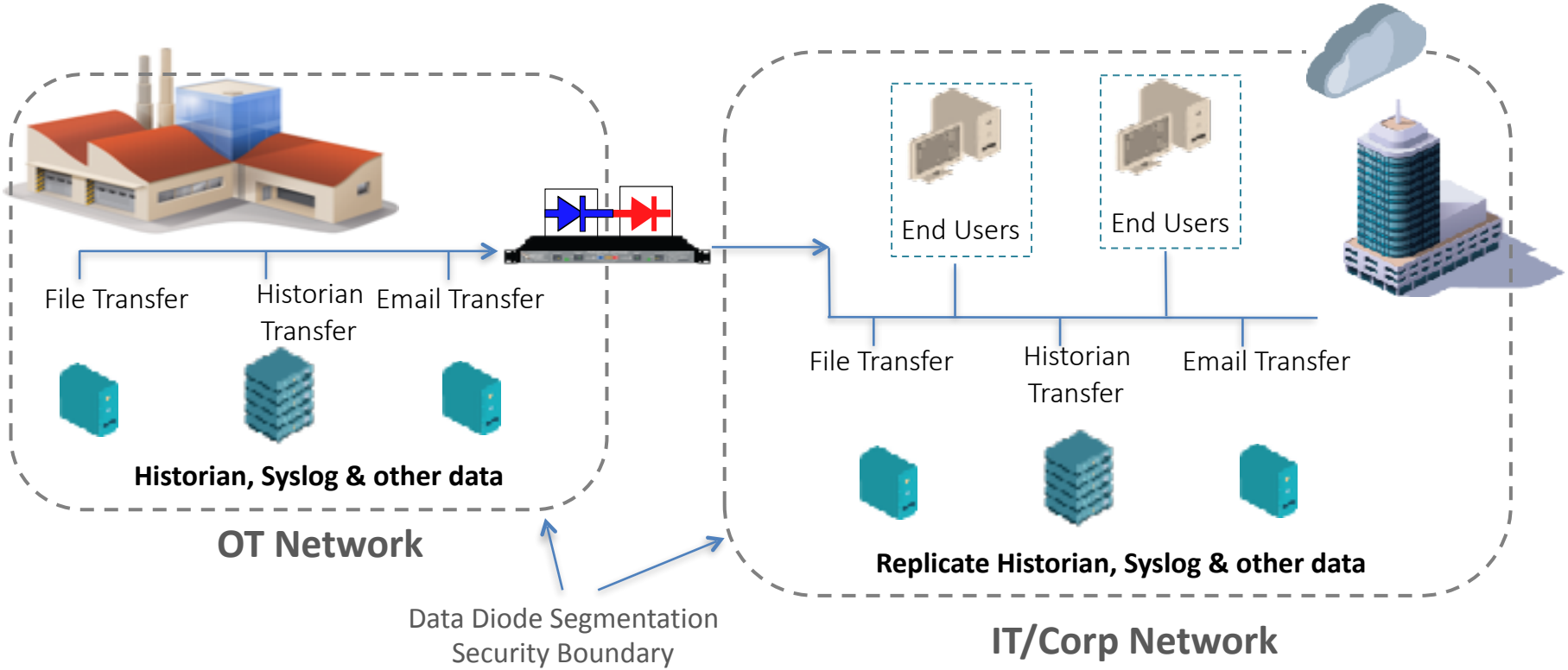
OT Network

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 within 1U enclosure
- Non-routable ATM protocol breaks
- TCP/IP proxies that break and join single whitelisted session

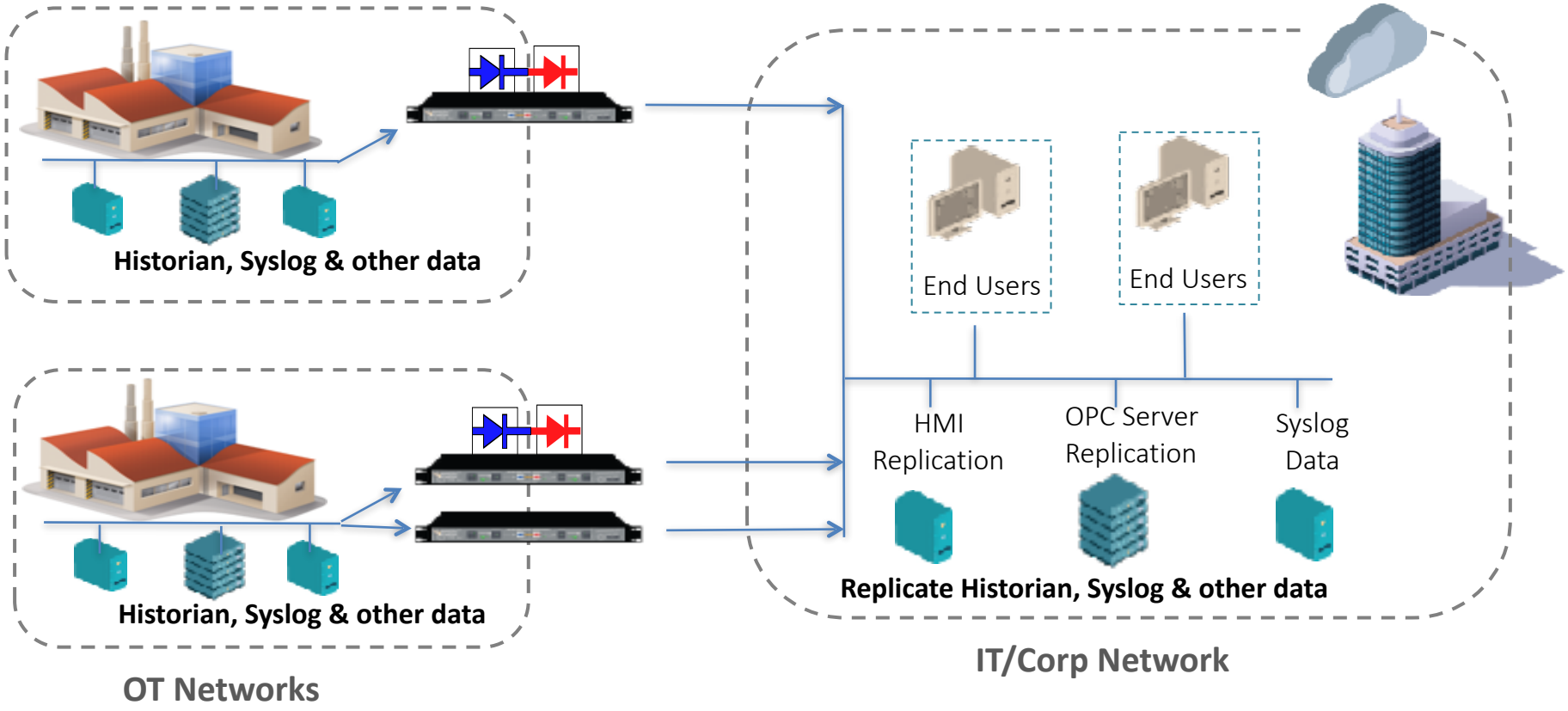
IT Network

Small Enterprise Architecture



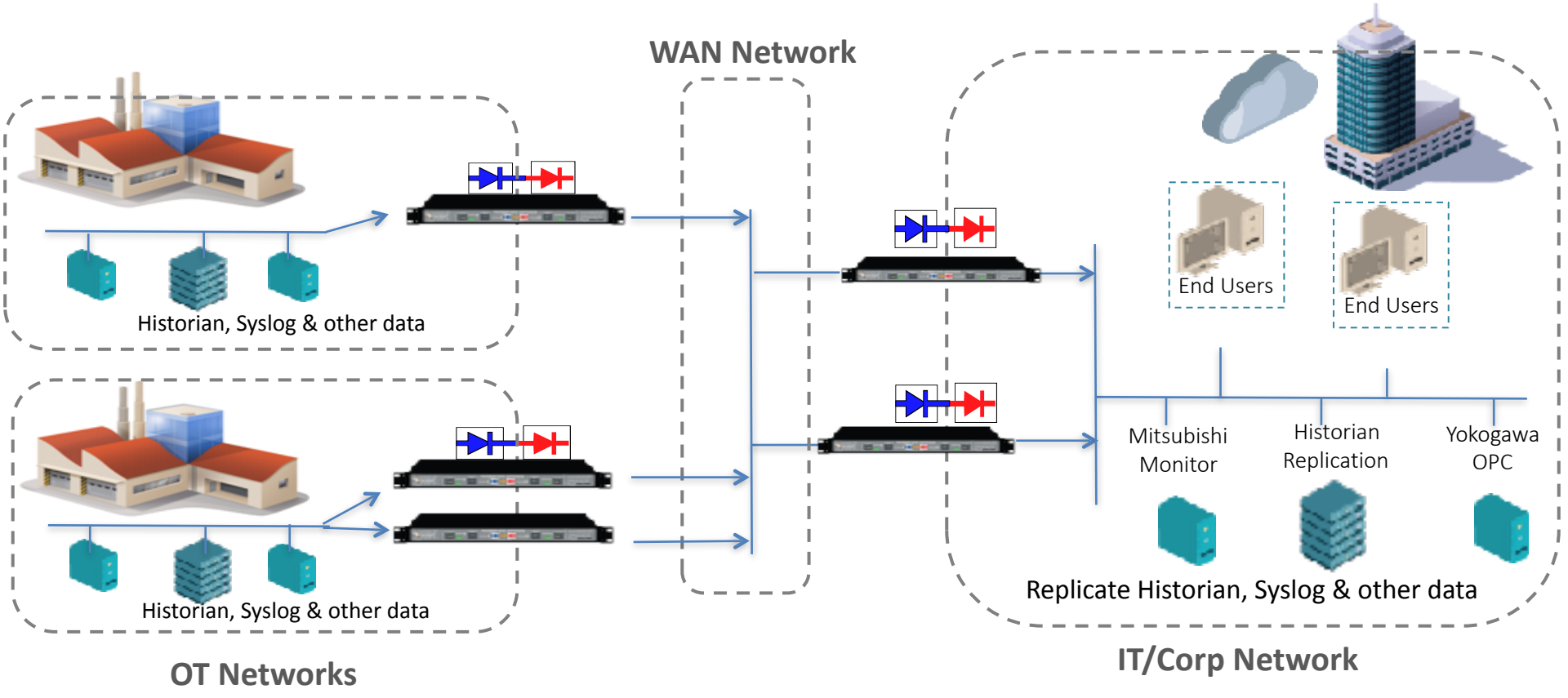
Supports simple and easy security and established data replication flows

Medium Enterprise Architecture



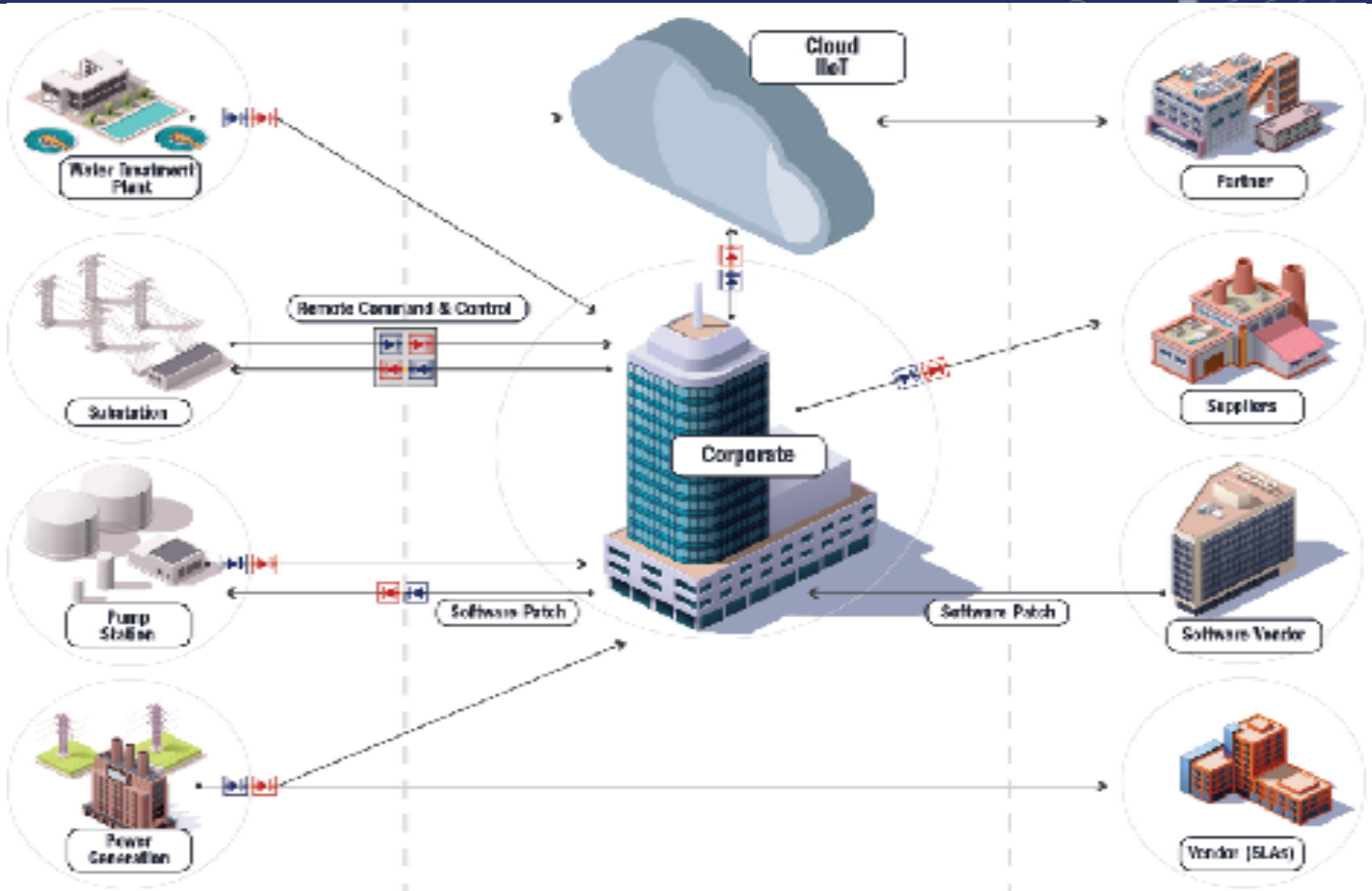
Meets the needs of any midsize company security and data needs

Large Enterprise Architecture



Supports largest enterprise needs with failover, redundancy and load balancing

Examples of One-Way in, One-Way Out and Bi-Lateral



Industry Use Cases

- **Power Generation, Substations, Transmission and Distribution (T&D)**
  - Gas 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 replication
  - Historian data
- **Financial and Banking**
  - Data transfer between secure and less secure locations
  - Financial transactions

Underlying Interface Technology

- **Network Hardware Interfaces**
  - Ethernet, serial, USB, dial up modem
- **Standard Vendor Software Interfaces**
  - Rockwell Factory Talk Historian, Rockwell Asset Center, Rockwell RS-Links
  - OSIsoft PI Historian
- **Network application interfaces:**
  - Syslog, SNMP, FTP, SFTP
  - Email (SMTP)
  - UDP, multicast, broadcast, unicast (video)
  - TCP/IP
- **Standards Bodies interfaces:**
  - OPC Foundation interfaces: DA, A&E, UA
  - Modbus

OPDS Data Diode Product Line

- OPDS-5D , OPDS-100D
  - Compact, single box solutions
  - Vertical DIN rail mount
  - Operate in Environmental Extremes
  - Market entry and high end solutions

- OPDS-100, OPDS-1000
  - 1U, 19” rackmount
  - IT environments
  - Variable bandwidth licenses
  - Scale from 10 Mbps to 1 Gbps

Demonstrations here at Automation Fair

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 Software Update Service
    1. Secure file transfer into the plant
    2. With Secure SHA hash code validation

Summary

1. Threats to the Connected Enterprise demand improved cybersecurity measures

2. US Dept. of Homeland Security provides strategies for protecting ICS:
   - Reduce the overall number of connections into the OT network
   - Convert two-way connections to one-way data diode connections
   - For remaining external command and control requirements:
     - use protected, single purpose, transient connections

3. Existing Owl Use Cases illustrate successful implementation of these DHS recommendations for protecting ICS

Owl Computing Technologies, Inc

Ridgefield, CT

+1 203-894-9342

www.owlcti.com

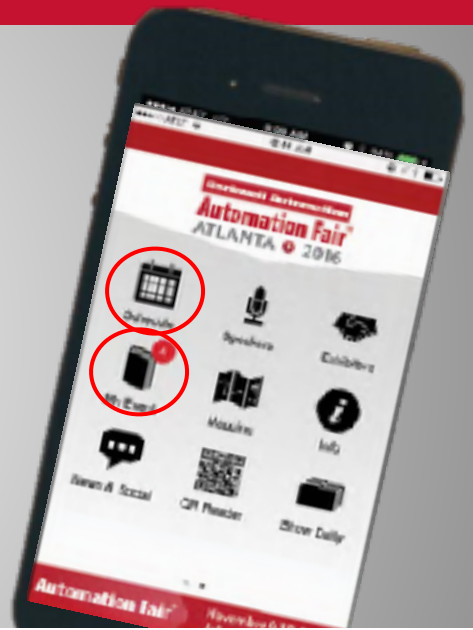
Dennis Lanahan
Email: dlanahan@owlcti.com
Phone: +1-203-894-9342

COMPLETE A SURVEY

Please take a moment to complete the brief session survey using the ROKEvent mobile app.

- **Login to the ROKEvents mobile app with your username and password (set up when registering for the 2016 Automation Fair® Event)**
- **Locate the session in “Schedule” or “My Event”**
- **Click on the survey icon in the lower right corner in the session details**

We want to hear from you and value your opinion!



Like what you heard? Need more information?
Let us know in the survey and we will contact you!