Meeting the Cybersecurity Standards of ANSI/ISA 62443 with Data Diodes

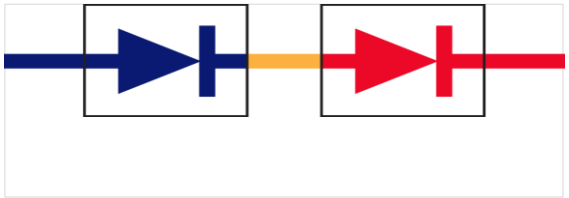
Dennis Lanahan

June 1, 2015

Securing the convergence of OT and IT with ST

Introduction to Owl

US Owned and Operated



Suite of cybersecurity products

2000+ Security Solutions Deployed

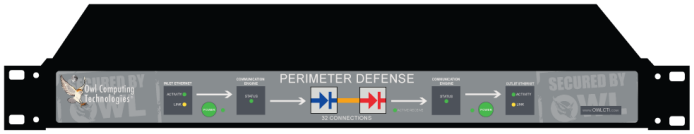
- Started 16 years ago with data diode technology from US DOE Sandia National Laboratory
  - Patented and Proprietary DualDiode technology
  - Hardware enforced, network protocol break, One way link (Owl)
- Over 2000 deployments globally
- Serve US DoD & Co-Commands, US Intelligence agencies, DISA, DOE, DHS, DOS and many other US Gov. agencies
  - Accredited solutions for unclassified, secret, top secret and coalition partner networks
- Supporting Critical Infrastructure for 9 years
  - Protecting over 200 process control sites in critical infrastructure
  - Oil & Gas, Nuclear, Fossil, and Hydro power generation, T&D, petrochemical, water/wastewater, mining
- Rockwell Encompass Partner since 2013

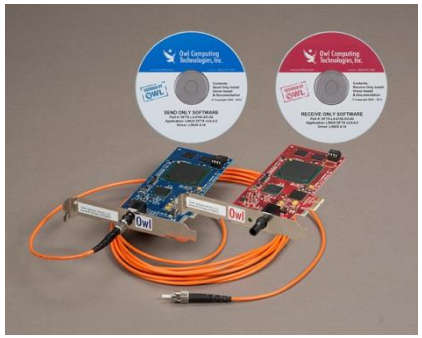
Introduction to Owl

Enabling the Connected Enterprise

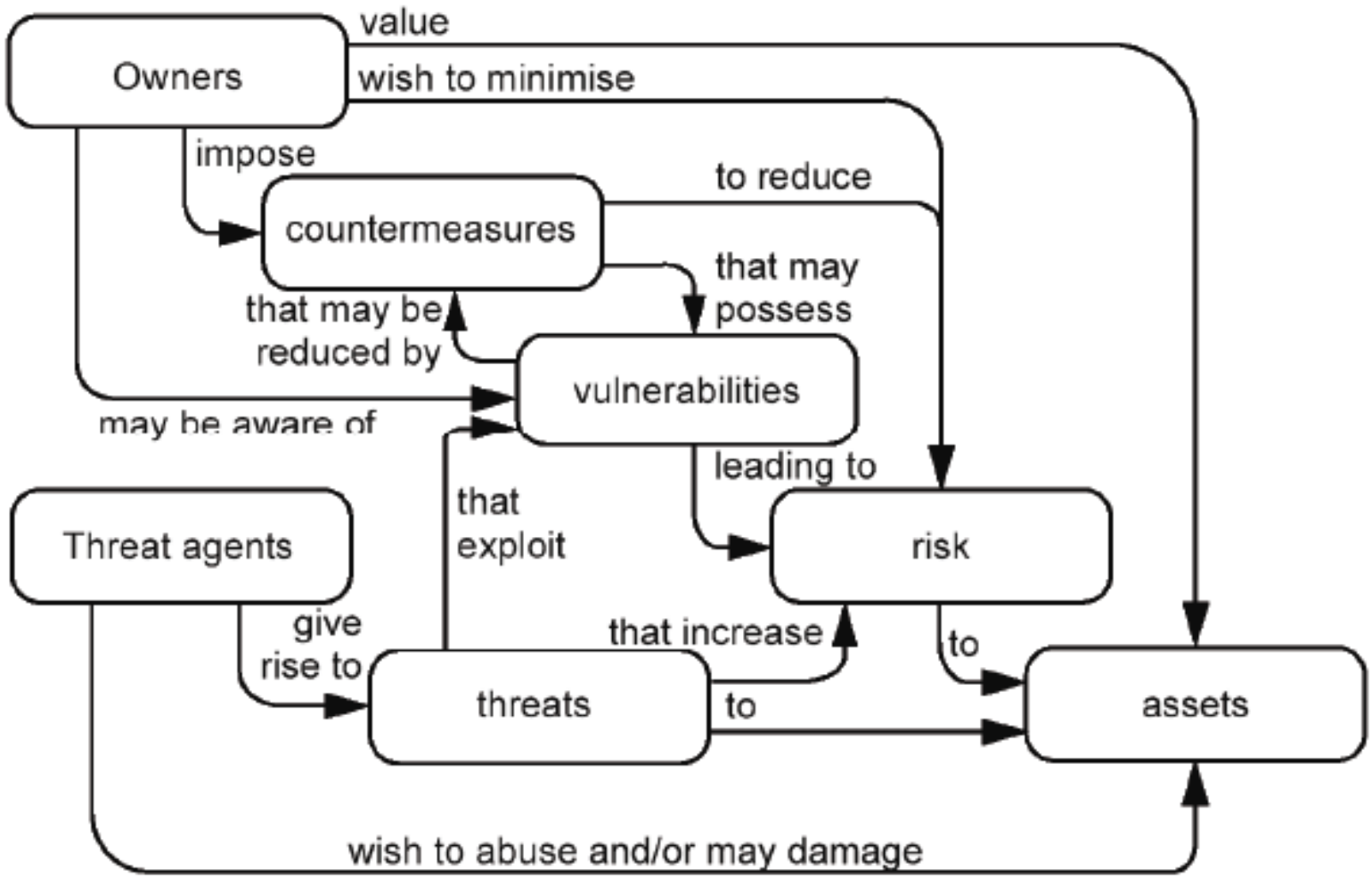
Securing the convergence of OT and IT with ST

- Owl DualDiode *is* Security Technology (ST)
- Designed and Deployed at the intersection of OT and IT
- Hardware Enforced Security Policy – cannot change
- Ethernet connectivity for ease of implementation in networks
- Rack-mounted & DIN Rail appliance utilize DualDiode technology





Why we need Cybersecurity



* Common Criteria Part 1: Introduction and general model, 2005, v2.3

Cybersecurity Standards

- ANSI/ISA-62443
- NERC CIP 002-009
- NIST SP800-82
- API Standard 1164
- ChemITC
- AWWA G430-09

- Owl has mapped solutions to the various standards
- Same implementation process applies

Definitions (ANSI/ISA 62443)

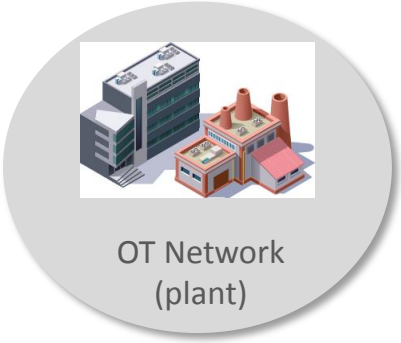
- **Security Zone:**
  - A logical grouping of physical, informational and application assets sharing common security requirements.

- **Conduit:**
  - Communication flows that represent information exchanges between security zones.

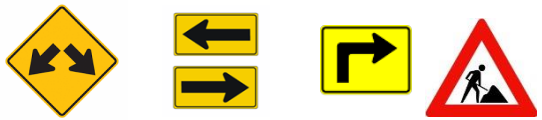
- **Defining Security Zones:**
  - In building a security program, zones are one of the most important tools for program success and proper definition of the zones is the most important aspect of the process.

How to Approach a Standards Based Security Implementation

1) Define the network security zones



2) Define work, workflows and data needed within and between zones

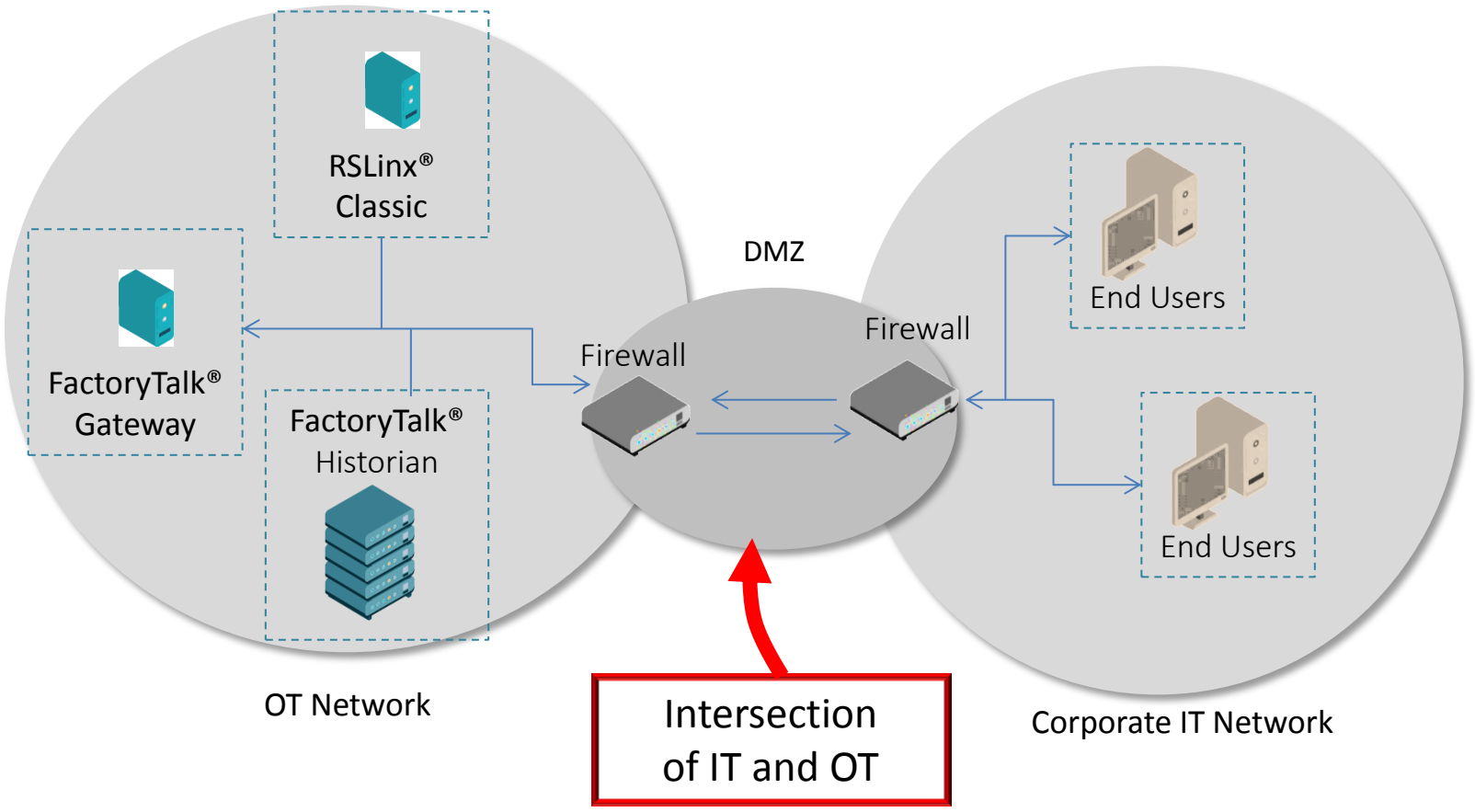


3) Define security policies for network zones

4) Define security solutions that enable and enforce requirements

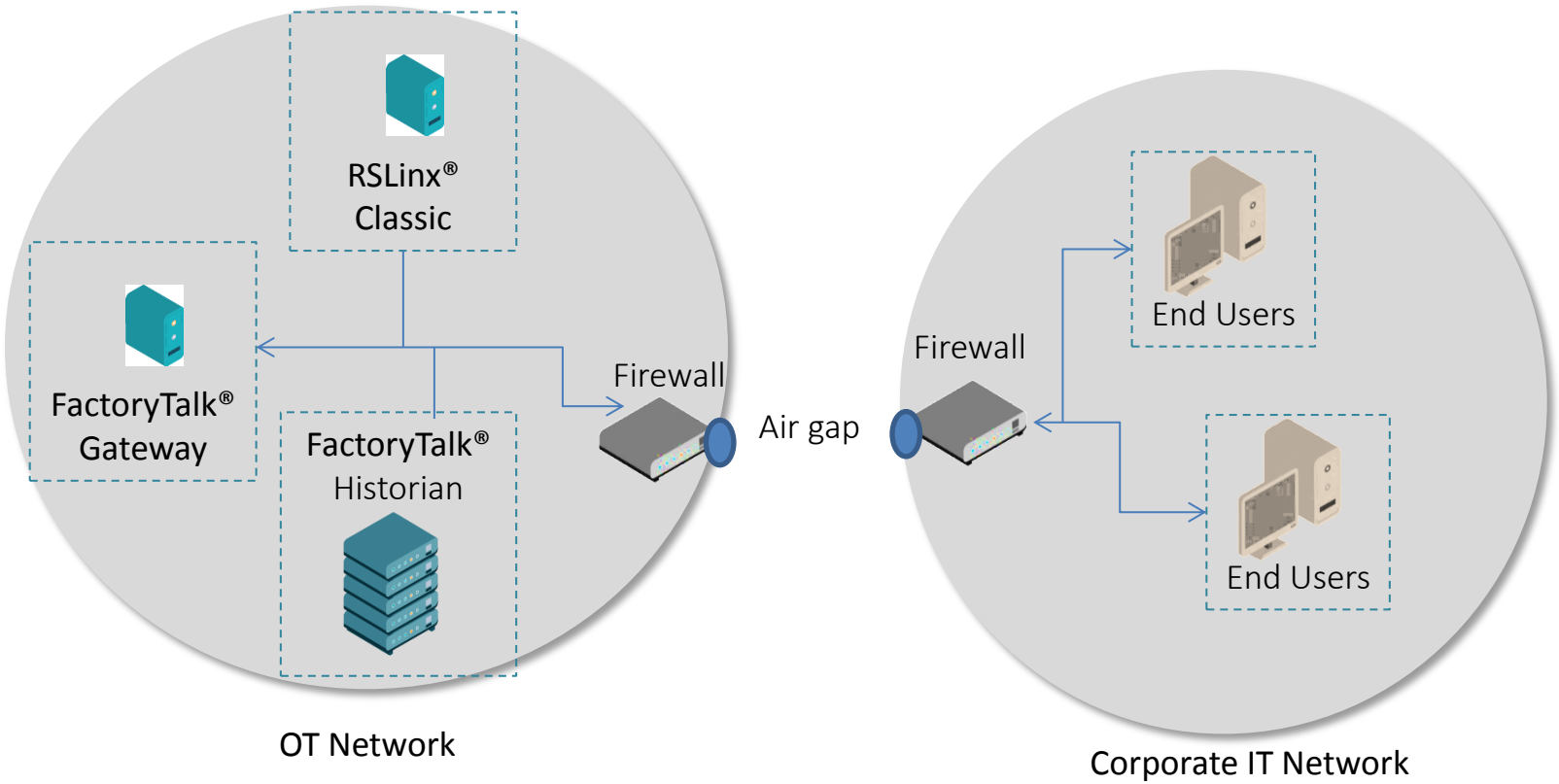
Typical Industrial Network

- EXCELLENT BUSINESS CONTINUITY
- LIMITED CYBER SECURITY



Air gap network security

- EXCELLENT CYBER SECURITY
- *LIMITED, OR NO, BUSINESS CONTINUITY*



The Connected Enterprise requires both

EXCELLENT BUSINESS CONTINUTIY

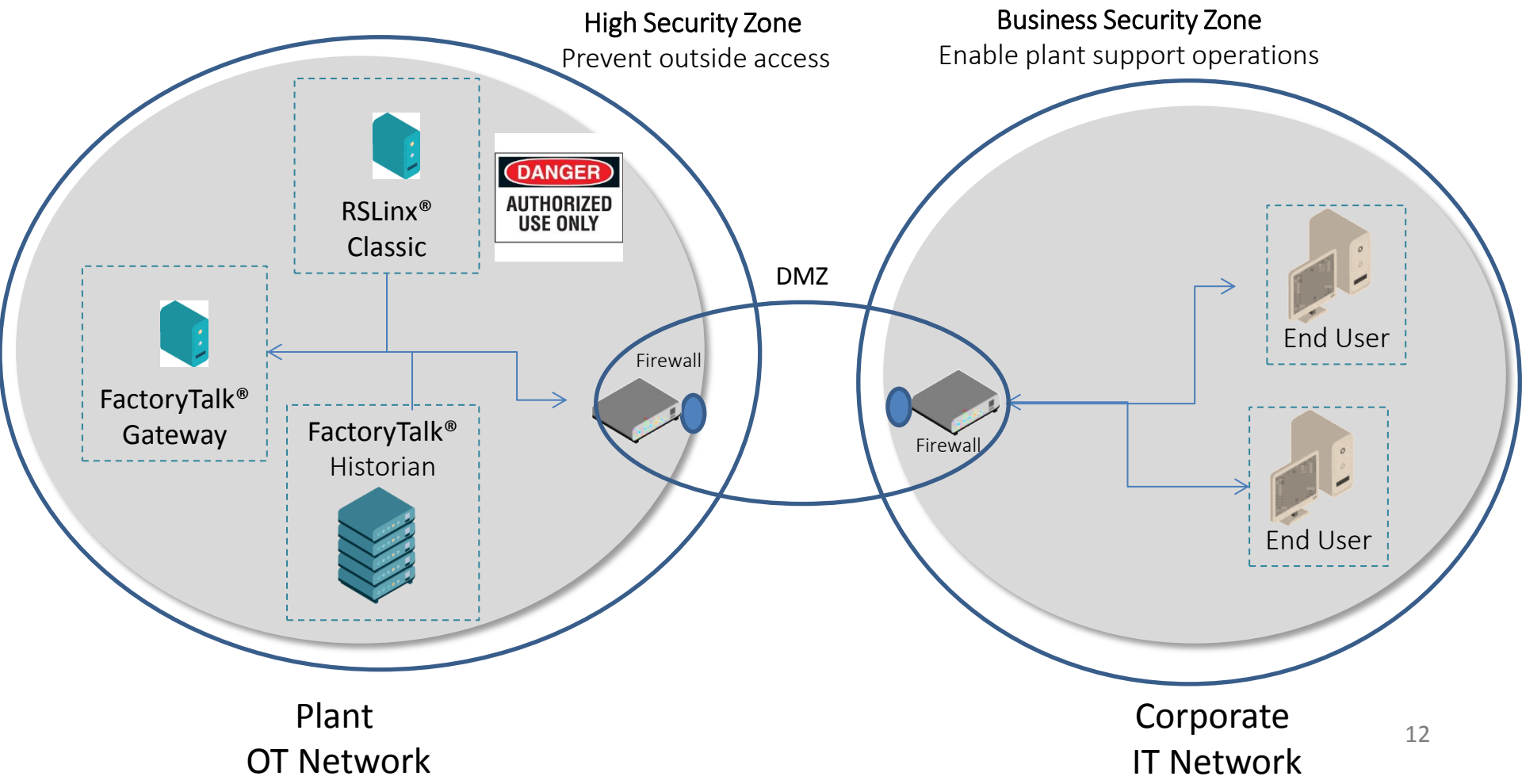
AND

EXCELLENT CYBER SECURITY

How do you Achieve this?

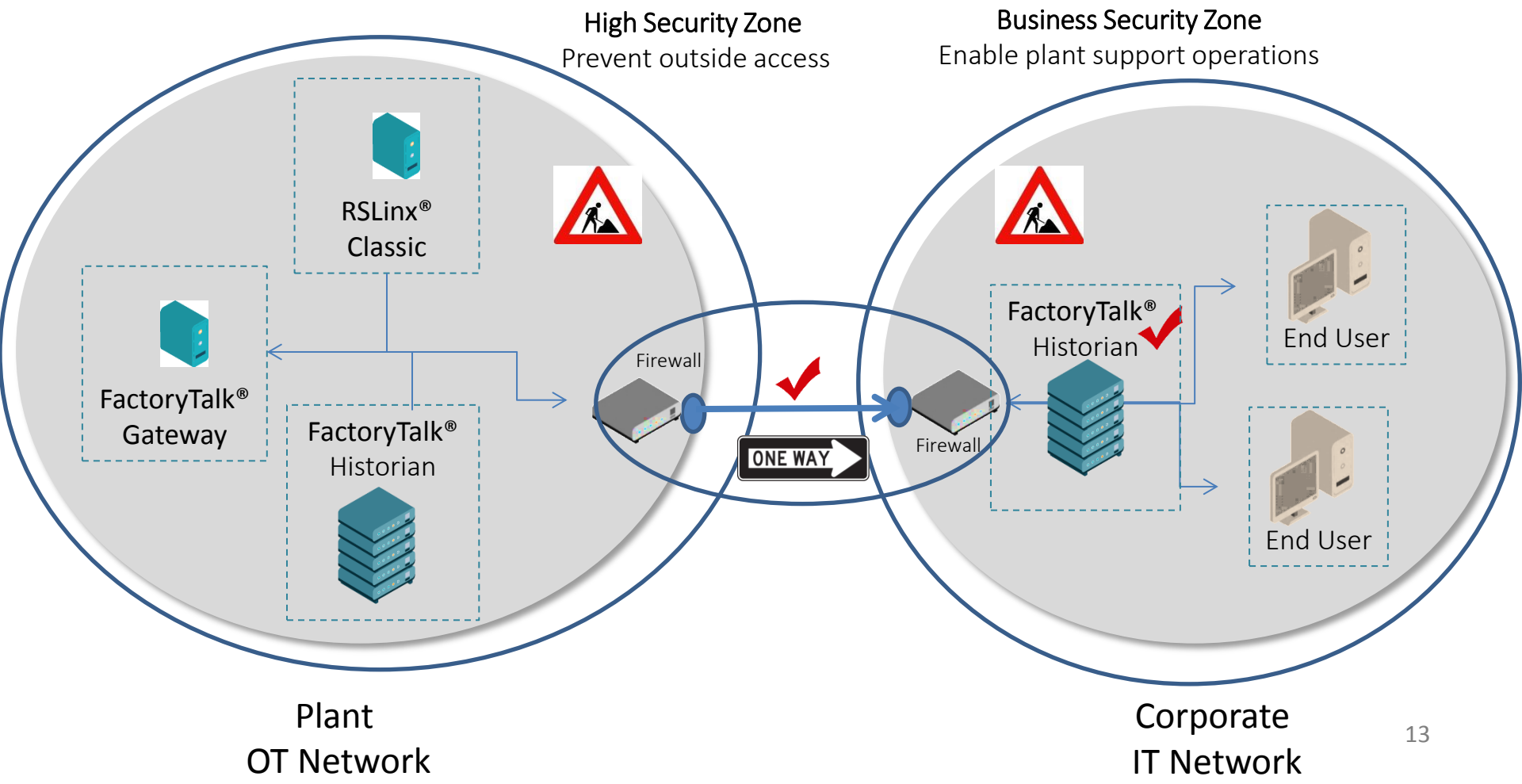
Key Decisions to Remedy Business Challenges

1. Define security zones



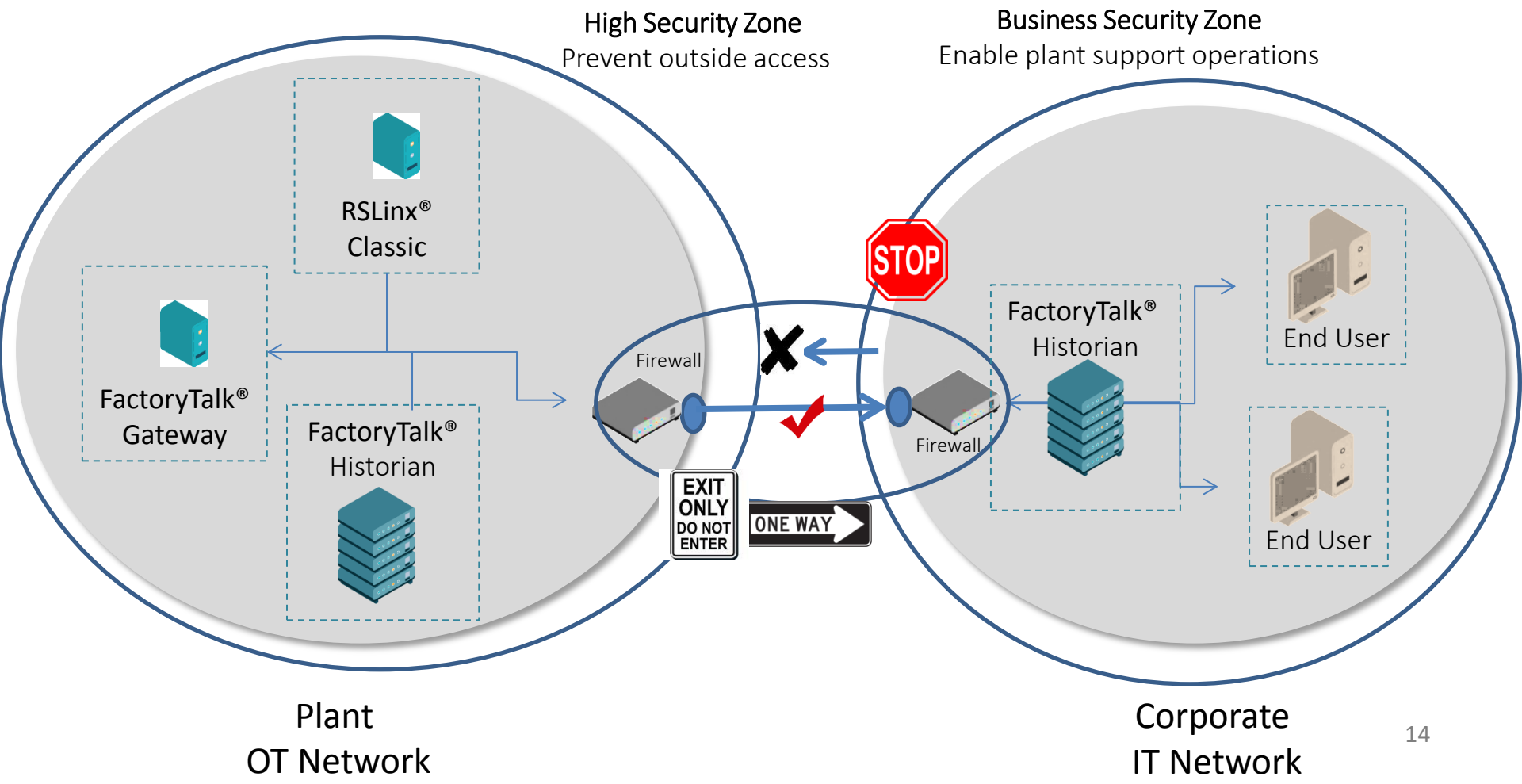
Key Decisions to Remedy Business Challenges

1. Define security zones
2. Define work zones, workflows and data transfers within the zones



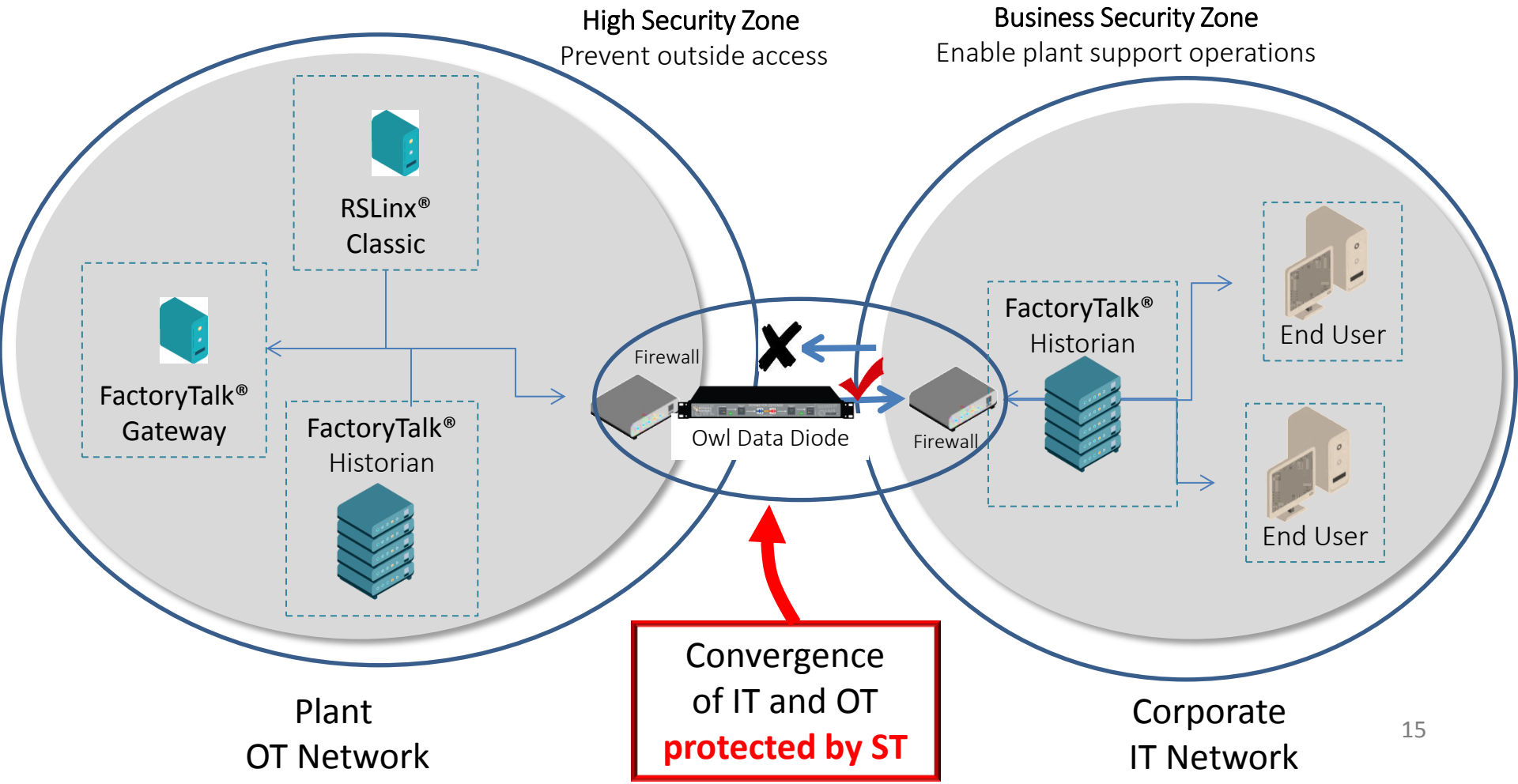
Key Decisions to Remedy Business Challenges

1. Define security zones
2. Define workflows and data transfers within the zones
3. Define security policy – data transfers out, no attack vectors in



Key Decisions to Remedy Business Challenges

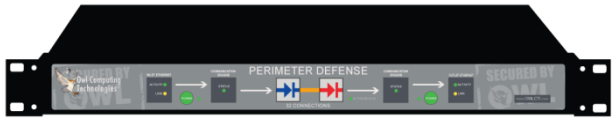
1. Define security zones
2. Define workflows and data transfers within the zones
3. Define security policy – data transfers out, no attack vectors in
4. Define security solution to support all requirements

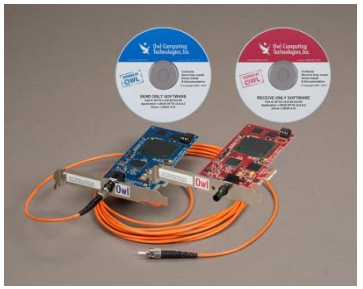


Features = Benefits

- ✓ **Well defined security zones and policies = Security standards met**
- ✓ **Separation of network domains = Improved cyber security**
- ✓ **OT Network secured = Increased Plant Reliability**
- ✓ **OT data flows to IT = End users in IT domain have data so they can work**
- ✓ **Business continuity = Improved business operations**
- ✓ **Owl's Security Technology = Enables the Convergence of OT and IT**

Data Diode Hardware Security Policy

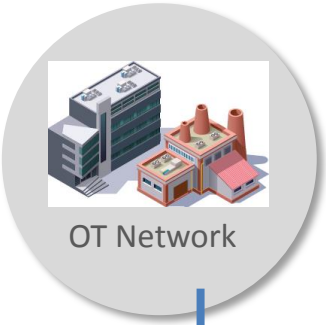




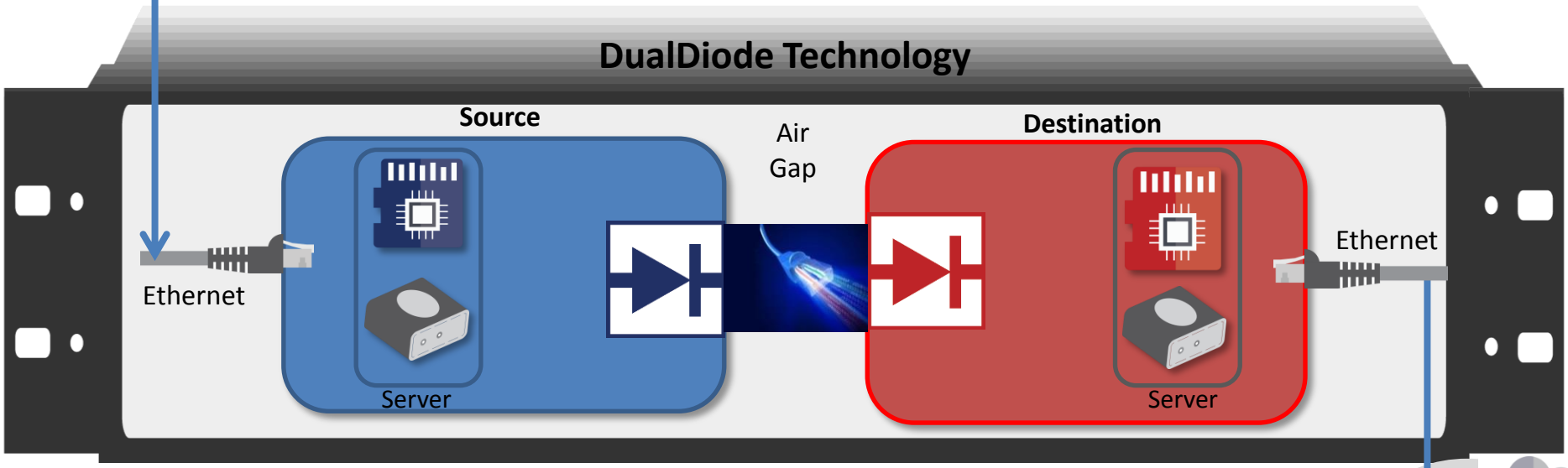
- **Hardware enforced one-way only data transfer**
  - One-way data flow out of secure network zone
  - No external access into the secure network zone
  - No bidirectional TCP/IP connection
  - Software attack can not modify hardware security policy

- **Network Confidentiality**
  - Network protocol break = Asynchronous Transmission Mode (ATM)
  - Source Network IP data -> ATM -> Destination Network IP data
  - Only the “payload” of IP data packets cross the DualDiode
  - Data Diode remains “invisible” on the network
  - Data Diode has no IP or MAC address
  - Protects all IP and MAC addresses of the source network devices
  - No external network scanning or mapping of secure network

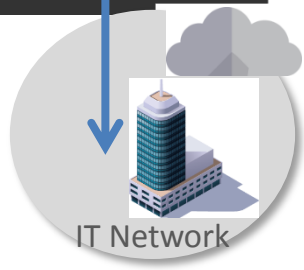
DualDiode Operational Architecture



- DualDiode hardware enforced security solution
- Two diodes, in series, enforce “air gap” network separation
- One-way hardware constrained by single fiber optic cable



- Diode server terminates each network endpoint
- Hardened Linux OS further secures each server
- Servers only support specific & whitelisted data transfer applications

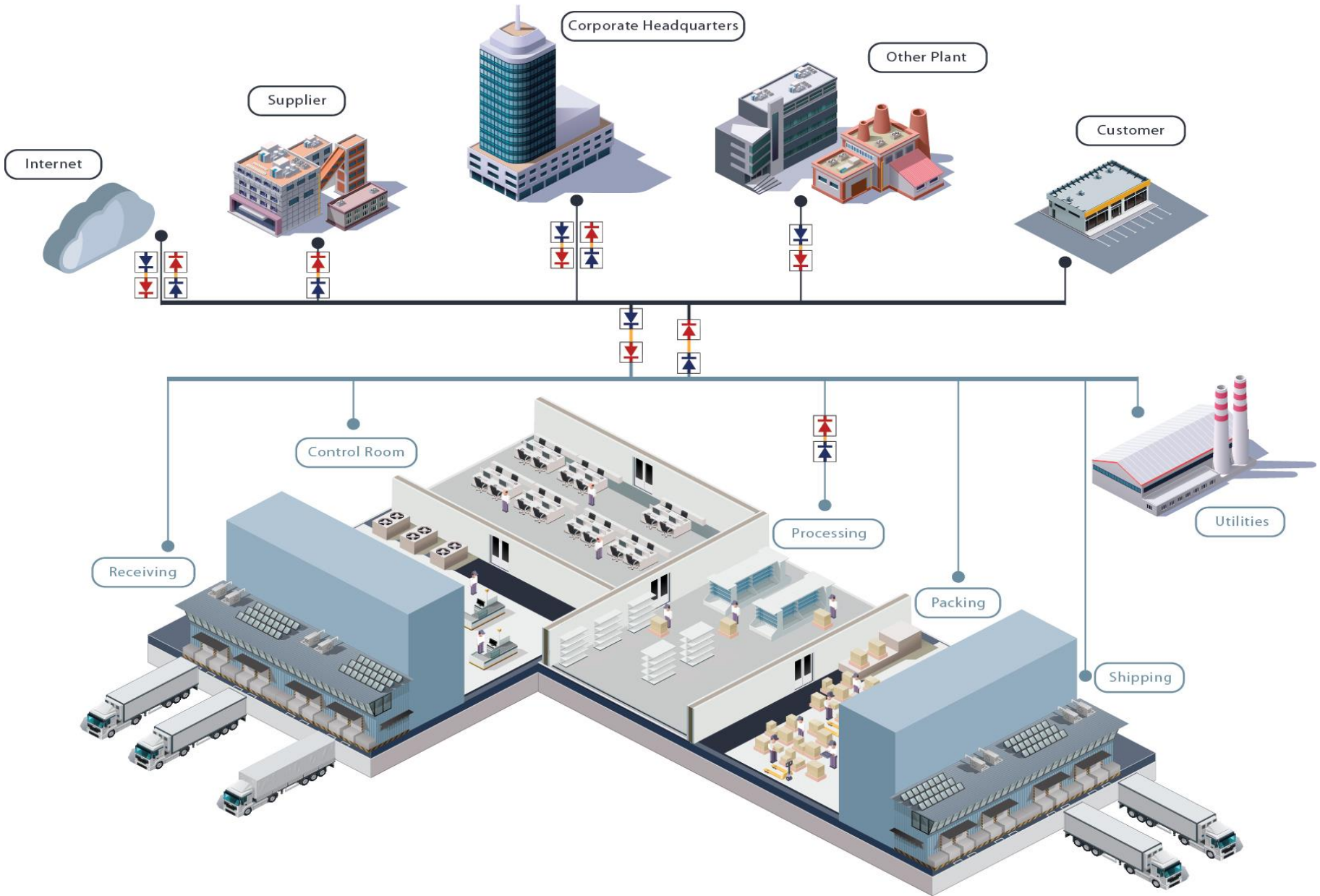


Data Transfer Applications

- **Owl Supports Rockwell Applications**
  - **RSLinx® Classic**
  - **FactoryTalk® Gateway**
  - **FactoryTalk® Historian**

- **Owl Supports other Transfer Applications**
  - **Historian replication**
  - **SQL Database replication**
  - **Syslog transfer**
  - **Email Alerts and events**
  - **Remote HMI Screen replication**
  - **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…**

Enterprise Wide Deployment Locations



Summary

1. Pick a cybersecurity standard
2. Define your network security zones
3. Define work, workflows and data transfers needed
4. Define network security policies
5. Define security solution to support all requirements

Owl Secures the convergence of OT and IT with ST


SECURED BY
OWL