# Tennessee Valley Authority's (TVA) Data Diode Program

*ICSJWG Spring Conference*
*May 8 - 9, 2012*


*Presenters:*
*Carl Scarbrough, Cyber Security Program Mgr, TVA*
*Ron Mraz, President & CTO Owl Computing Technologies, Inc.*


Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

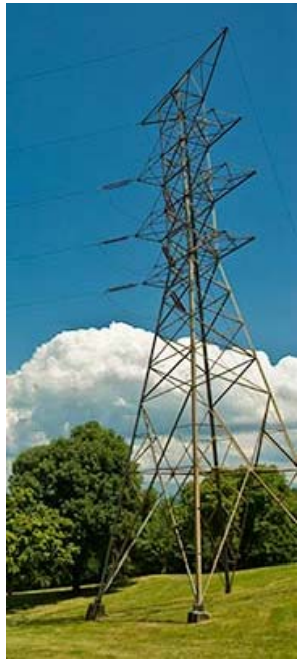
# TVA Data Diode Program

## Purpose

*Provide a general overview of the TVA Data Diode program and an overview of the underlying technology provided by Owl, so that each of you will have a better understanding and so you might see how the technology could fit into your company's security program*

Agenda:

- Why TVA chose Data Diodes
- One-way Data Diode technology
- Benefits & Challenges of using Data Diodes
- Remote Monitoring & Management
- TVA's Implementation – Fossil, Nuclear, & Hydro



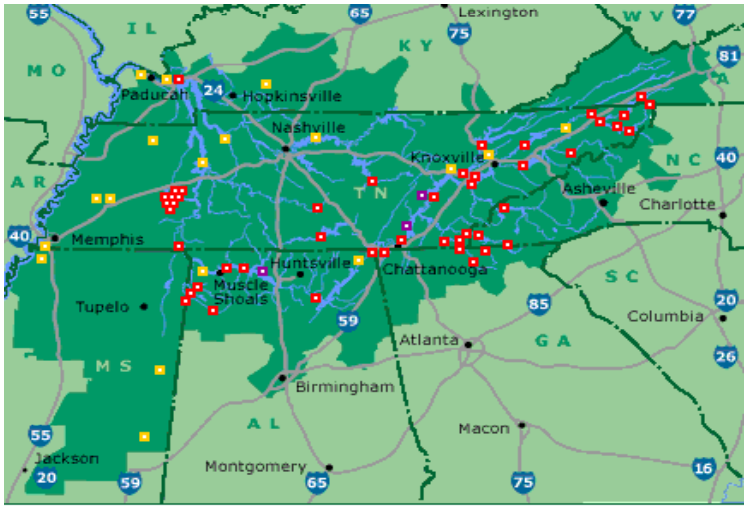
Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

# About TVA

- Federal utility that provides electricity for 9 million people in parts of seven states
- Nation's largest public power company
- Provides wholesale power to 155 municipal and cooperative power distributors, and by directly serving 57 large industries and government installations
- Annual sales revenue in 2011: $11.7 billion
- Generating capacity: 5th in the nation



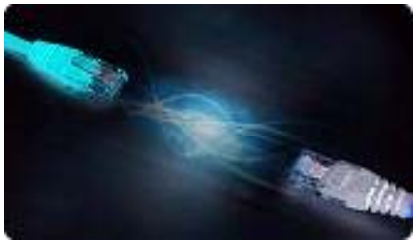

Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

# Why TVA Chose Data Diodes

- **GAO audit** released in May 2008 found that TVA needed to address weaknesses in control systems and networks.
  - "Although TVA used multiple network segments to separate more sensitive equipment, such as control systems, from the corporate network, **weaknesses** in the **separation** of these network segments could allow an attacker who gained access to a less secure portion of the interconnected network, such as the corporate network, to **compromise equipment** in a more secure portion of the interconnected network."
- **TVA Senior Management** wanted to completely air gap the control systems from the corporate network.
  - This would not have allowed critical plant data to be received on corporate applications



- One of the **best defenses** to provide secure protection of essential cyber assets from various ***threat challenges***

# Threat *Challenges*

- Zero-day attacks - becoming more complex
  - Stuxnet: total of four zero-day vulnerabilities
- Growth rate of OS & application vulnerabilities rising
  - Microsoft Fixes 64 Bugs In Biggest Ever Patch Tuesday Update, 4/12/11
- Poor patching of systems & software – *especially ICS's*
- Internal attacks

  - "security breaches caused by once-trusted employees and contractors account for one in five attacks across all industry sectors", *2/28/11, Federal Computer Week*, http://fcw.com/articles/2011/02/28/feat-cybersecurity-insider-threats.aspx
- External attacks

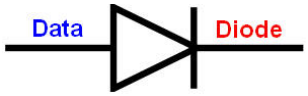
  - Twitter channel recently promised that "Anonymous (hacktivist group) will target national infrastructure", *3/21/12, Information Week,* *http://www.informationweek.com/news/security/attacks/232602962*

# Threat *Challenges* – cont.

- "Government network security experts told a U.S. Senate panel federal networks are thoroughly penetrated by foreign spies. They said current *perimeter-based defenses* that attempt to curb intrusions are outdated and futile."[1] *, 3/21/12, Threatpost*

- "the US Department of Homeland Security (DHS) said that in the period from October 2011 to February 2012 there had been 86 reported attacks on computer systems that control US critical infrastructure" [2], *3/28/12, Energy Risk*

**All of these threats are mitigated and reduced in risk by using a Data Diode based one-way technology.**

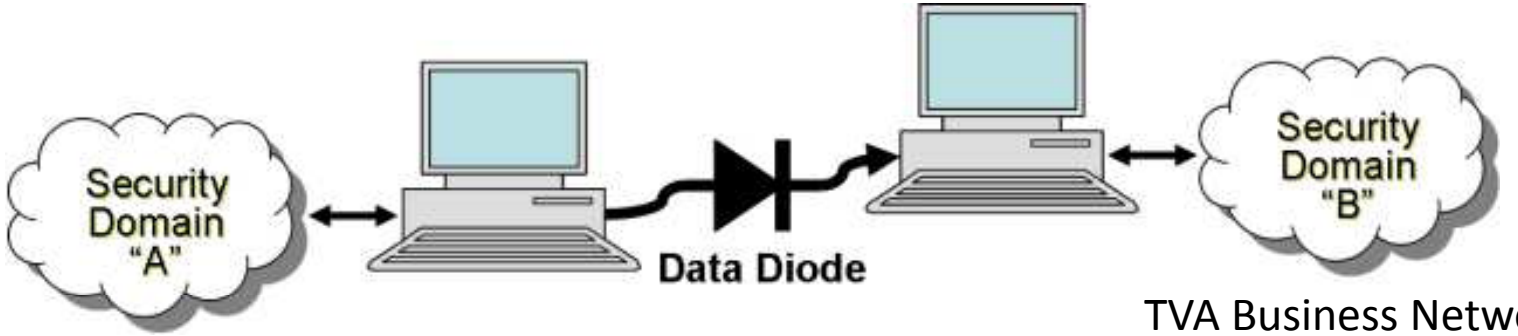



[1] http://threatpost.com/en_us/blogs/inadequate-pay-outdated-approaches-and-bureaucracy-all-contribute-foreign-ownership-federal-sy

[2] http://www.risk.net/energy-risk/feature/2164202/assessing-cybersecurity-power-grid

# What is a Data Diode?

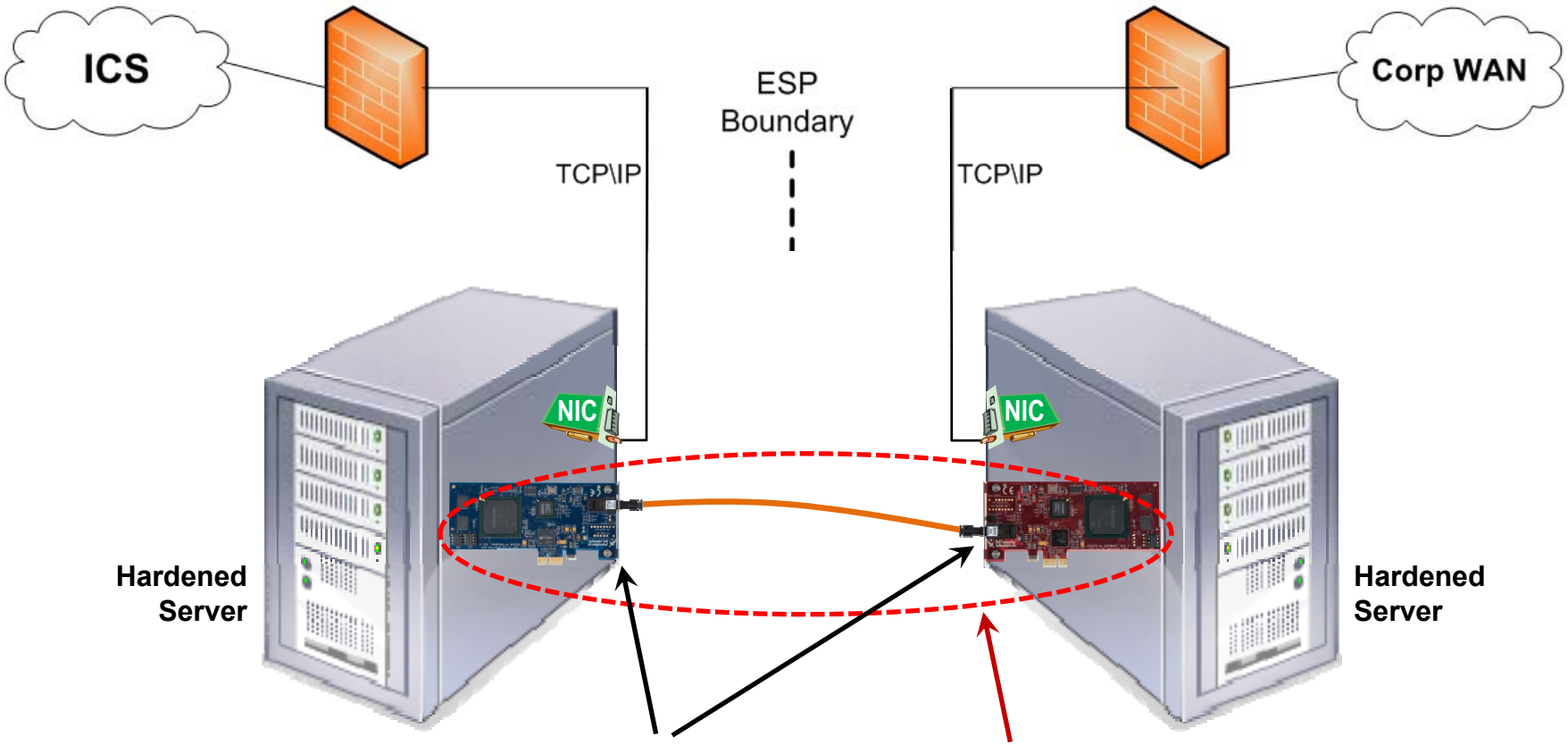
An appliance or device that creates a unidirectional (one-way) network to ensure that data travels *securely* in only one direction




TVA Business Network

TVA Control System

# TVA's Data Diode Implementation




**Data Diode Device**
**Owl 155 v4 Communication Cards**
**EAL-4 Certified**
**NO IP or MAC Address**

**Layer 1-2 Proprietary Protocol**
**NON-routable**

Owl Computing Technologies, Inc.

SECURE ONE-WAY
INFORMATION TRANSFER

TVA

# Owl Computing Technologies, Inc.

- US owned & operated

  All US based Controlled Supply Chain
  All US based: R&D, manufacturing, sales & services

- Develops & markets

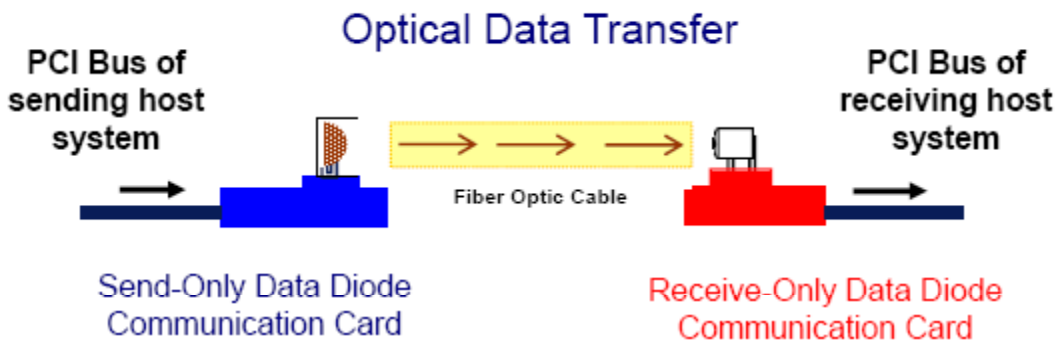
  Owl Perimeter Defense Solution
  One-way transfer systems
  Configuration management & life cycle support

- Over 1,200 security solutions deployed

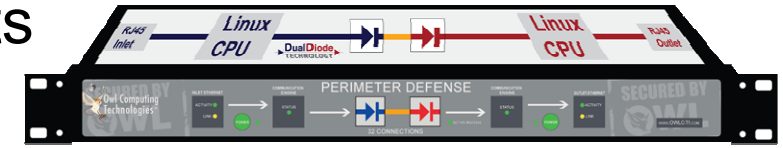
  Nuclear, Fossil & Hydro generation,
  OSI PI, TVA Dataware, GE Proficy, Invensys ArchestrA, DSS R&R, Scientech, EDNA
  US DOD, US Intelligence Agencies, Telecommunications

# One-Way Network

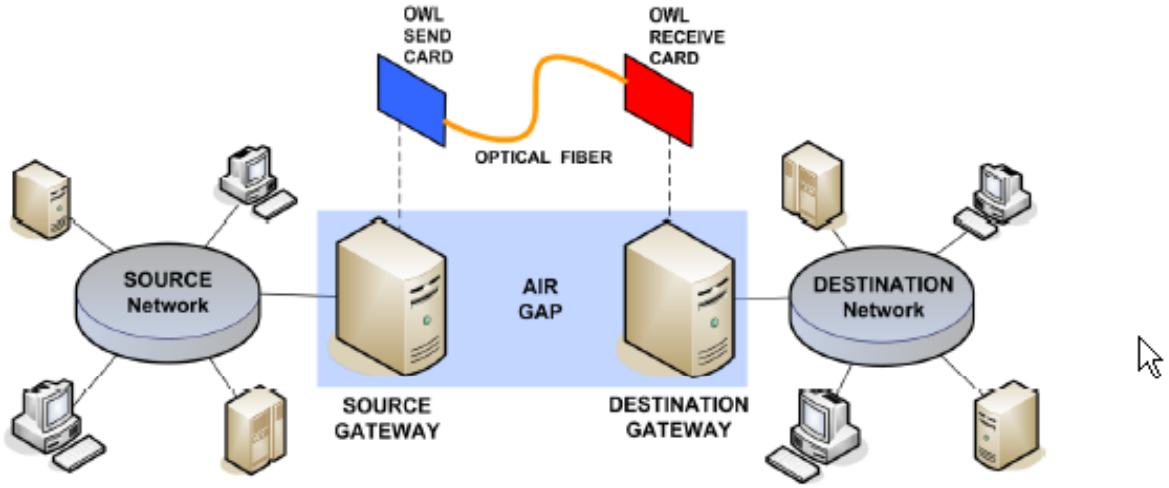
One-way network is enforced at the physical layer or Layer 1 of the OSI model



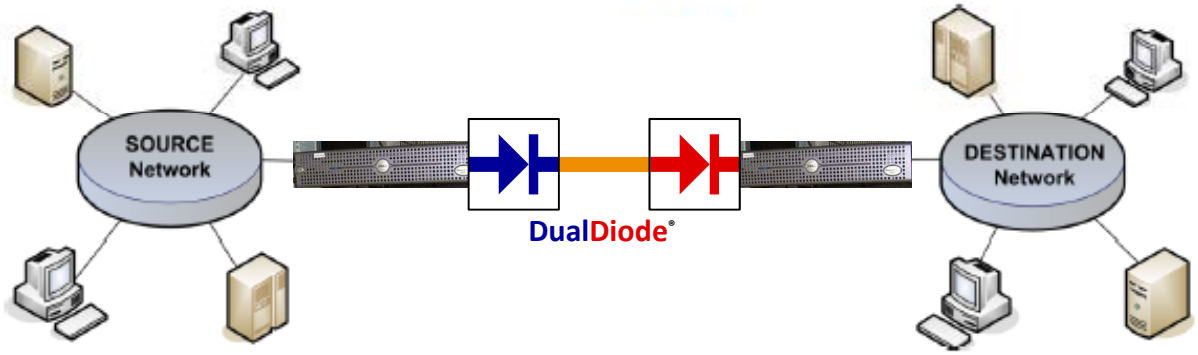
- Sending computer connects through LED transmitter
- Receiving computer connects through an optical receiver
- Certified NIAP EAL 4



# Typical Installation




**Send and Receive Owl Cards installed in host computer platforms…**



# Owl DualDiode Technology

- Owl technology is NERC CIP compliant
  - ✓Owl diodes have No network address (MAC)
  - ✓Owl diodes are Non-routable across the ESP
  - ✓Owl diodes do Not route IP data across the ESP
  - ✓A Non-routable connection is used across the ESP
  - ✓Non-routable ATM cells transfer across the ESP

- Types of data transfers
  - ✓ TCP/IP
  - ✓ UDP
  - ✓ File transfers

Owl 155 v.4 Cards
155Mbps link speed

15 MByte/sec throughput
Multimode
PCI-x / PCI-e

Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

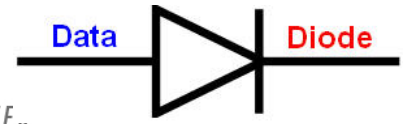
# Benefits

## Benefits

- Guarantee of one-way only communications out of control system network is enforced in hardware.
- No connection to outside network via routable protocol (no MAC or IP addr)
- Provides the best protection technology for securing cyber assets from outside threats.
- Peace of mind: password vulnerabilities non-existent, physical access to bypass the diode is the only threat
- SE Linux Security Policies to harden OS in transfer systems.
  - DoD Security Technical Implementation Guides.
- Role based access menus for administration

Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFE..

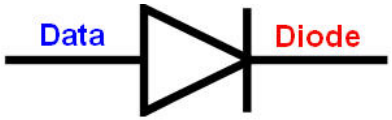



TVA

# Challenges

## Challenges

- On-demand 24x7 remote access to control system for IT, Engineering, and Operations support is limited or eliminated
  - Increases local responsibilities for both site and corporate support
- Verifying data integrity – verifying existing applications can co-exist with one-way data transfers  OSI PI, TVA Dataware, GE Proficy, Invensys ArchestrA, DSS R&R, Scientech, EDNA
- Monitoring – integration into current procedures takes planning
- Footprint of solution requires planning
- Bandwidth needed at the ESP requires planning



# *Owl Performance Management Service (OPMS)*

- Global View of Monitored Systems Status
  - Monitor individual crossing, and multiple crossings
  - Status of individual connector transfers
- Log File Monitor of Owl Applications
  - Errors noted from send-only & receive-only log files
- Application Support
  - All Owl applications
  - Custom application log files
- Browser-based Monitoring System
  - Supports Microsoft Internet Explorer 6+, Mozilla
  - User authentication, data encryption

# TVA Implementation

## Fossil Power

Coal – 10 coal fired plants

## Hydro Power

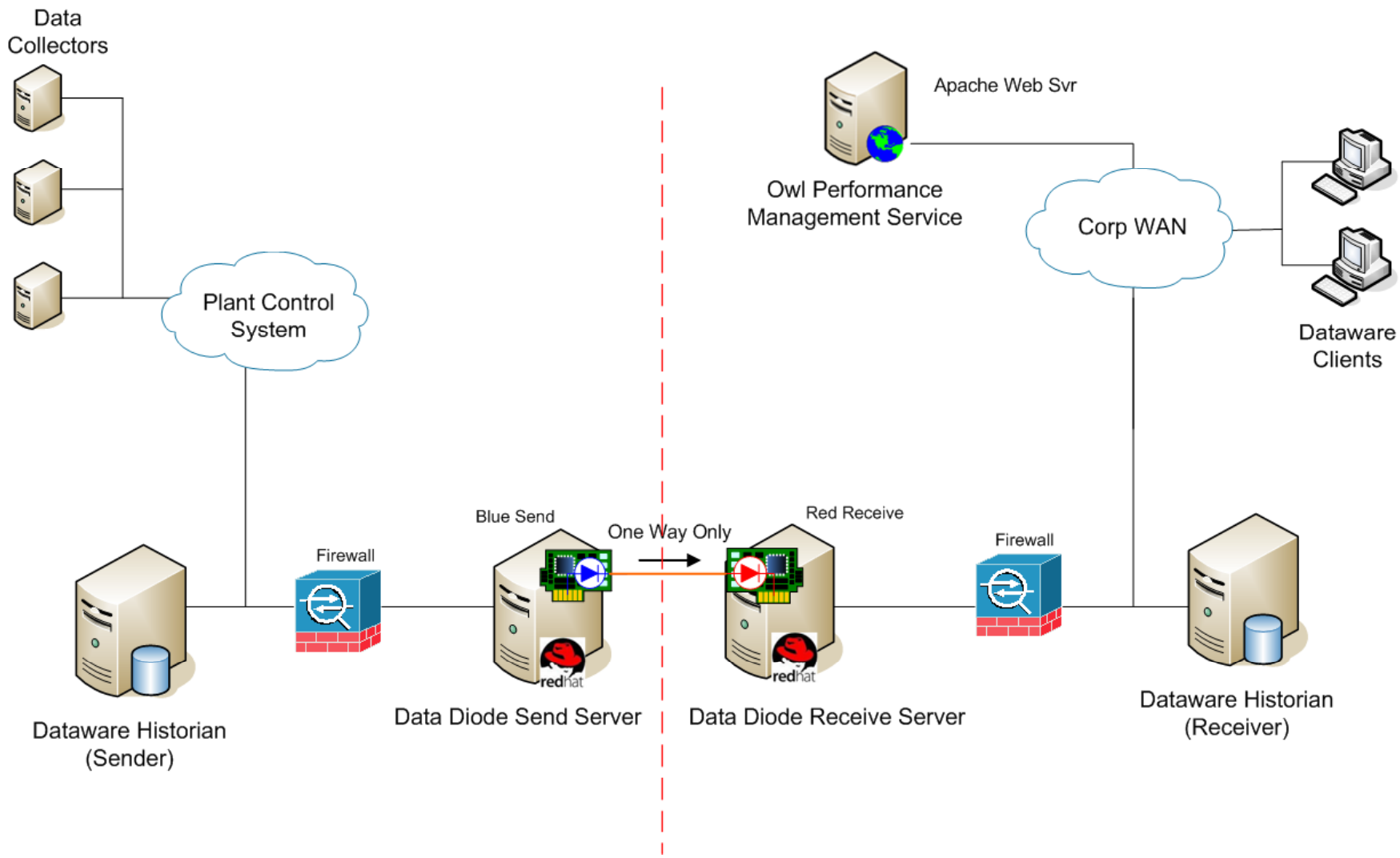
29 Hydroelectric plants

## Nuclear Power

3 Nuclear plants

# Typical Fossil Data Diode Implementation

(Similar for each of 10 plants)

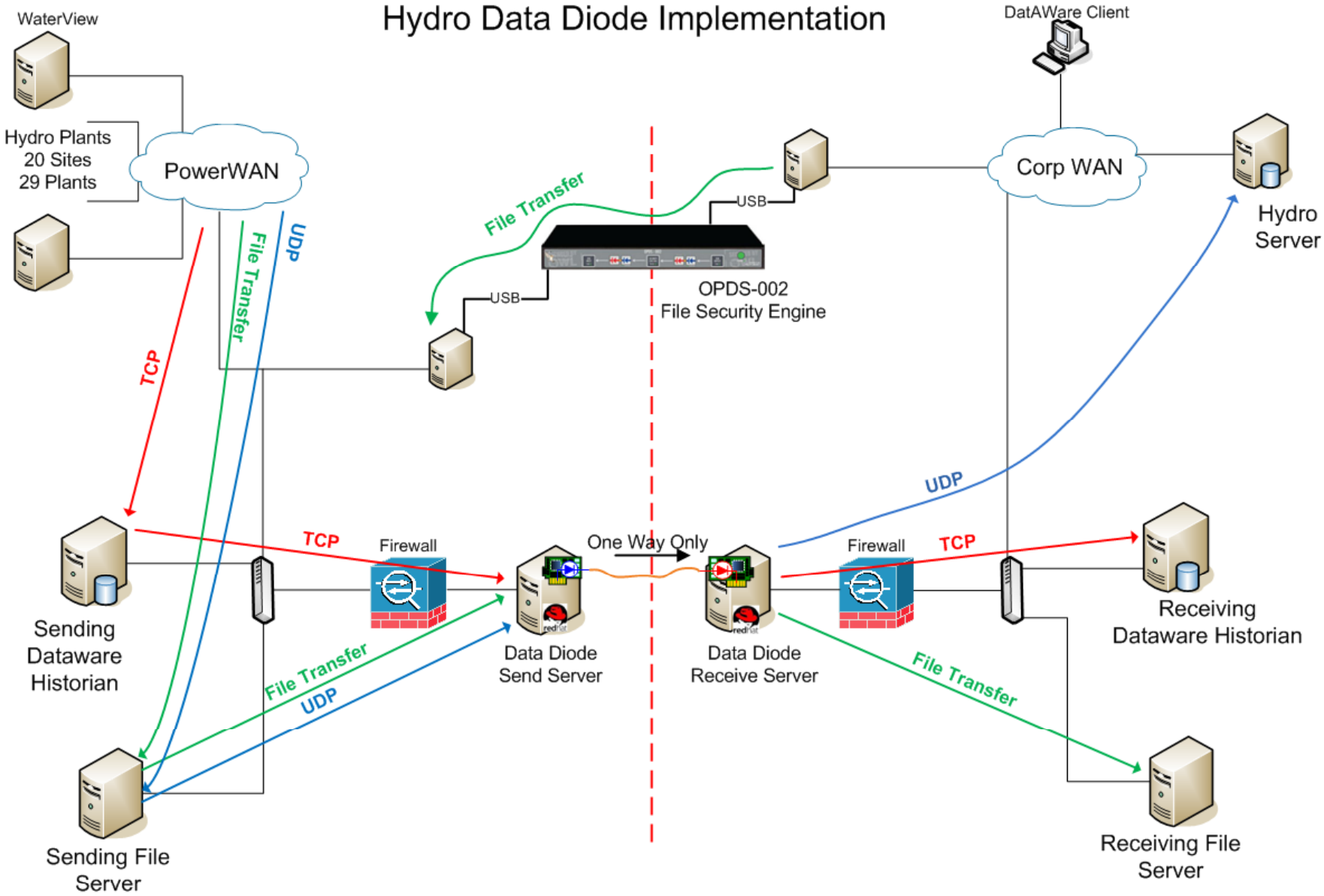



Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

# Hydro Data Diode Implementation



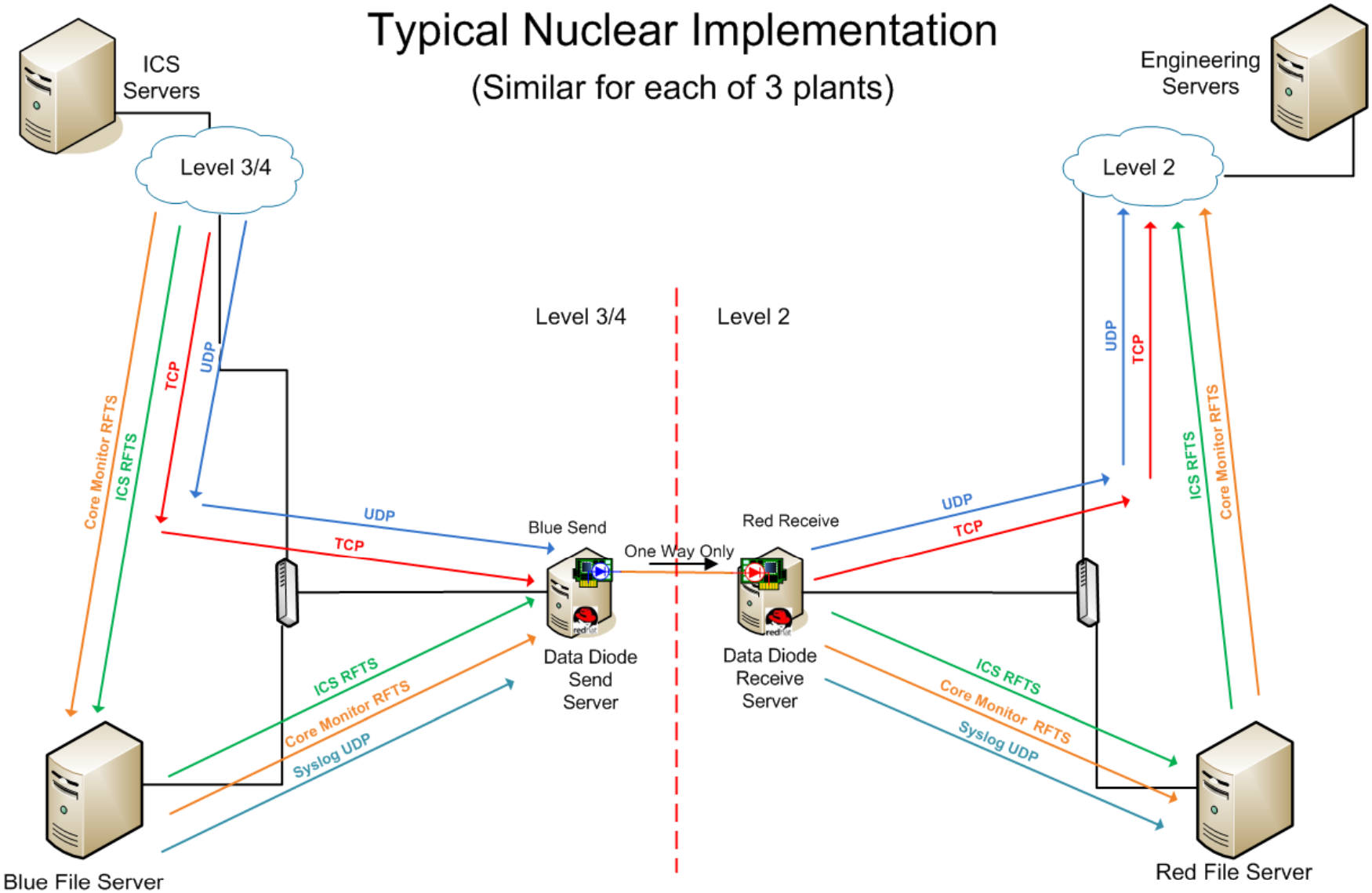

Owl Computing Technologies, Inc.

SECURE ONE-WAY
INFORMATION TRANSFER

TVA

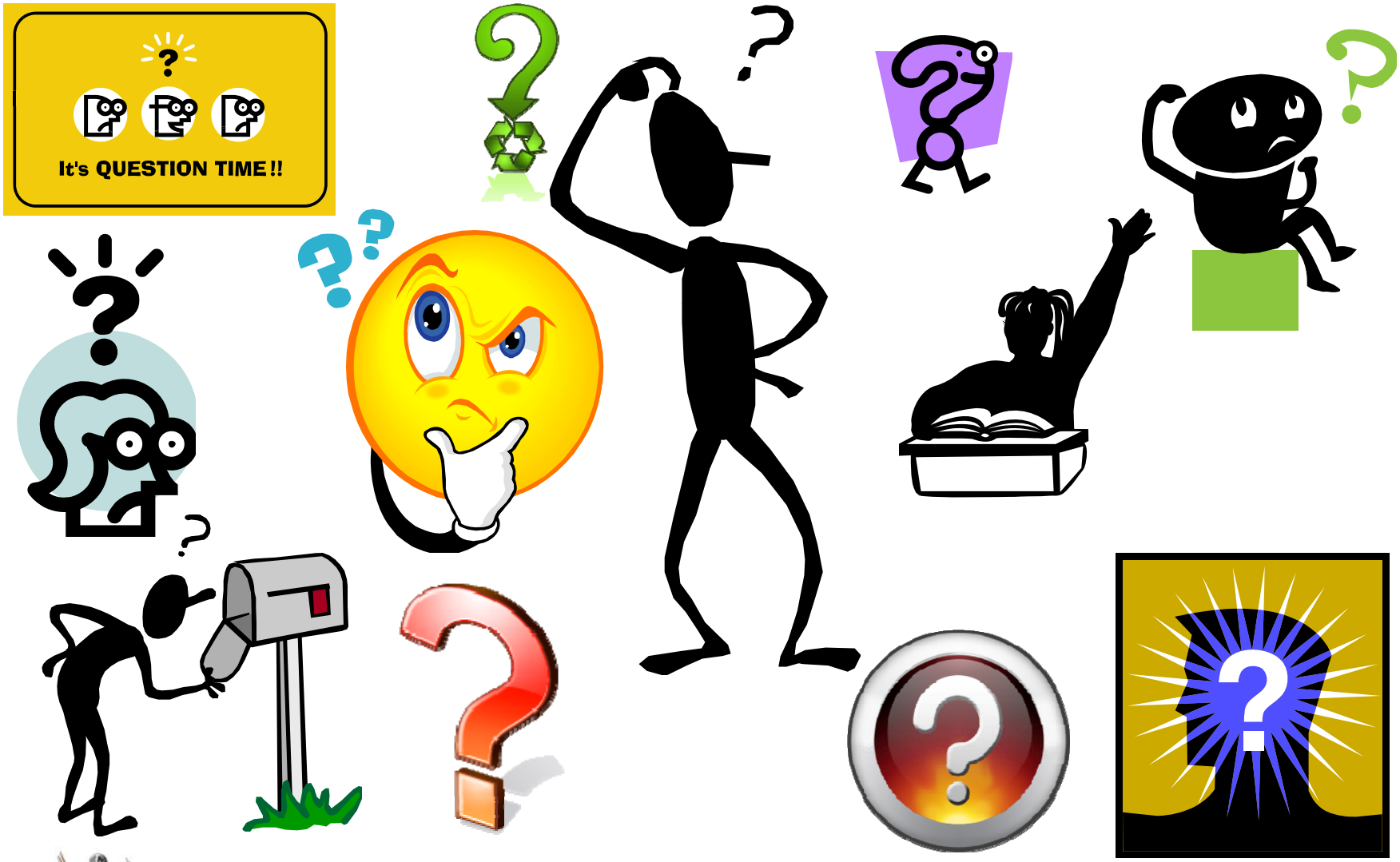
# Typical Nuclear Implementation

(Similar for each of 3 plants)




Owl Computing Technologies, Inc.

SECURE ONE-WAY INFORMATION TRANSFER

TVA

# Questions?