Process Control Systems
Industry Conference

Unidirectional Connectivity

A Novel and Robust Method for Absolute Protection of Process Control Systems

Process Control Systems Industry Conference

August 26 - 28, La Jolla, CA

Avner Turniansky, Director of Product Marketing,
Waterfall Solutions Ltd (www.waterfall-solutions.com)

Agenda

- I. The Changing Cyber-Environment
- II. Potential Security Solutions
- III. Unidirectional Connectivity – Basic Concept
- IV. Unidirectional Connectivity – Use-Cases
- V. Summary

- I. The Changing Cyber-Environment
- II. Potential Security Solutions
- III. Unidirectional Connectivity – Basic Concept
- IV. Unidirectional Connectivity – Use-Cases
- V. Summary

The Changing Environment

- Communication systems are evolving
- Process control systems are evolving
- Cyber-Threats are evolving
- Security measures – Better evolve as well…

Communication Systems' Evolution

- Proprietary O/S & Protocols → Open standards
- Segmented data flows → Integrated data flows
- Closed systems →Open systems
- Centralized computing → Distributed computing

Process Control Systems' Evolution

- Convergence to IP based networks
- Move to public/open standard O/S
- Open and interconnected systems

Connecting PCS Networks to External Networks

- **PCS networks are required to be connected to *external networks:***
  - **Business/Administrative networks for monitoring and status reports, etc.**
  - **Third party networks – Remote infrastructure monitoring, remote equipment maintenance, etc.**
  - **External feeds sending information into the PCS network**

- **These connections are facilitating *business needs and requirements,* as well as *operational needs***

- **These connections impose *security risks* on the PCS networks and systems**

Connecting Critical and Administrative

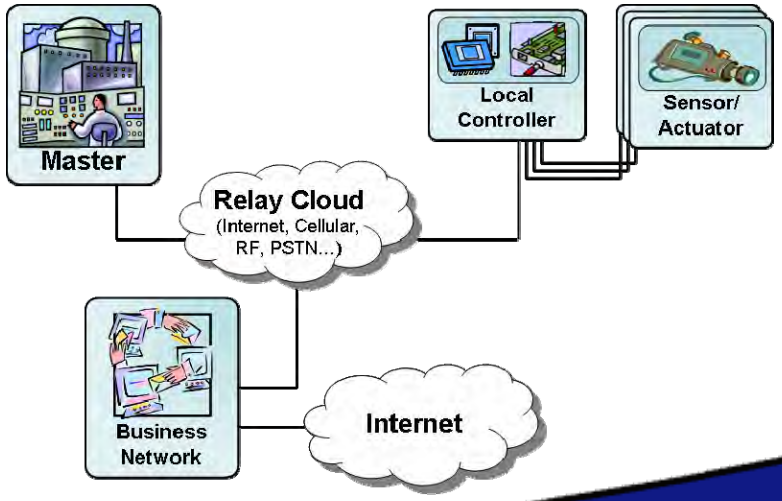
- Connecting process and administrative networks
  - Manufacturing and Enterprise interconnect
  - Connecting ERP (SAP, Oracle etc.) to the manufacturing network:
    - From production history to production orders
    - From production history to financial reports
    - From incoming purchase orders to production orders
    - From production history to equipment maintenance
    - Managing quality assurance and maintenance

Connecting Critical and Business Networks

- **The PCS network is required to send or receive online information to/from the business/administrative networks:**
  - Production status and statistics for the ERP/CRM
  - Monitoring and status information
  - Incoming production requests

- **The business network is commonly connected to other networks, including the *Internet***

- **Via these connections, attackers can *gain access to the critical network* and facilitate remote, online attacks into it**



Remote Monitoring – Inherent Vulnerabilities

- **A vendor is remotely monitoring its installed equipment, installed at a SCADA/PCS network:**
  - **As part of the maintenance agreement (SLA requirement)**
  - **From one central location**
- **This vendor is monitoring many *other customers***
  - **From the same central location, effectively acting as a hub**
- **The SCADA network can be accessed from these other** customers
  - Via the hub
  - Other customers' networks may be
    - Less secure
    - Less sensitive and hence – less guarded
    - Open to the Internet / unprotected
- **In some cases network is connected to several such vendors**

PCS Vulnerabilities:

- Insecure interconnectivity with external networks
- Insecure interconnectivity with remote sites/systems
- Adoption of standard technologies with publicly known vulnerabilities
- Widely available info on SCADA/PCS systems
- Limitations on use of existing security practices

PCS Networks as the New "Cyber-Targets"

- **PCS networks are a Prime Target for Cyber-Crime and Cyber-Terror :**
  - Nationwide damage
  - Extensive media coverage
  - Huge financial impact
- **This is true for all relevant installations, public and private, US and worldwide**
- **Modern SCADA/PCS systems are more vulnerable than ever:**
  - Use **IP infrastructure**
  - Deploy **standard protocols**, applications and operating systems
  - Are **connected** to other networks, including the **Internet**

Modern History of SCADA/PCS Networks Events

Over the past two years, **hackers penetrated and extorted hundreds of millions of dollars from multiple companies using SCADA systems**, says Alan Paller, director of the SANS Institute

-*Newsweek, Mar 2008*

Authorities have become **increasingly concerned about vulnerabilities in SCADA systems as they've moved from closed networks to being connected to the Internet**

- *MSNBC, Aug 2007*

We have information **that cyber attacks have been used to disrupt power equipment.**../.. In at least one case, the disruption caused **a power outage affecting multiple cities** ../.. **all involved intrusions through the Internet**

- *SANS org, Jan 2008*

The Hatch Nuclear Power Plant Event - ...occurred on March 7, 2008 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. **The trouble started after an engineer**, ...**installed a software update on a computer operating on the plant's business network**.

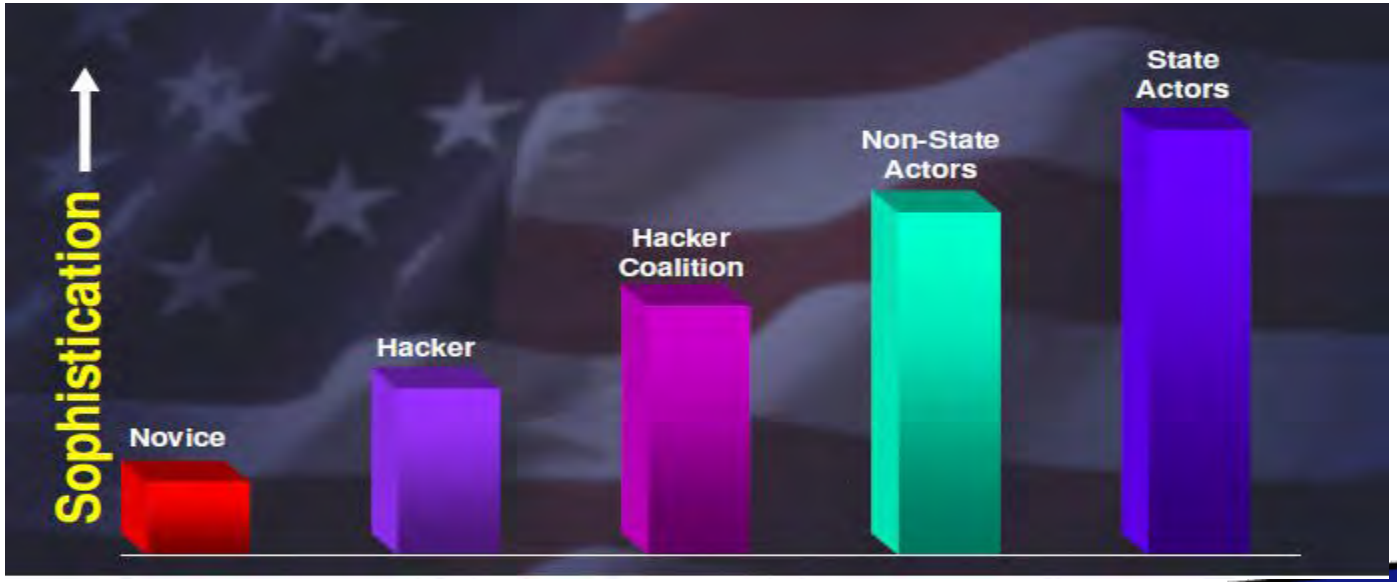
The Washington Post, June 2008

Cyber-Threats Evolution

- Mid 80's – the first basic viruses…
- Today – a host of attack and weapon types:
  - Viruses
  - Worms
  - Trojans
  - Phishing
  - Hacking
  - DDoS
  - BotNets and Zombies
  - ….

Cyber Threats' Vectors

- Nation-States (External)
- Terror & Criminal Organizations (External)
- Disgruntled Insiders (Internal & External)
- Mischievous Individuals (Internal & External)
- Mishap (e.g. inadvertent cascading update)



- I. The Changing Cyber-Environment
- **II. Potential Security Solutions**
- III. Unidirectional Connectivity – Basic Concept
- IV. Unidirectional Connectivity – Use-Cases
- V. Summary

Protection Evolution

- Protection must evolve to answer these new challenges
- Balancing the picture - the positive aspects of:
  - Convergence
  - CPU power
  - Growing awareness
  - Standardization
  - Certifications

I - The Traditional Approach – IT Security

- **Deploy standard IT security means and techniques:**
  - **Firewalls, intrusion detection and prevention systems**
  - **Anti-viruses and content filters**
  - **Encryption and authentication**
- **BUT - Is the existing IT security level (99.???%) enough, *when considering the relevant risk?***
- **IT Security is not enough here:**
  - **All IT Security products suffer from software vulnerabilities, bugs and misconfiguration – thus, able to be hacked and circumvented**
  - **Attackers are financially backed up and highly motivated**
  - **Hacking information and know-how is out there, plentiful and readily accessible**

II - The Strict Approach – Total Segregation

- Fully segregate the SCADA network from the outside world !!
- Pros:
  - No online attacks…No penetration possibility…No data leakages…
  - No need to worry any more!
- Cons:
  - No more online information to the business network
    - Only manual, offline, transfer of data
  - No more remote monitoring or management
    - Onsite support, bad SLA and financial expenditure
  - Can not deploy modern IP based sensors
    - Only “analog” devices

II - The Strict Approach – Total Segregation

- **Business processes will not work, or will be drastically impaired:**
  - **To extract data from the network:**
    - **Collect and organize it inside the network**
    - **Burn on perishable media**
    - **Examine and verify content**
    - **Transfer data to external network, then to destination**
    - **Destroy perishable media**
  - **To insert data to the network:**
    - **Collect and organize data on outer network**
    - **Burn on pristine perishable media**
    - **Examine and verify content**
    - **Transfer data to internal network, then to destination**
    - **Destroy perishable media**

Total Segregation - Limitations

- Lose all connectivity benefits
- Manual tedious work, prone to mistakes
- No real time or streaming capabilities
- Open access ports in segregated network
- Recurring costs for perishable media

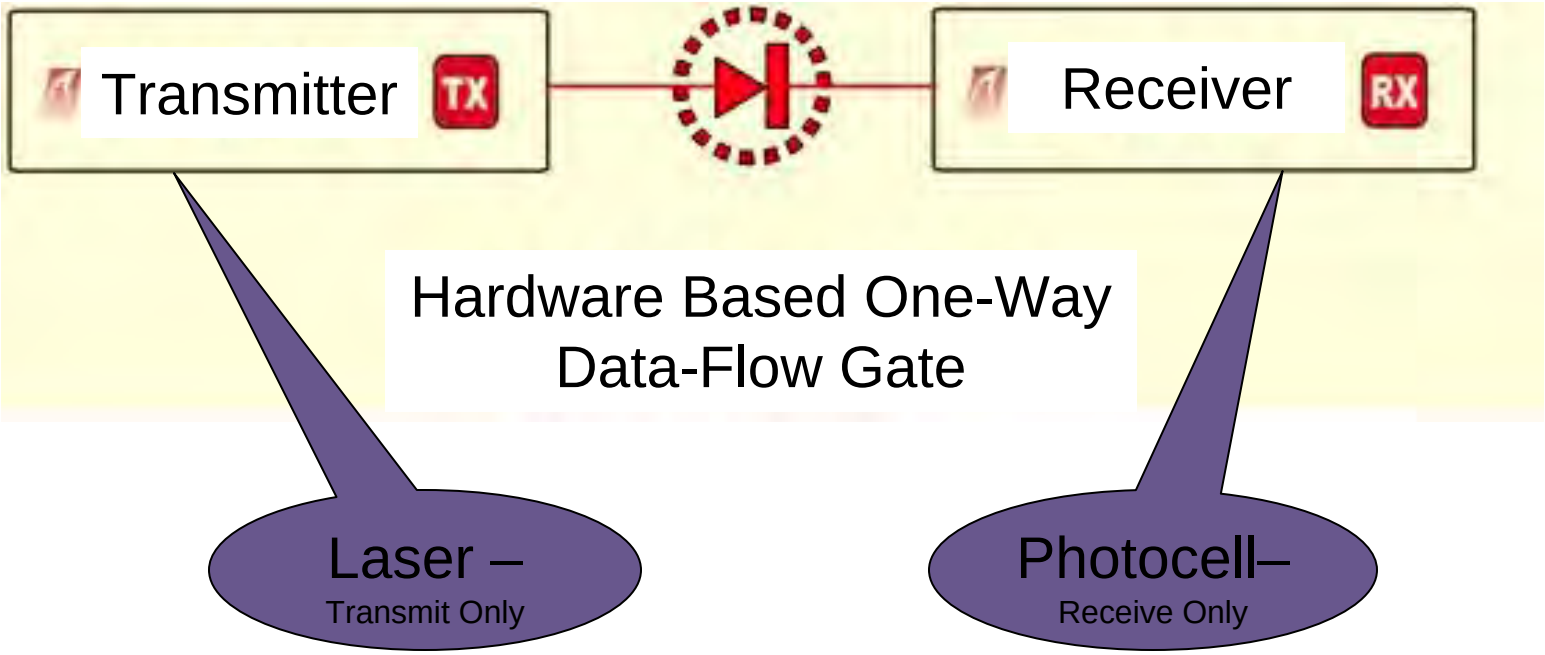
III–The Novel Approach: Unidirectional Connectivity

- **Deployment of physically based unidirectional gateways for external connections**
- **Leveraging the unidirectional logic of such connections for:**
  - **Sending production information to the business network**
  - **Sending status information to the remote monitoring network**
  - **Receiving information from IP surveillance/remote devices**
- **Benefits of the approach - *A Win-Win situation***
  - **Enabling all business needs and requirements ("traditional approach")**
  - **Top security level – practical "physical segregation" ("strict approach")**

- I. The Changing Cyber-Environment
- II. Potential Security Solutions
- III. Unidirectional Connectivity – Basic Concept
- IV. Unidirectional Connectivity – Use-Cases
- V. Summary

Realizing Absolute Unidirectional Connectivity

- **Optical domain realization of absolute unidirectional connectivity:**

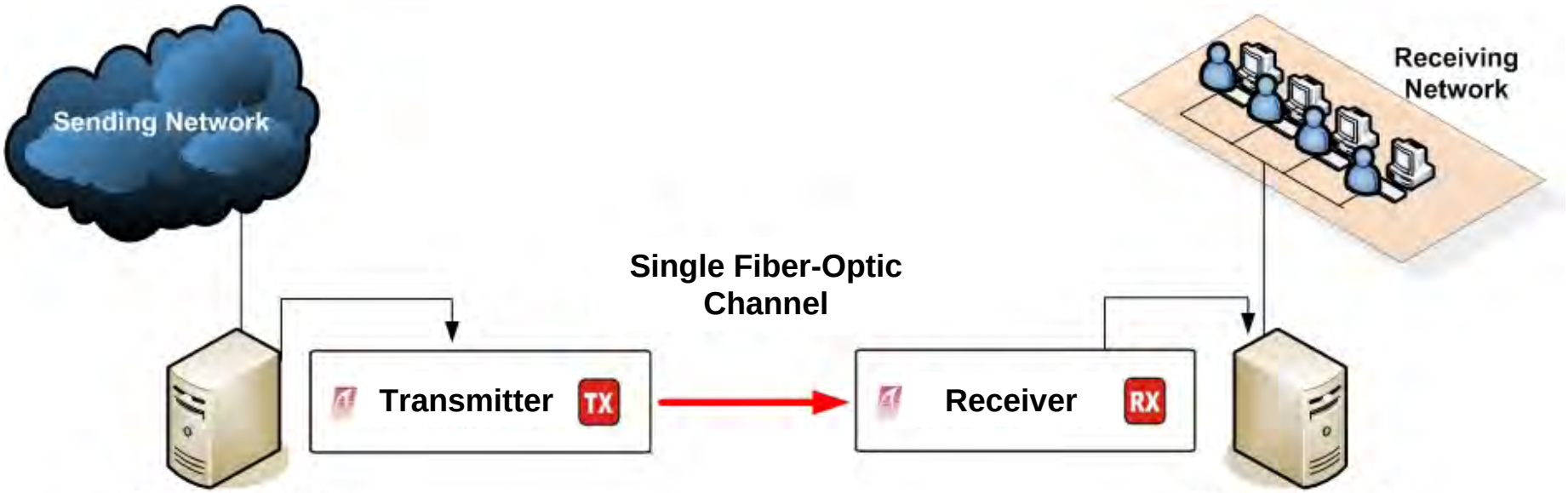


Connecting … But….

- **Nice, BUT - IP networks are bidirectional**
- **Unidirectional links have to be mediated into the bidirectional surrounding**
- **Solution – use mediating application software:**
  - Cheat Tx side to think transmissions reached destination
  - Cheat Rx side that sender received acknowledgements
- **Overall solution therefore integrates H/W and S/W**

Fully Integrated Solution

- Hardware Based One-Way Data-Flow Gate - Hardware based appliance
- Mediating Applications – Residing on both sides of the link



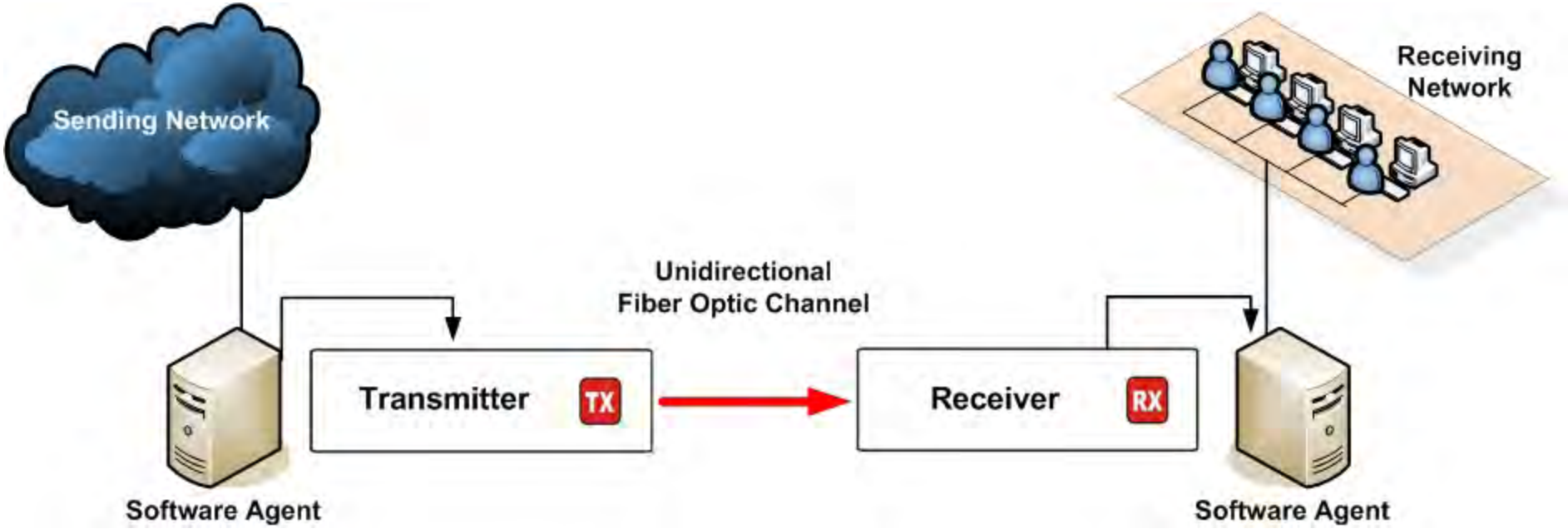
Mediating Software Agent

Mediating Software Agent

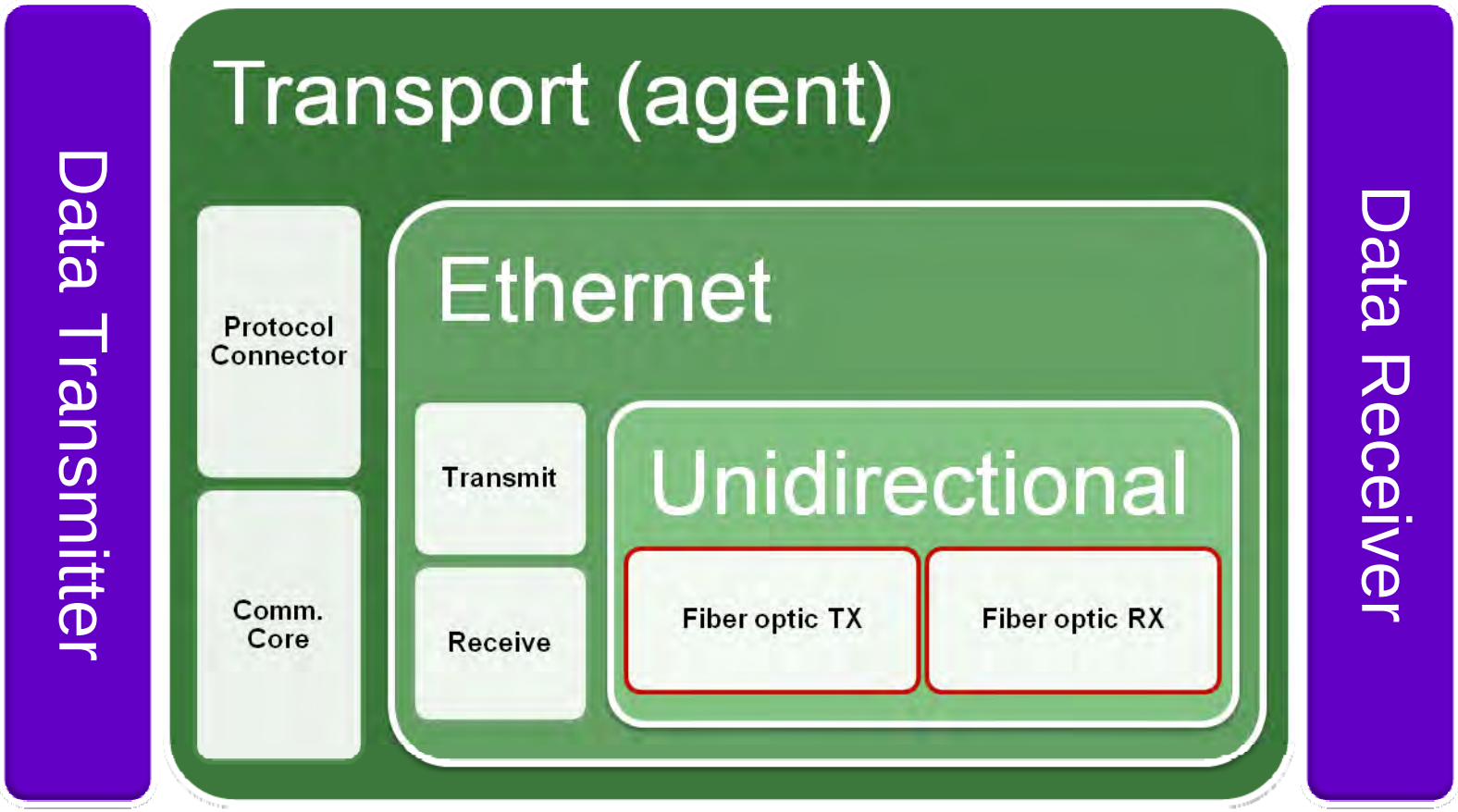
File transfer
Stream transfer
SCADA/DCS Protocols

Remote monitoring
Video/audio surveillance

Unidirectional Connectivity – Basic Architecture

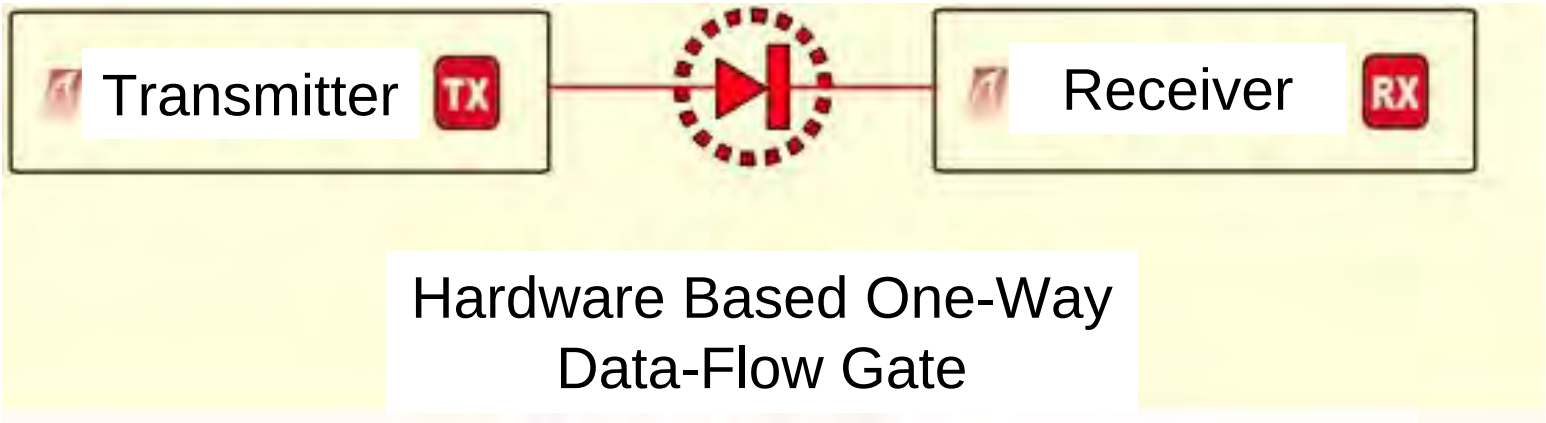


Solution Architecture:



Unidirectional Connectivity – Two Promises

- **Impossible to hack across – No session can be initiated, hacker at most will be working blind**
- **Absolutely no data transfer in the "wrong" (i.e. RX→TX direction)**



Unidirectional Connectivity – Benefits - I

- The best of both worlds
- Segregated yet connected
- Flexibility at the application layer
- Real-time and streaming support
- Foolproof – configuration mistakes do not harm security profile
- Future-proof – solution core remains the same

Unidirectional Connectivity – Benefits - II

- Automated and independent solution
- Misconfiguration of application – No deterioration in H/W degree of protection (foolproof)
- H/W core requires no updates (future-proof)
- No recurring costs

Unique Advantages of Unidirectional Connectivity:

- **Security**
  - Hardware based physical data control-valve
  - No physically possible return channel
  - Immune to software bugs, exploits and configuration faults
  - Human error does not effect security level
  - Immune against known and unknown attacks

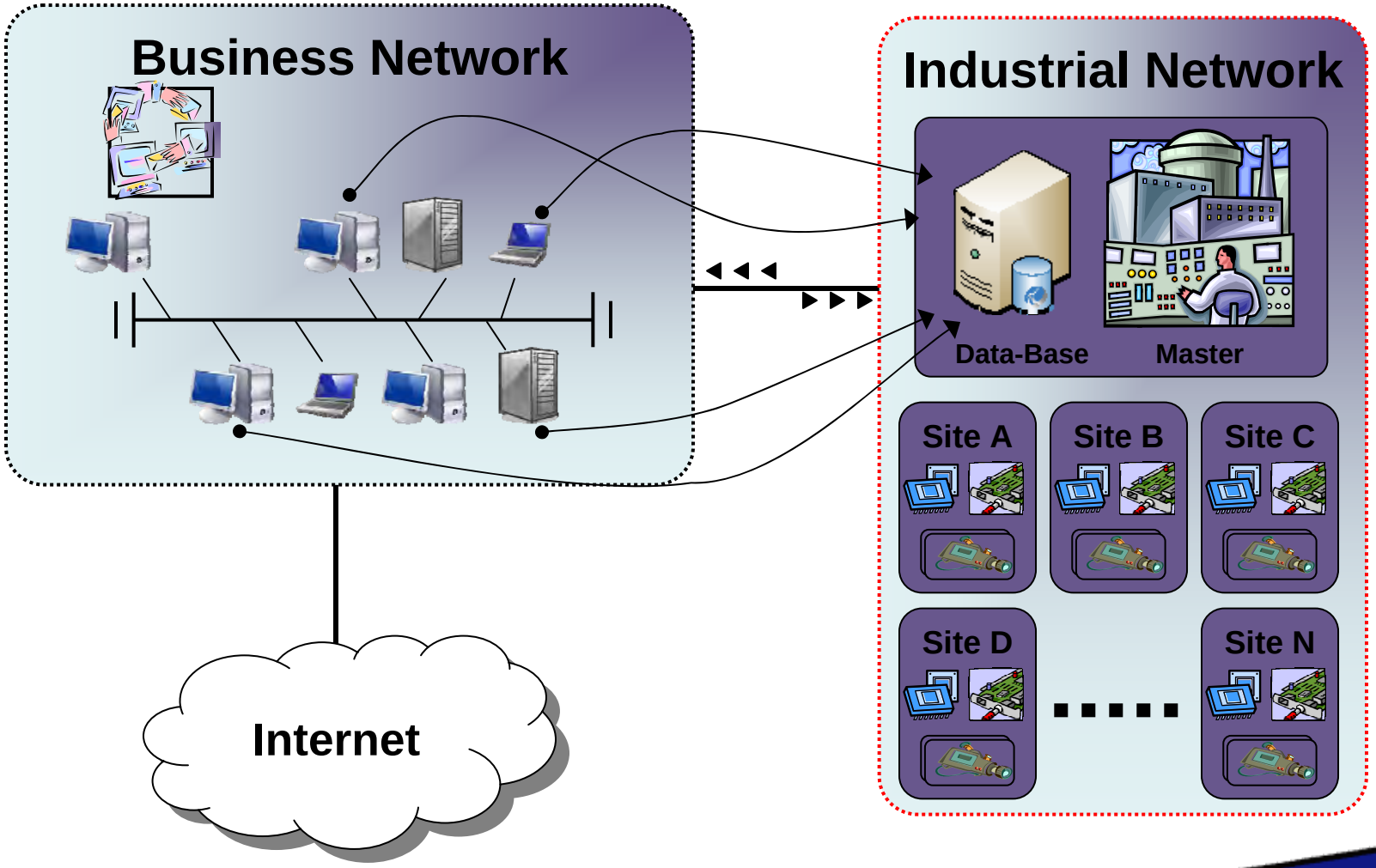
- **Usability**
  - Application allows for maximum flexibility
  - Connect to any network/protocol

Unidirectional Connectivity - Uses

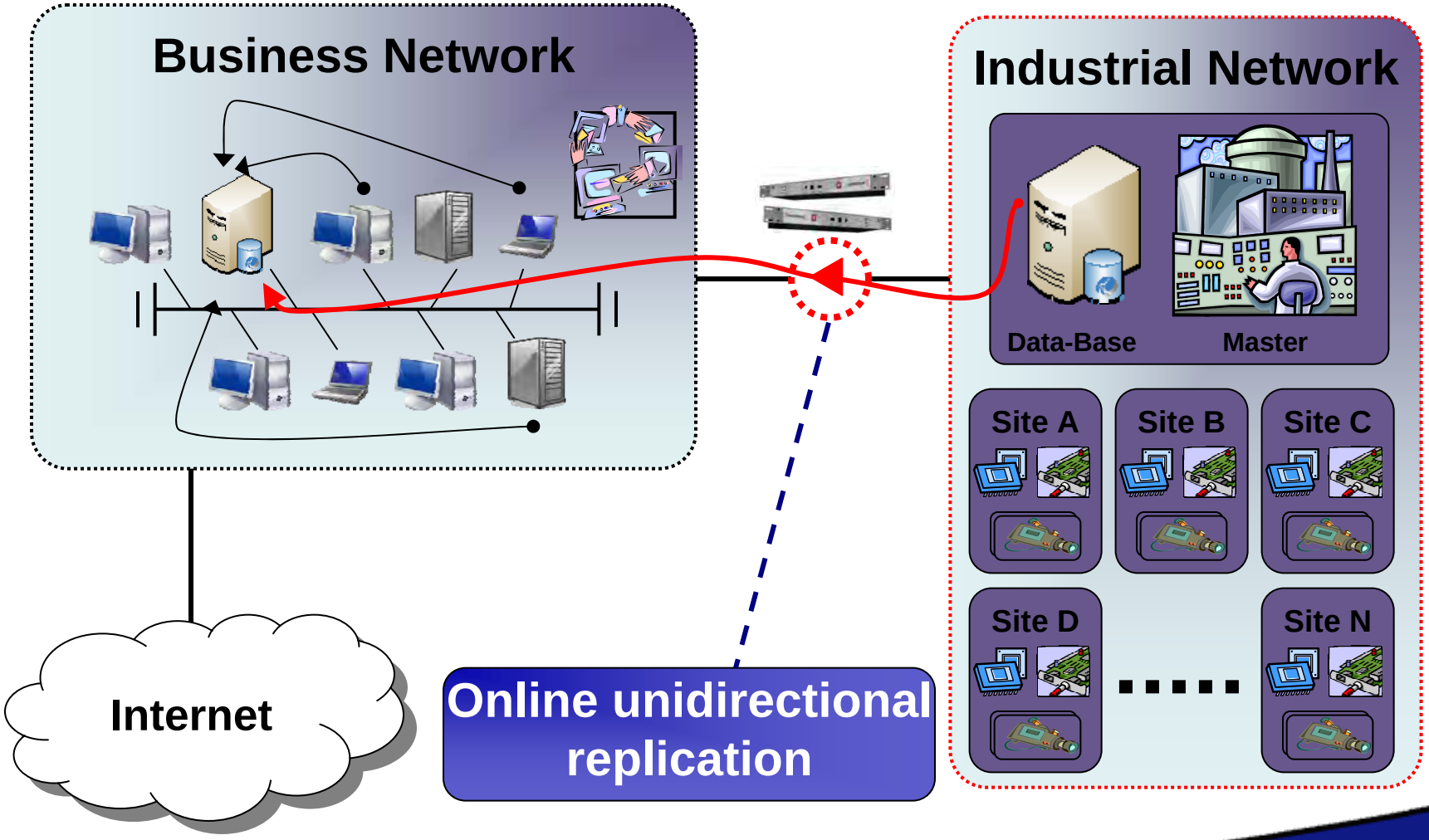
- Unidirectional connectivity can be used to provide high-grade and absolute security in different scenarios
- Let's investigate some of the possible uses of this novel security concept

- I. The Changing Cyber-Environment
- II. Potential Security Solutions
- III. Unidirectional Connectivity – Basic Concept
- IV. Unidirectional Connectivity – Use-Cases
- V. Summary

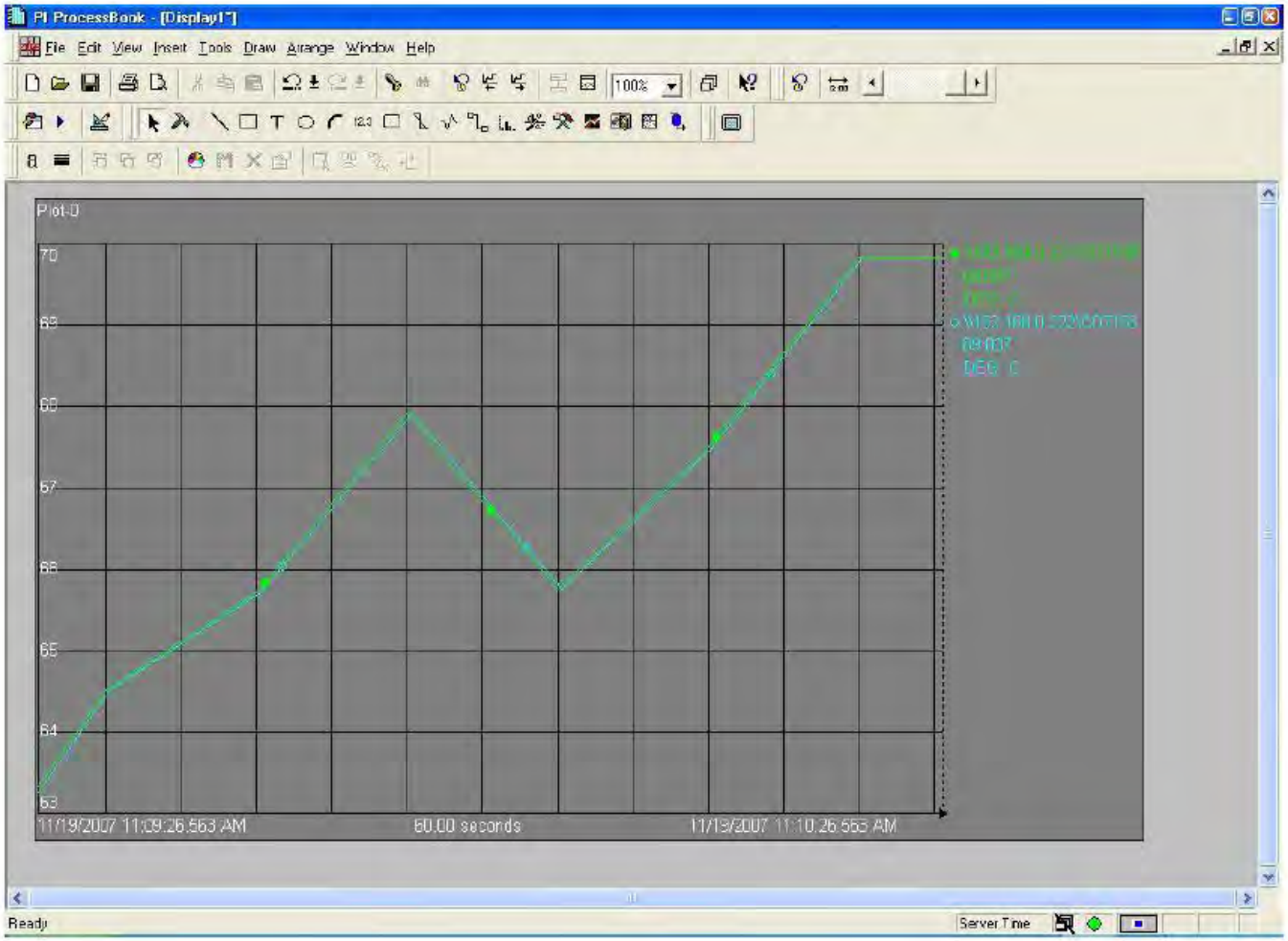
Energy Company – SCADA system - Insecure



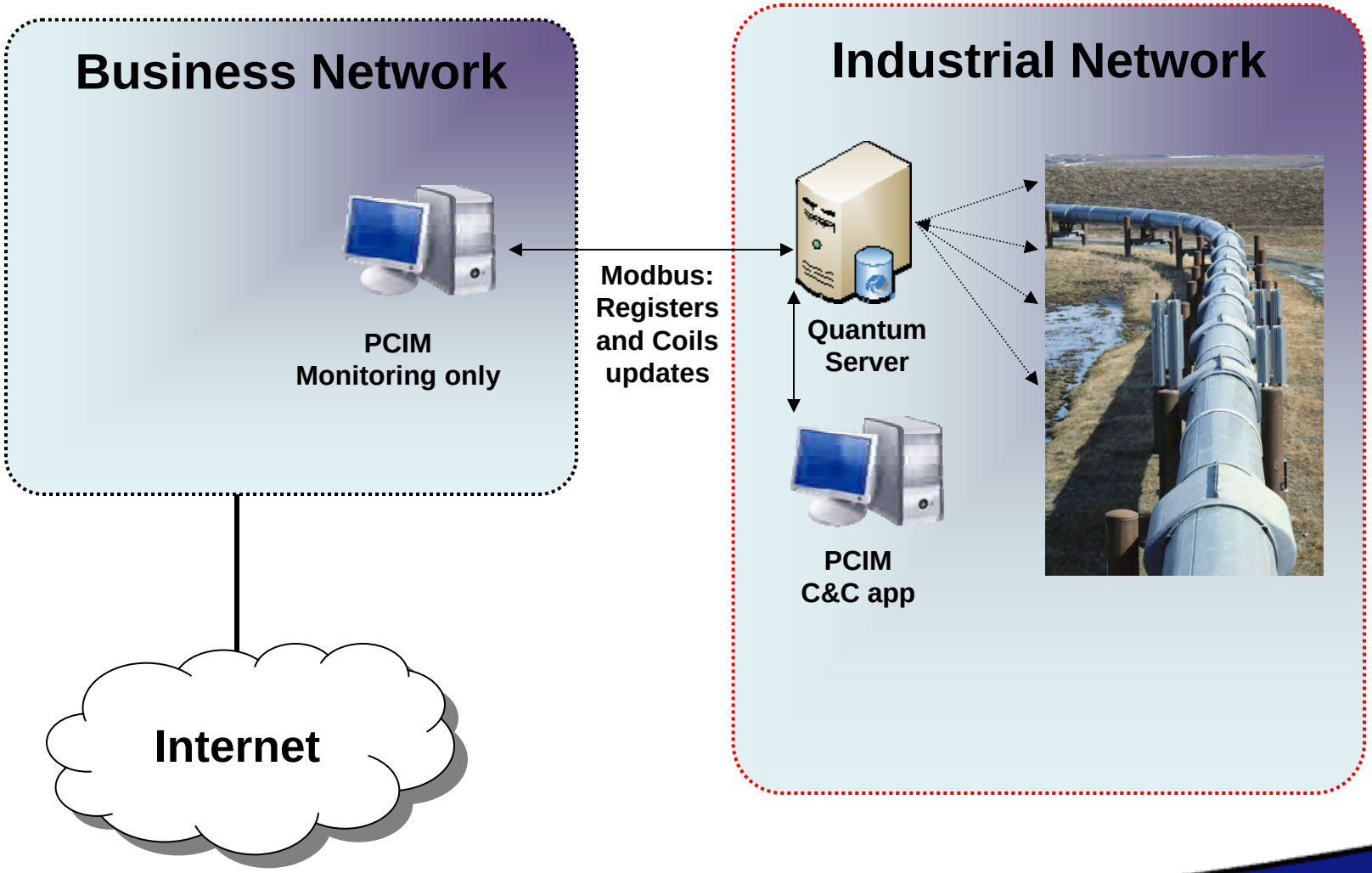
Energy Company – SCADA system - Secure



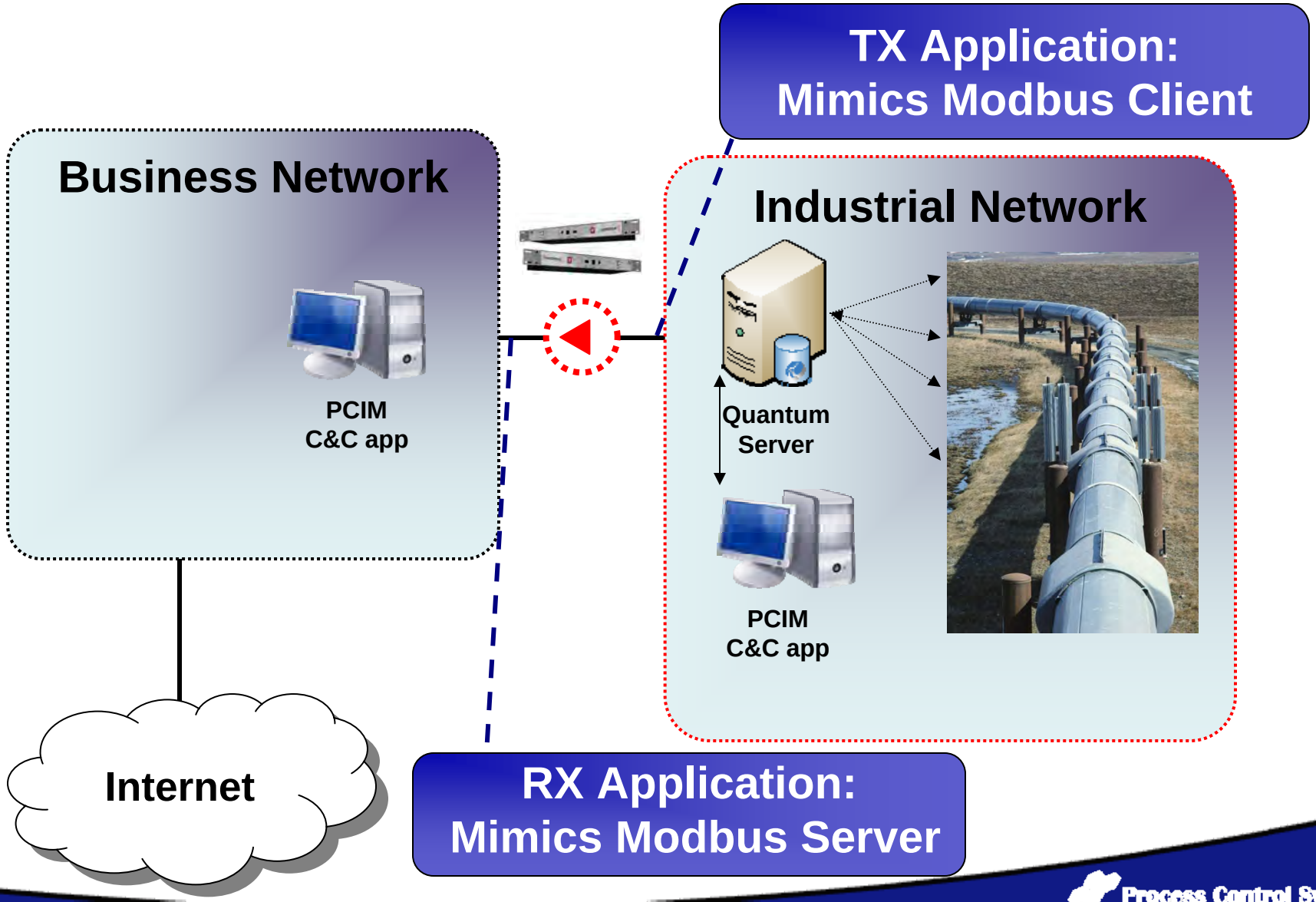
SCADA System – Required Performance



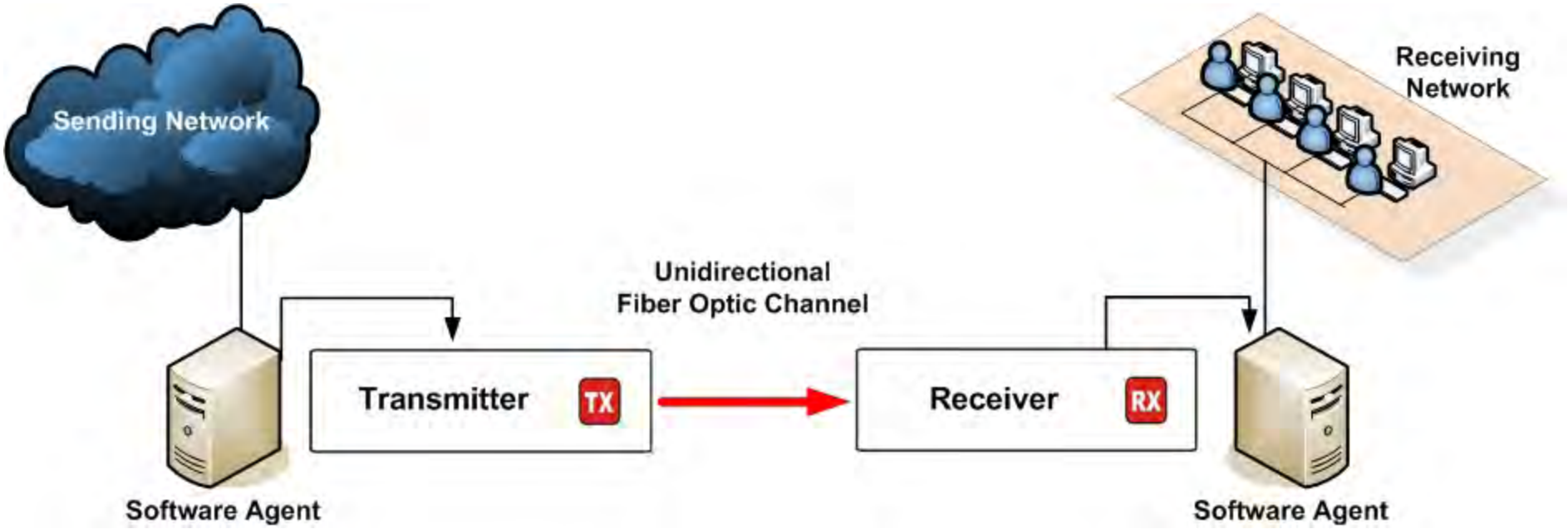
Oil Pipeline – Modbus (SCADA) - Insecure



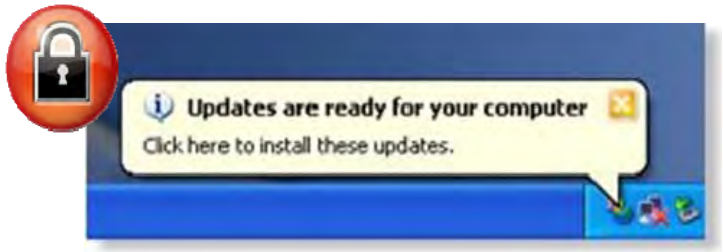
Oil Pipeline – Modbus (SCADA) - Secure

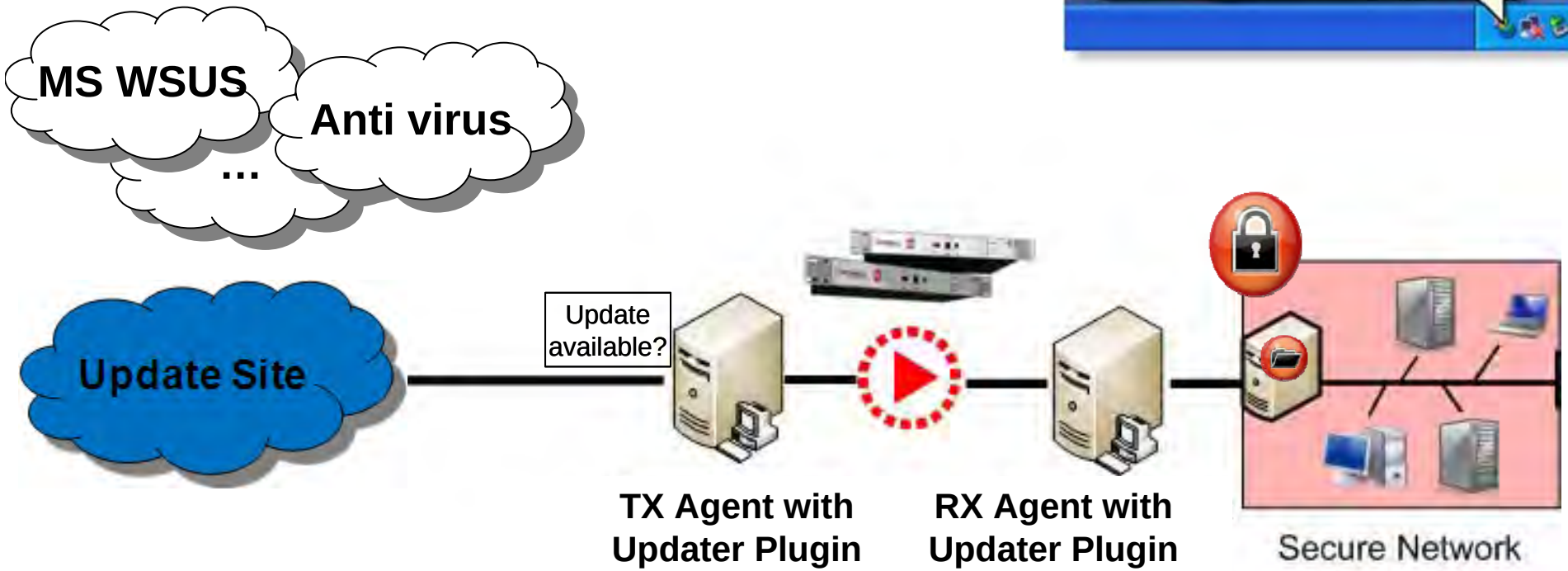


General Unidirectional Solution – File Transfer

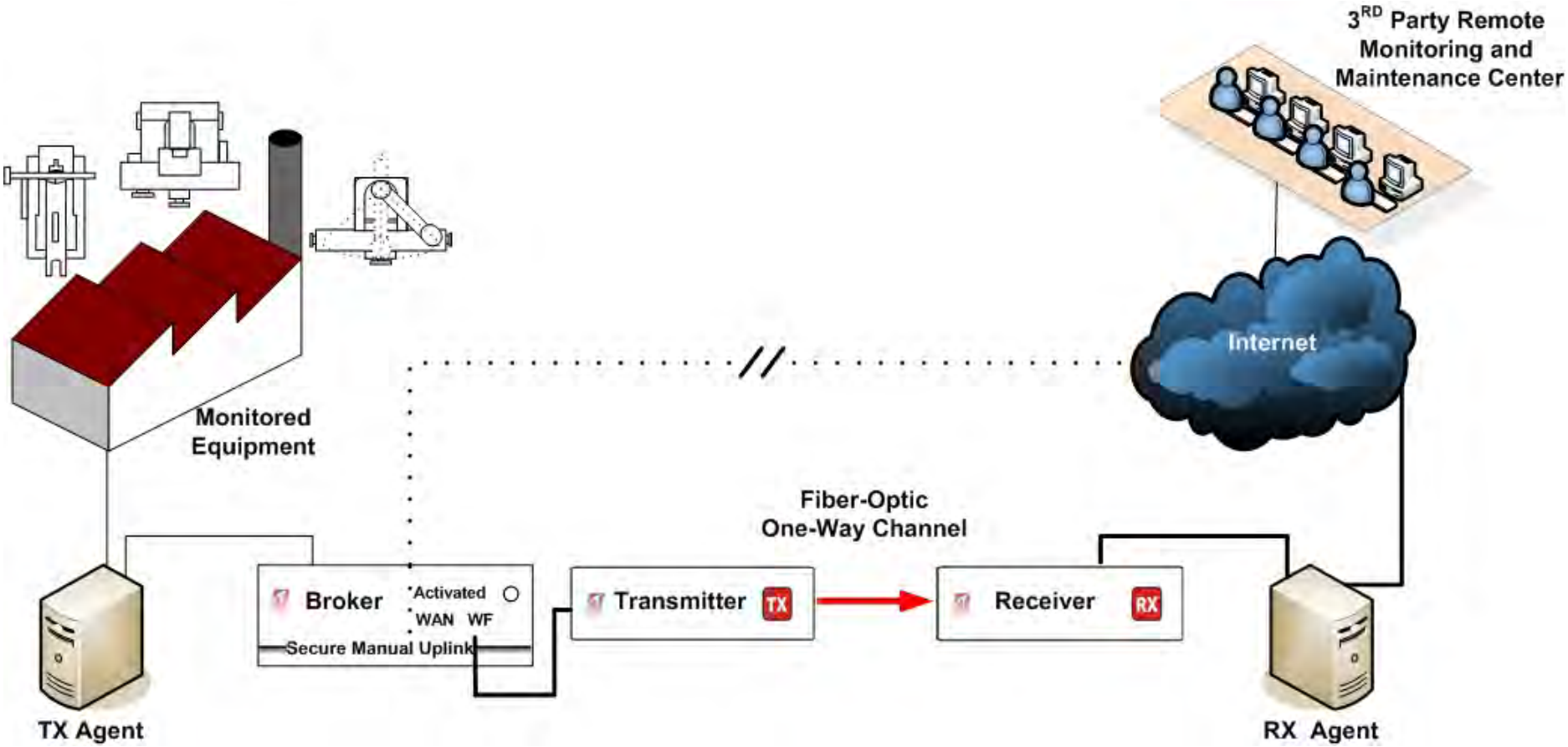


Secure Software Updates in Critical Networks:

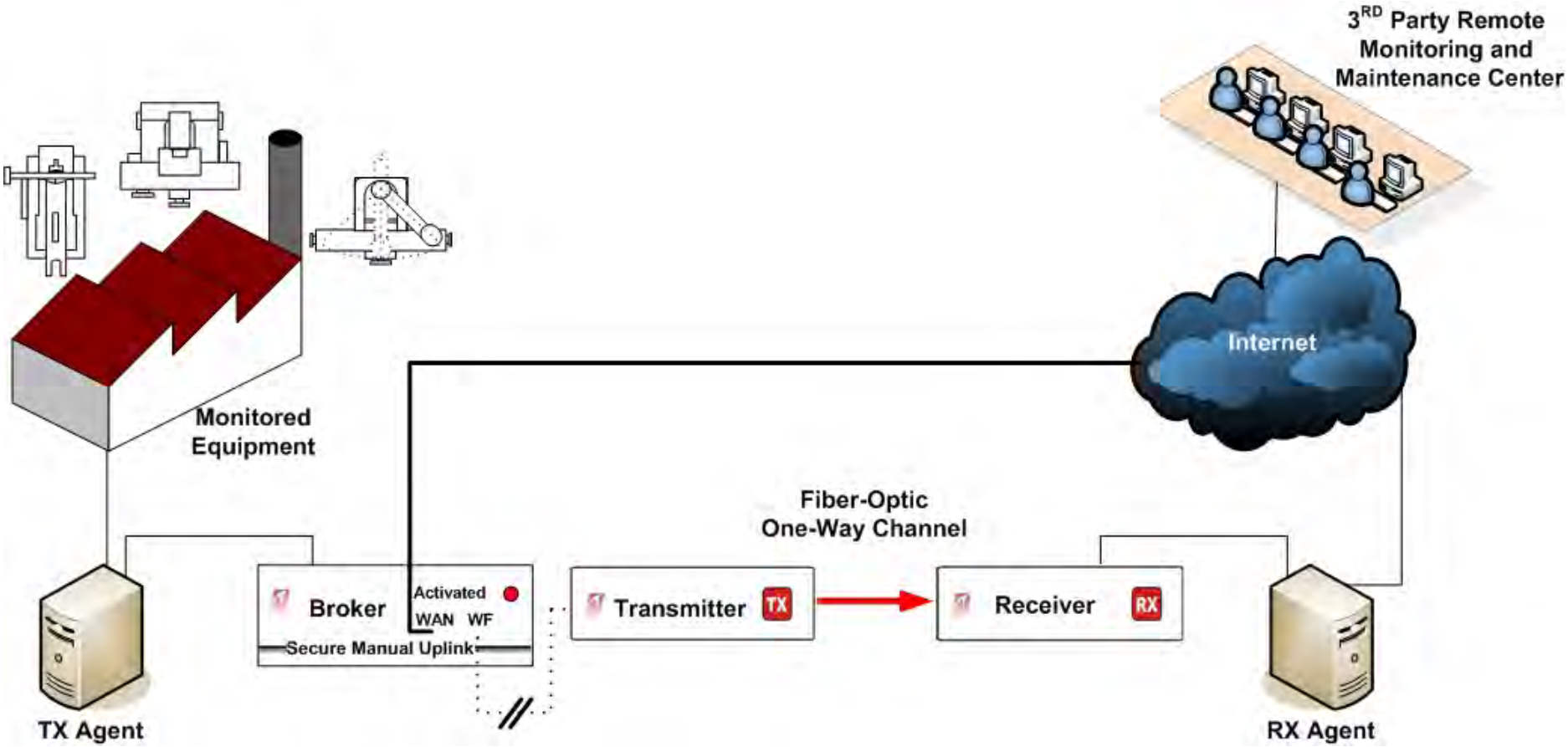




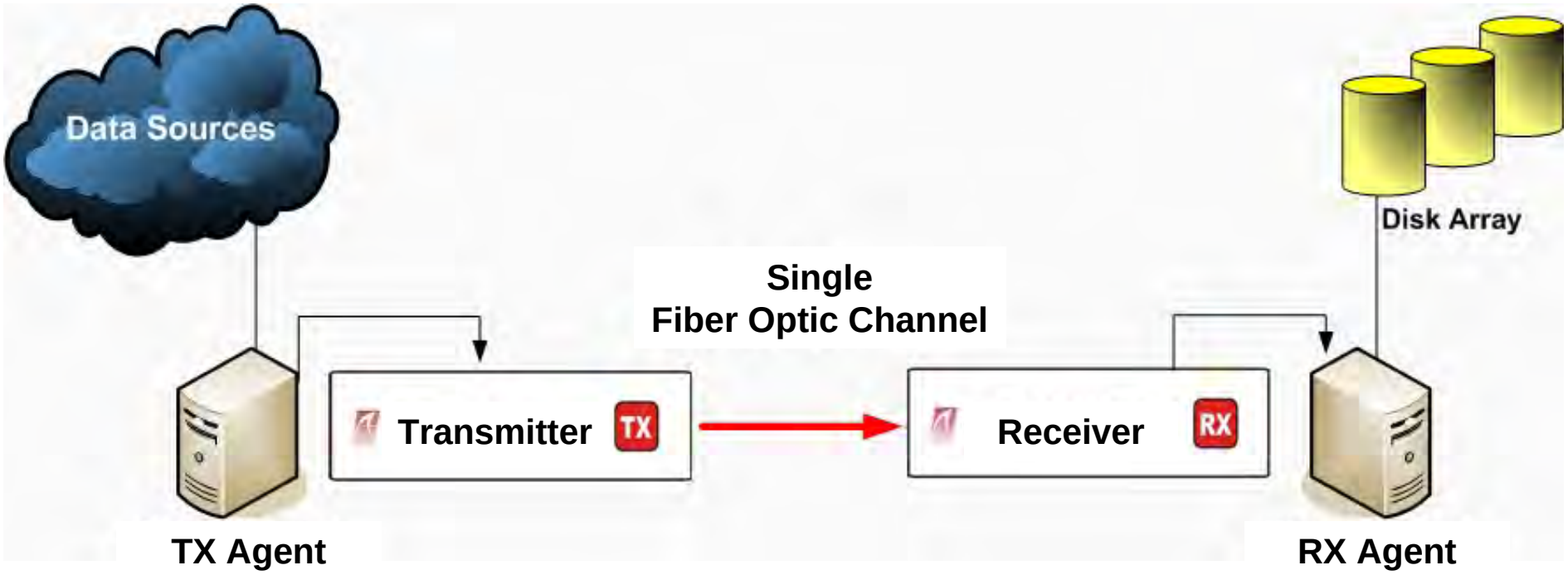
When Bi-Directionality is Needed - Monitoring:



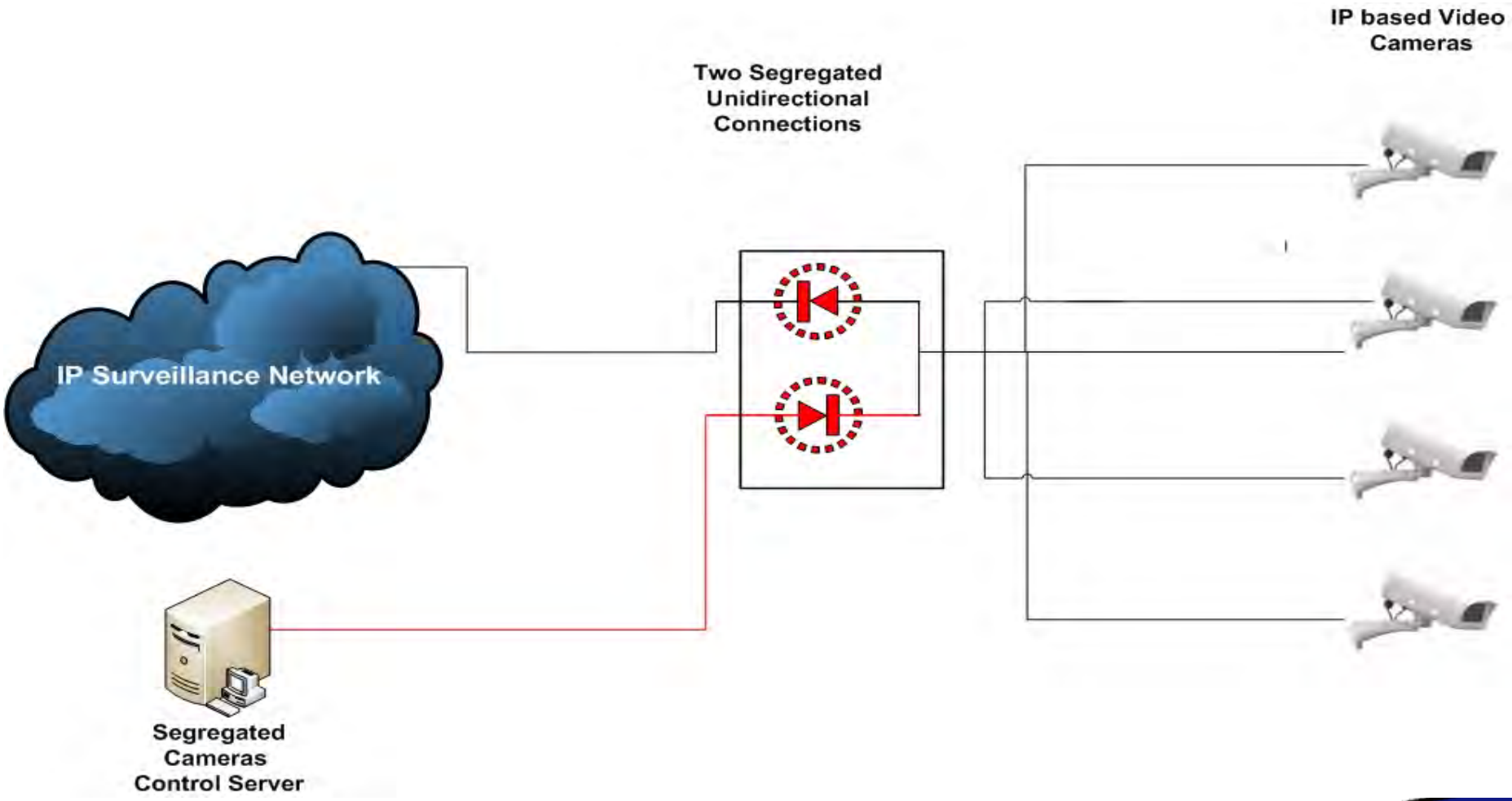
When Bi-Directionality is Needed – Maintenance:



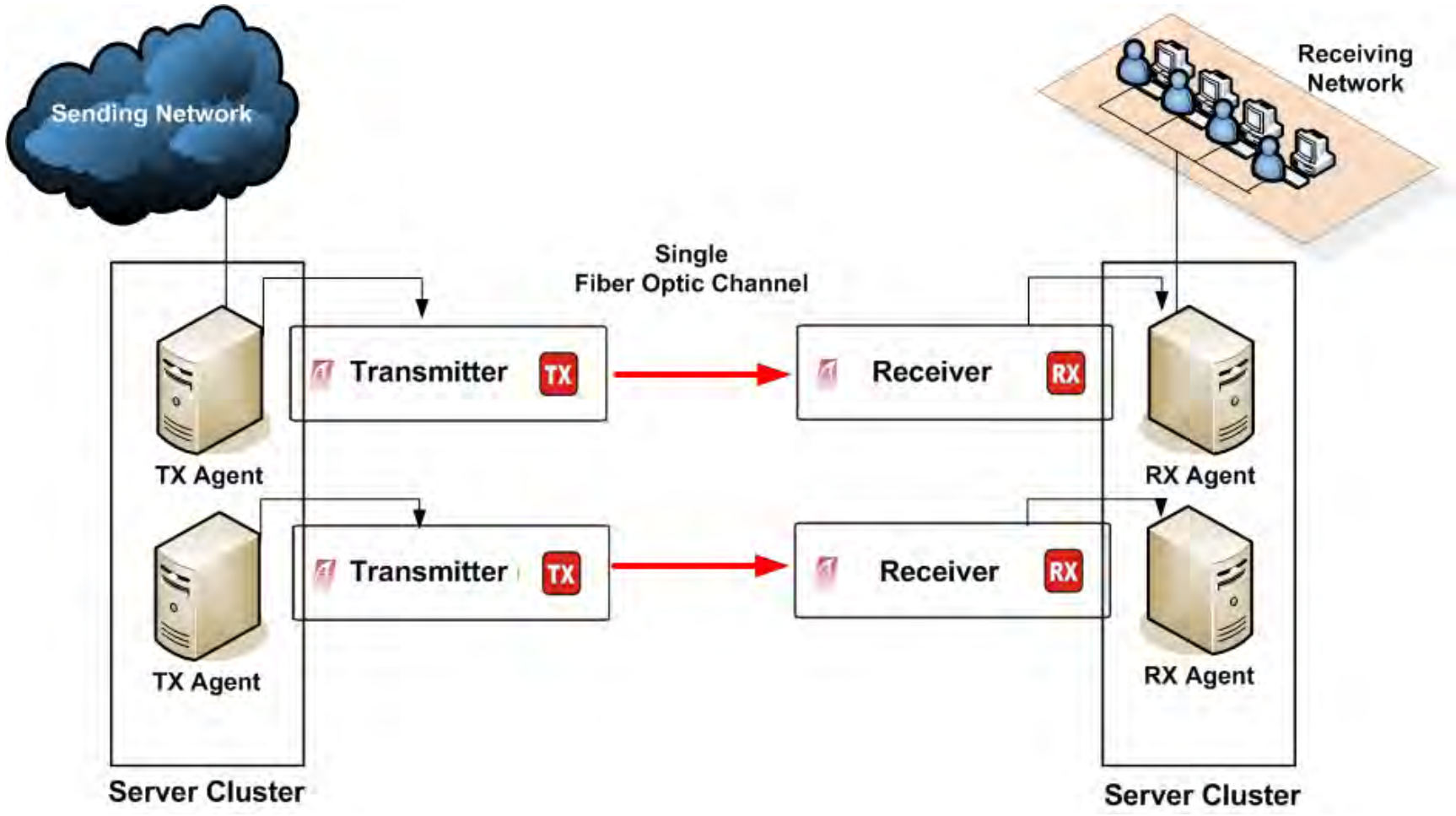
Secure and Compliant Data Storage & Retention:



When Bidirectionality is Needed for Control:



Redundancy for Extra Security:



Summary

- Process Control networks are prime targets for cyber-terror and cyber-vandalism
- The potential damage of a successful attack on such installations is huge
- Connectivity provides a relevantly simple way to penetrate and attack process control networks
- Physical unidirectional connections (controlled connectivity) enables Process Control networks to remain connected to the outside world while retaining absolute security

Questions Time…

Thank You