Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații
în contextul noilor abordări privind securitatea cibernetică.

WATERFALL
One Way to Connect
FROST & SULLIVAN
2012 BEST PRACTICES AWARD
NORTH AMERICAN NETWORK SECURITY FOR INDUSTRIAL CONTROL SYSTEMS ENTREPRENEURIAL COMPANY OF THE YEAR AWARD
One Way to Connect

Stronger Than Firewalls: Unidirectional Security Gateways

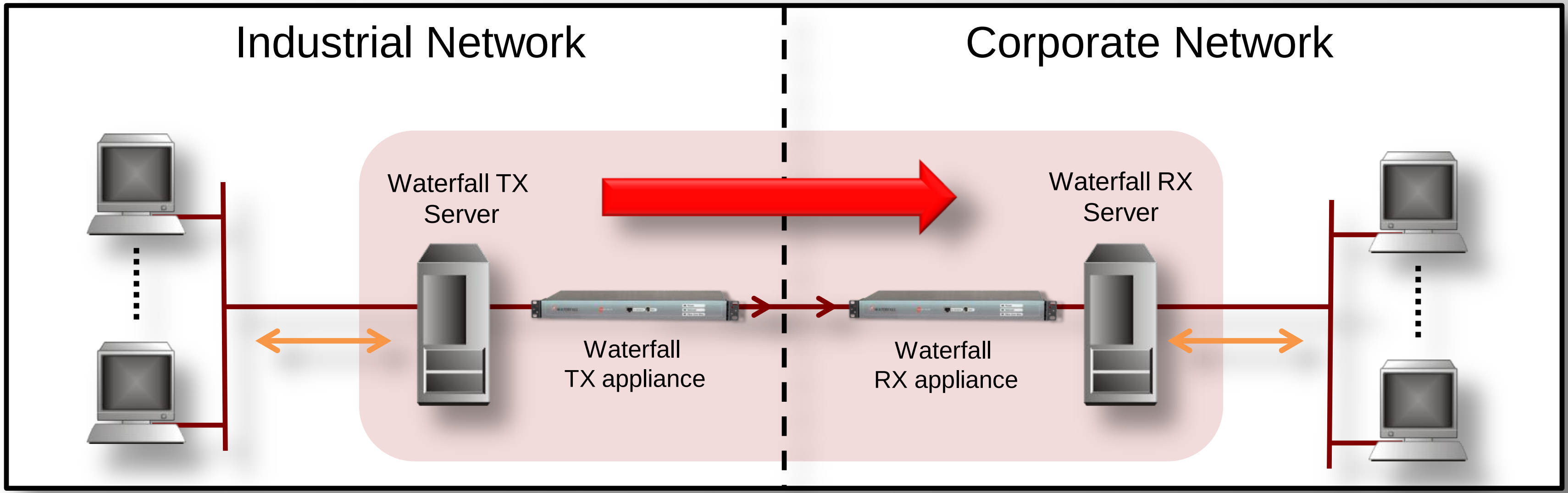
Colin Blou
VP Sales NA and EU

Ben Bernfeld
Sales Director

Waterfall Security Solutions

Unidirectional Security Gateways

- Laser in TX, photocell in RX, fibre-optic cable – you can send data out, but *nothing* can get back in to protected network
- TX uses 2-way protocols to gather data from protected network
- RX uses 2-way protocols to publish data to external network
- Server replication, not protocol emulation



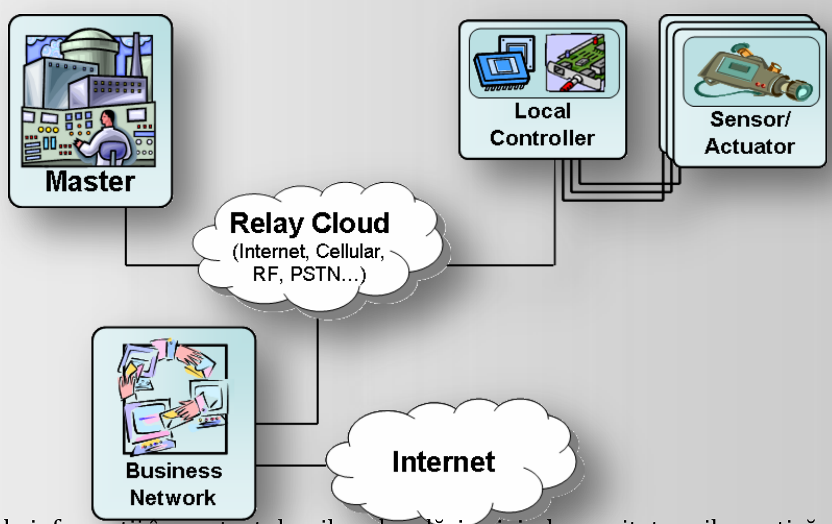
Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

Industrial Network Connectivity: Drivers & Risks

- Predictive maintenance: crew scheduling, HR integration, spare parts inventories and ordering
- Just-in-time manufacturing, real-time inventories, batch records, LIMS integration, production planning, SAP/ERP integration
- Centralized support: more effective use of skilled personnel, critical mass of current experts next decade's experts

- Industrial network connects to business network, which connects to Internet & other networks

With these connections, attackers target critical network with remote online attacks

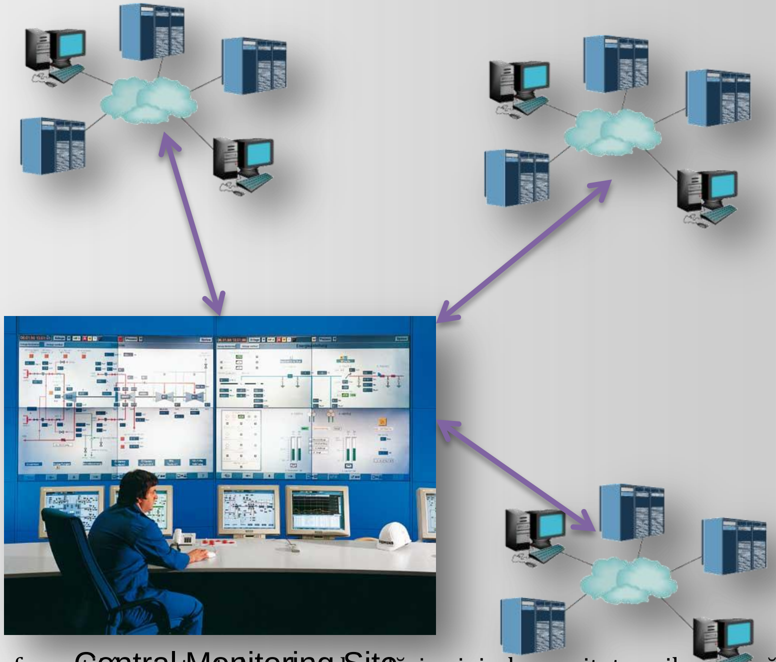


Scenario: Remote Monitoring and Diagnostics

- Control system / equipment / turbine vendor site "monitors" many customer sites, in many countries
- Central vendor site configured for "occasional" remote control
- Industrial network exposed to attack from central site and from other customers / countries
- Remote control attacks, virus propagation

Vendor connection bypasses corporate security protections

Industrial network completely dependent on vendor security



13 Ways Through a Firewall

1) Phishing / drive-by-download – victim pulls attack

2) Social engineering / steal a password / keylogger

3) Compromise domain controller – create fwall acct

4) Attack exposed servers – SQL injection / DOS / etc

5) Attack exposed clients – compromise web servers

6) Session hijacking – MIM / steal HTTP cookies

7) Piggy-back on VPN – split tunnelling / viruses

8) Firewall vulnerabilities –zero-days / design vulns

9) Errors and omissions – bad rules / IT errors

10) Forge an IP address –rules are IP-based

11) Bypass network perimeter – eg: rogue wireless

12) Physical access to firewall – reset to fact defaults

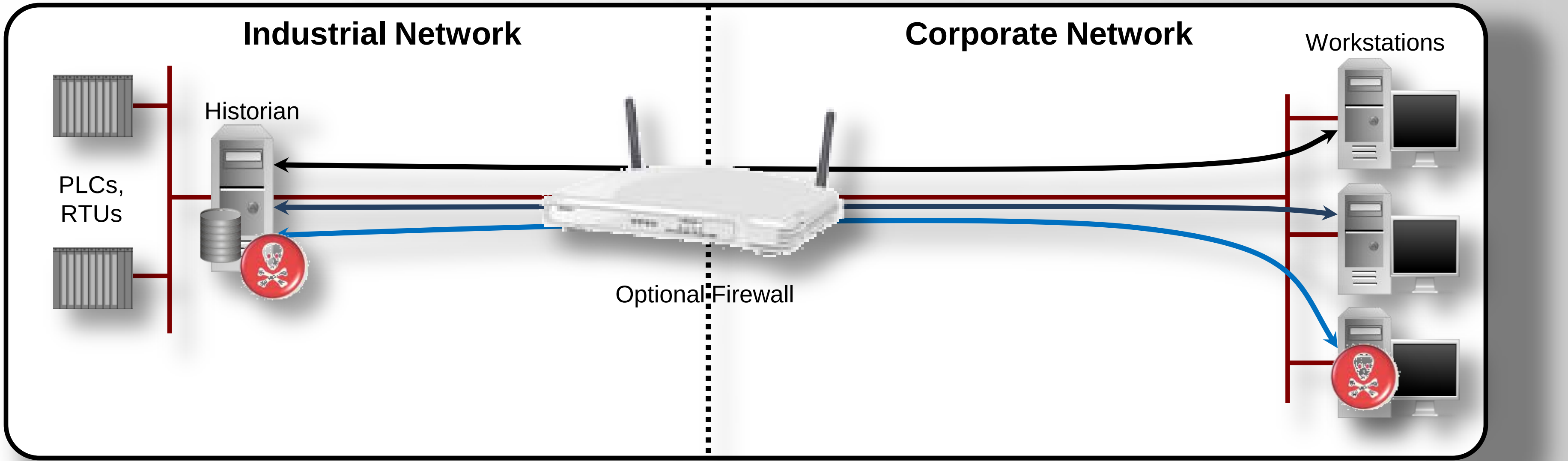
13) Sneakernet – removable media / laptops

Photo: Red Tiger Security

Keeping a firewall secure takes people and processes…

Common Insecure Topology

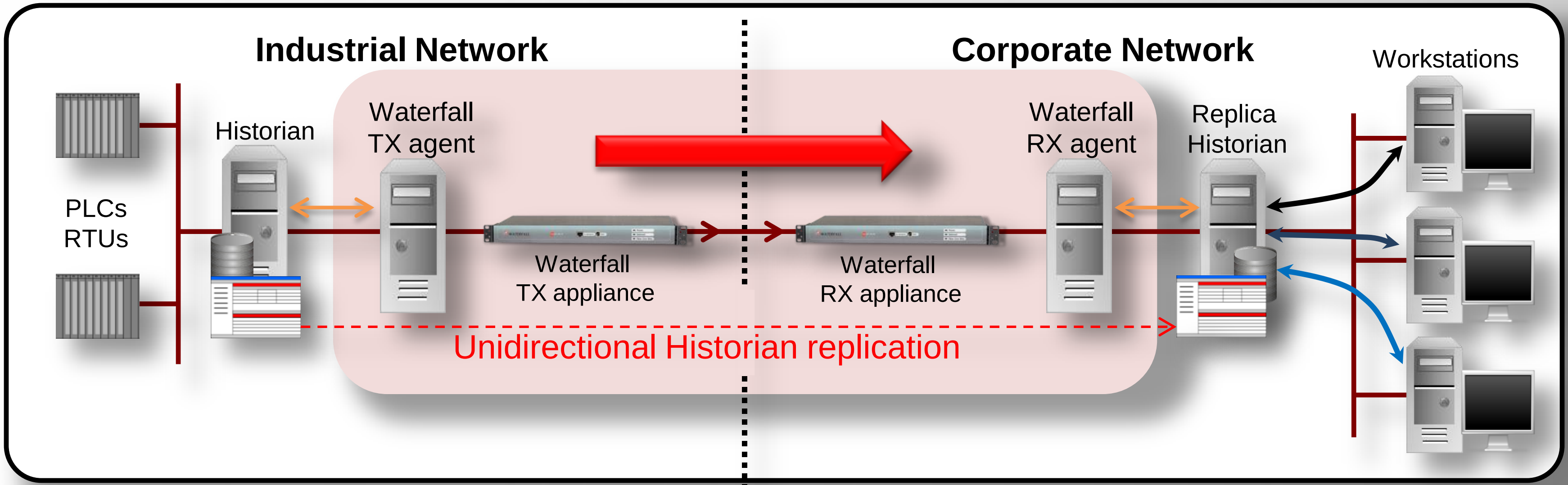
- Critical assets are located in industrial network
- Corporate network connected to Internet is under constant threat
- Corporate workstations directly access Historian on industrial network / DMZ
- Industrial Network and critical assets are at risk



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații în contextul noilor abordări privind securitatea cibernetică.

Secure Historian Replication

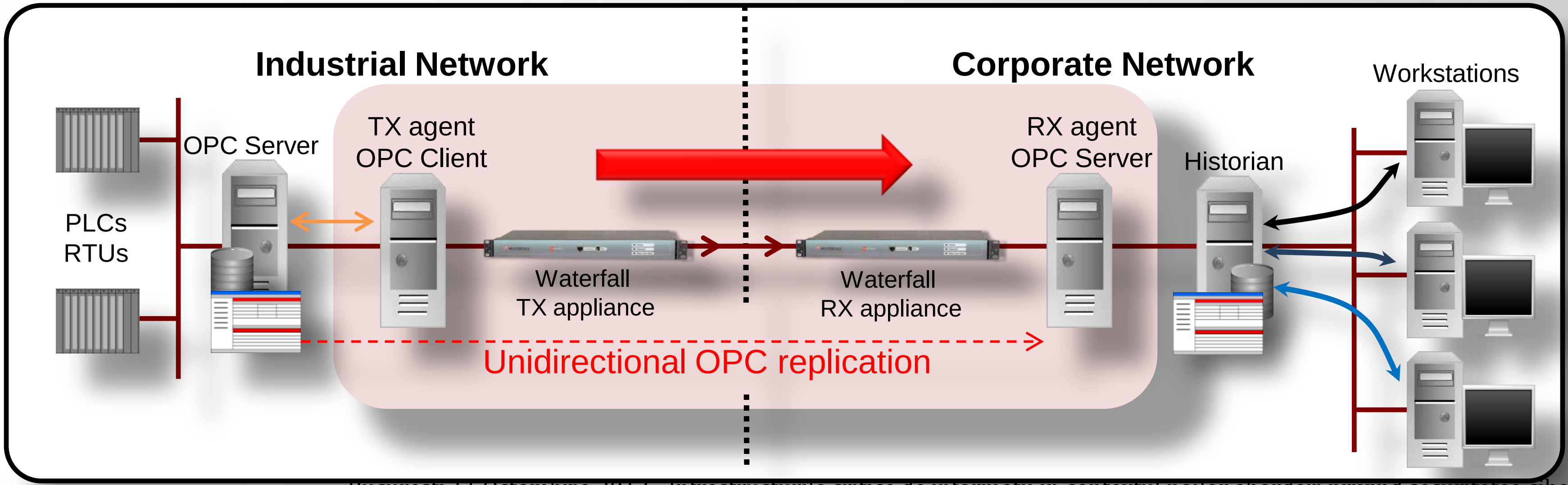
- Hardware-enforced unidirectional historian replication
- Replica historian contains all data and functionality of original
- Corporate workstations communicate only with replica historian
- Industrial Network and critical assets are physically inaccessible from corporate network & 100% secure from any online attack



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

Secure OPC Replication

- OPC-DA protocol is complex: based on DCOM object model – intensely bi-directional
- TX agent is OPC client: gathers data from production OPC servers
- RX agent is OPC server: serves data to business OPC clients
- OPC protocol is used only in production network, and business network, but not across unidirectional gateways



Waterfall Unidirectional Gateway Connectors

Leading Industrial Applications/Historians

- OSIsoft PI, GE iHistorian, GE iFIX
- Scientech R*Time, Instep eDNA, GE OSM
- Siemens: WinCC, SINAUT/Spectrum
- Emerson Ovation, SQL Server, Oracle
- Wonderware Historian
- AspenTech, Matrikon Alert Manager

Leading IT Monitoring Applications

- Log Transfer, SNMP, SYSLOG
- CA Unicenter, CA SIM, HP OpenView, IBM Tivoli
- HP ArcSight SIEM , McAfee ESM SIEM

File/Folder Mirroring

- Folder, tree mirroring, remote folders (CIFS)
- FTP/FTFP/SFTP/TFPS/RCP

Leading Industrial Protocols

- Modbus, OPC (DA, HDA, A&E, UA)
- DNP3, ICCP, IEC 104, 61850

Remote Access

- Remote Screen View™
- Secure Manual Uplink

Other connectors

- UDP, TCP/IP
- NTP, Multicast Ethernet
- Video/Audio stream transfer
- Mail server/mail box replication
- IBM MQ series, Microsoft MSMQ
- Antivirus updater, patch (WSUS) updater
- Remote print server

Waterfall Security Solutions

- Department of Homeland Security selected Waterfall's technology for National Cyber Security Test Bed
- US Patents for SCADA/Control Networks security using Unidirectional Gateways
- Passed only cyber security assessment by Idaho National Laboratories of a unidirectional communications technology
- Certified Common Criteria EAL4+ (High Attack Potential)

Market leader for server replication in industrial environments

FROST & SULLIVAN

2012 BEST PRACTICES AWARD

NORTH AMERICAN NETWORK SECURITY FOR INDUSTRIAL CONTROL SYSTEMS ENTREPRENEURIAL COMPANY OF THE YEAR AWARD

Waterfall Security Solutions

- Headquarters in Israel, sales and operations office in the USA
- Hundreds of sites deployed in all critical infrastructure sectors

FROST & SULLIVAN — Best Practice Award 2012, Industrial Network Security

Gartner — IT and OT security architects should consider Waterfall for their operations networks

PikeResearch Cleantech Market Intelligence — Waterfall is key player in the cyber security market – 2010, 2011, & 2012

- Strategic partnership agreements / cooperation with: OSIsoft, GE, Siemens, and many other major industrial vendors

Secure Application Integration

- Security: absolute protection of safety and reliability of control system assets, from network attacks originating on external networks
- Compliance: best-practice guidance, standards and regulations are evolving to recognize strong security
- Costs: reduces security operating costs – improves security *and* saves money in the long run

FROST & SULLIVAN

Waterfall's unique solutions have the potential to be the industry's next game changing standard

The market leader for server replication in industrial environments

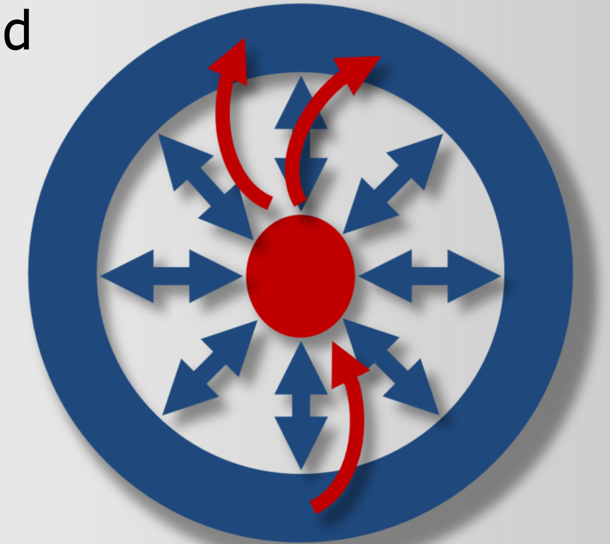
FROST & SULLIVAN

2012 BEST PRACTICES AWARD

NORTH AMERICAN NETWORK SECURITY FOR INDUSTRIAL CONTROL SYSTEMS ENTREPRENEURIAL COMPANY OF THE YEAR AWARD

Central Management: Risks

- IT Helpdesks are the favorite targets of RAT-style attacks: if the IT helpdesk can control everything, so can adversaries in control of the helpdesk
- Active Directory attacks: spear phishing takes over an unprivileged machine and deliberately causes malfunction. IT helpdesk with domain controller privileges investigates and attacker steals credentials
- Vendors connect to many customers – should we trust their security teams?



Central control = central risk

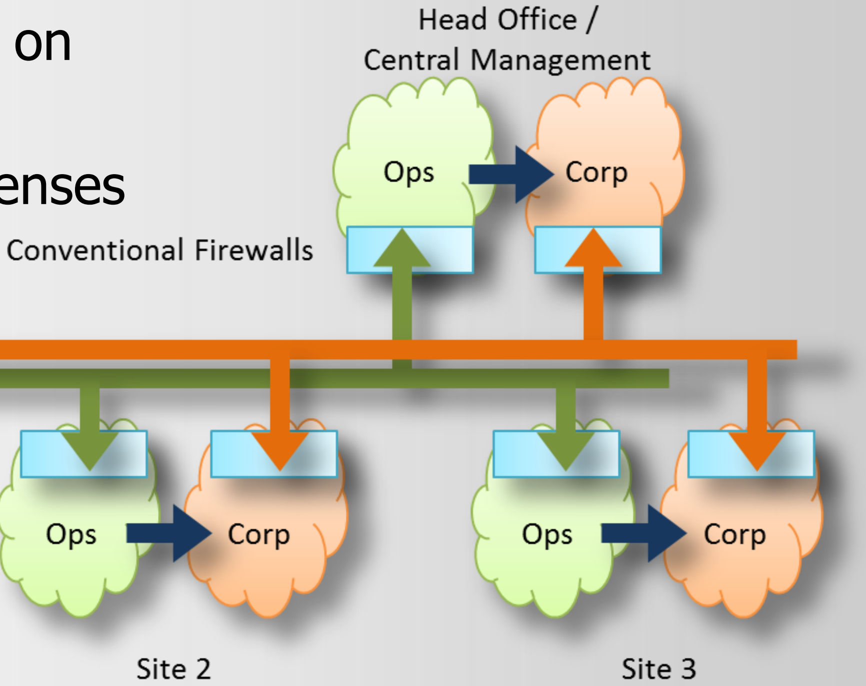
Is this safe? Is this an acceptable risk for dangerous physical processes?

Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

Central Management: Segregated Operations Network

- Operations WAN (green) separate from corporate WAN
- Unidirectional Gateways are only path from operations to corporate – breaks infection / compromise path from corporate WAN / Internet
- Central operations staff have two workstations: one on operations network, and one on corporate network
- Conventional firewalls and other defenses deployed to limit site to site threat propagation

Isolated, yet still centrally managed

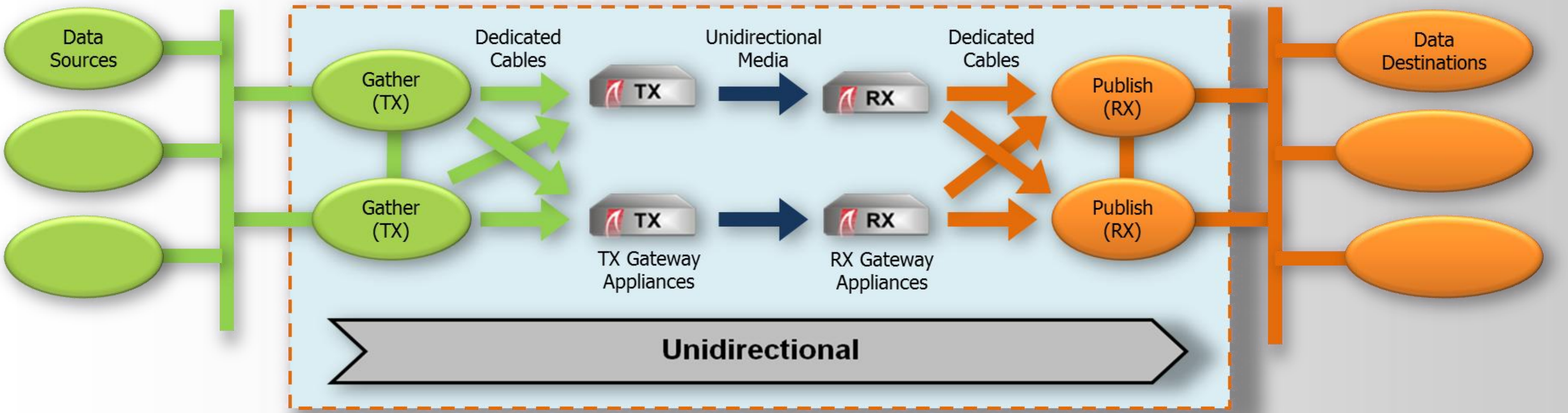


Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

High Availability

- N-way HA architecture supported
- All components are hot-swappable, no reconfiguration needed
- Windows agent host clustering – Microsoft and third-party clustering technologies supported

HA Architecture



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

Cost Recovery

- Unidirectional Gateways capital costs are usually higher than firewall capital costs
- Operating costs are much lower:
  - Firewall management
  - Audit and compliance documentation
  - Remote access training
  - Security incidents
  - Compensating measures

Most customers report operational cost savings repay initial capital costs within 12-16 months

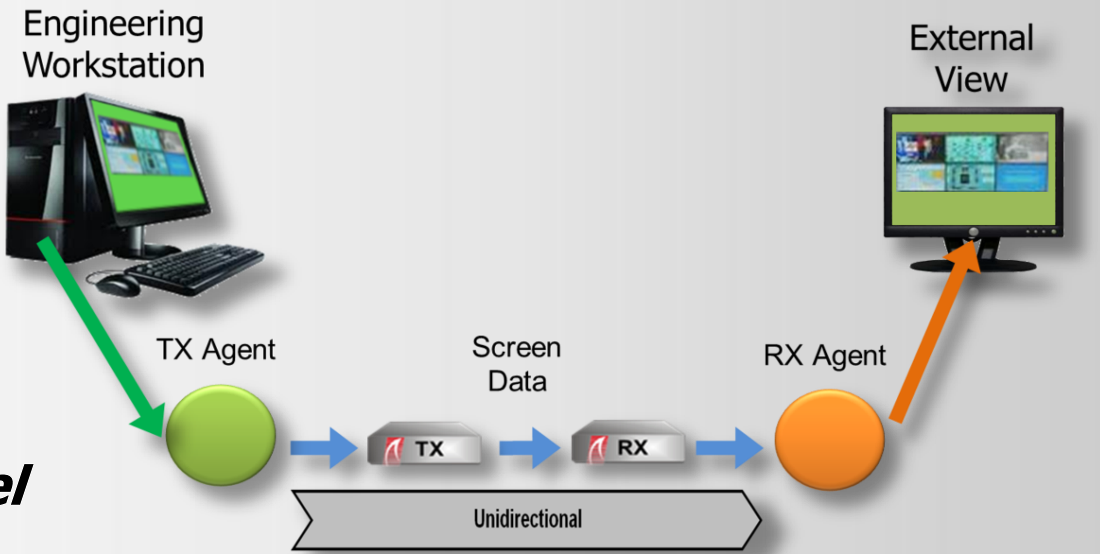
Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații în contextul noilor abordări privind securitatea cibernetică.

Optional Slides

Remote Screen View

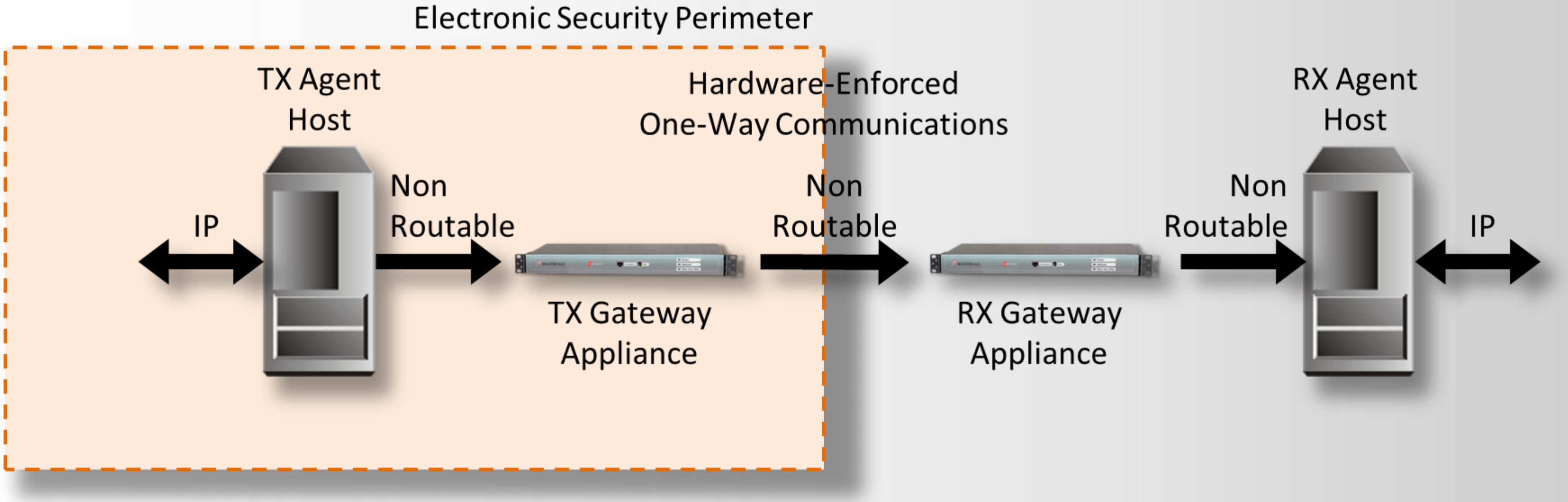
- 2011 Guidance for Secure Interactive Remote Access: "*This common configuration utilizes a unidirectional … outbound … connection to a read-only system. By its configuration, read-only monitoring prevents any access to, or control of, the BPS from occurring.*
- NERC Project 2009-26 supervised remote access: "*… would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?*

CIP: no "supervised remote access" – cyber access is only allowed by authorized local personnel



NERC-CIP V3-V4: Non-Routable Communications

- No IP address on gateways or agent host NICs connected to gateways
- Gateways exchange OSI layer 2 Ethernet broadcasts with agent hosts
- Waterfall-format application data and metadata in layer 2 broadcasts
- No IP addresses communicated from inside ESP to outside
- IP communications sessions terminate in agent hosts



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

NERC-CIP V5

- CIP V5 encourages the use of Unidirectional Security Gateways
- External Routable Connectivity: *The ability to access a BES Cyber System that is accessible from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a* ***bi-directional*** *routable protocol connection.*
- 37 of 103 medium-impact requirements apply only if the affected cyber asset has external routable connectivity

"When you are considering security for your control networks, you need to keep in mind innovative security technologies such as unidirectional gateways" *Tim Roxey, NERC CSSO*

Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informaţii în contextul noilor abordări privind securitatea cibernetică.

Non-ERC High-Impact & Medium-Impact Exemptions

Standard	Req	ERC Exempt	Remaining
002 BES Cyber System Categorization	7	-	
003 Security Management Controls	4	-	
004 Personnel & Training	19	16	3 HI only
005 Electronic Security Perimeters	8	6	ESP & dial-up
006 Physical Security	14	10	1 HI, process, mon, alert
007 Systems Security Management	20	5	
008 Incident Reporting & Resp. Planning	9	-	
009 Recovery Plans	10	-	
010 Change Mgmt & Vuln Assessments	10	-	
011 Information Protection	4	-	
Totals:	103	37	

Plus: many exemptions for Physical Access Control Systems without External Routable Connectivity

Select Customers – North America

Exelon

Ameren

ppl™

SOUTHERN COMPANY

Progress Energy

STP Nuclear Operating Company

Énergie NB Power

Westinghouse

NEXTera ENERGY RESOURCES

FPL.

International Power
GDF SUEZ

ONTARIO POWER GENERATION

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Constellation Energy®

noble energy

PSEG
We make things work for you.

The Communications Security Establishment of the Government of Canada

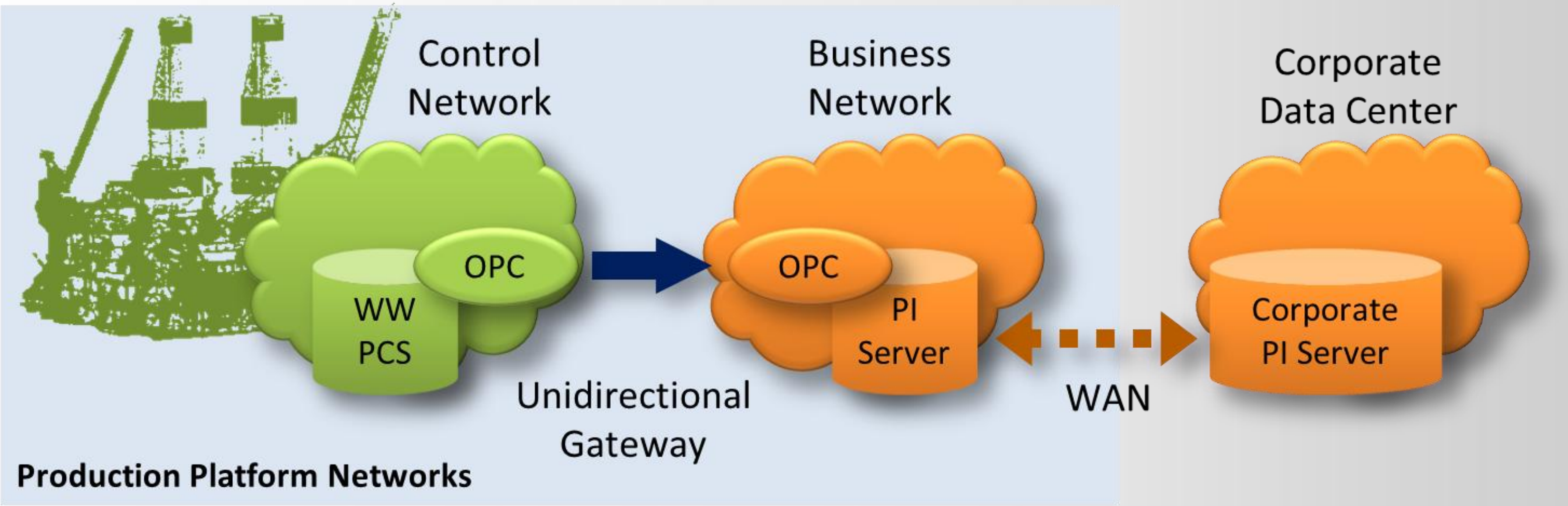
AEP AMERICAN® ELECTRIC POWER

Luminant ENERGY

WATER & SEWERAGE DEPT. DETROIT

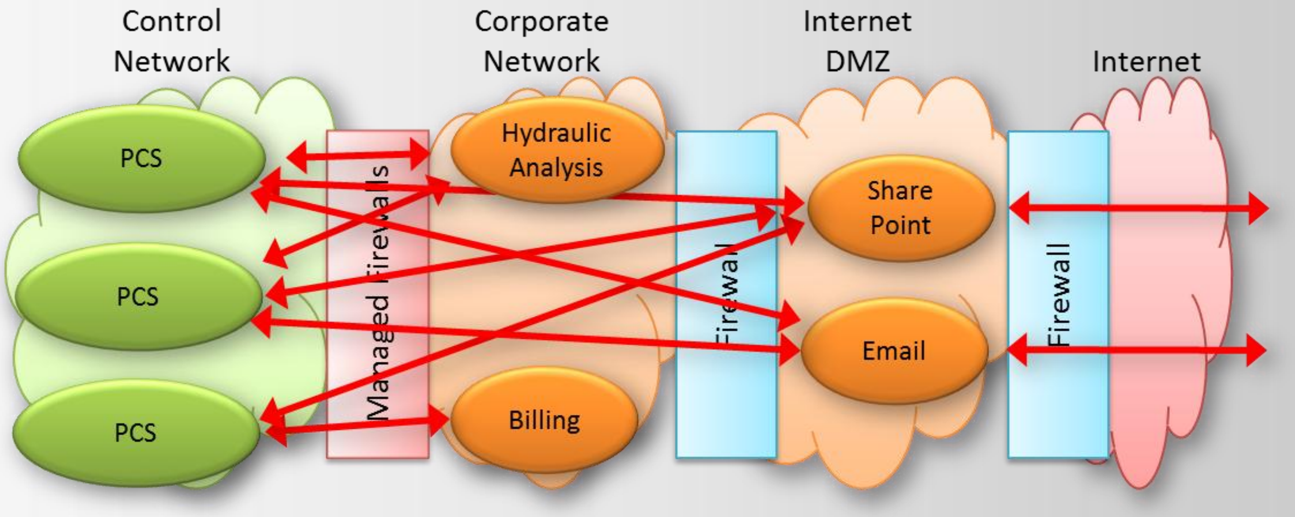
The Solution: Unidirectional Gateways

- Strong security: Unidirectional Security Gateways
- Wonderware Historian-> OPC -> PI Server unidirectional data replication
- Platform PI data from all platforms aggregated to corporate PI server



Detroit Water Original Network

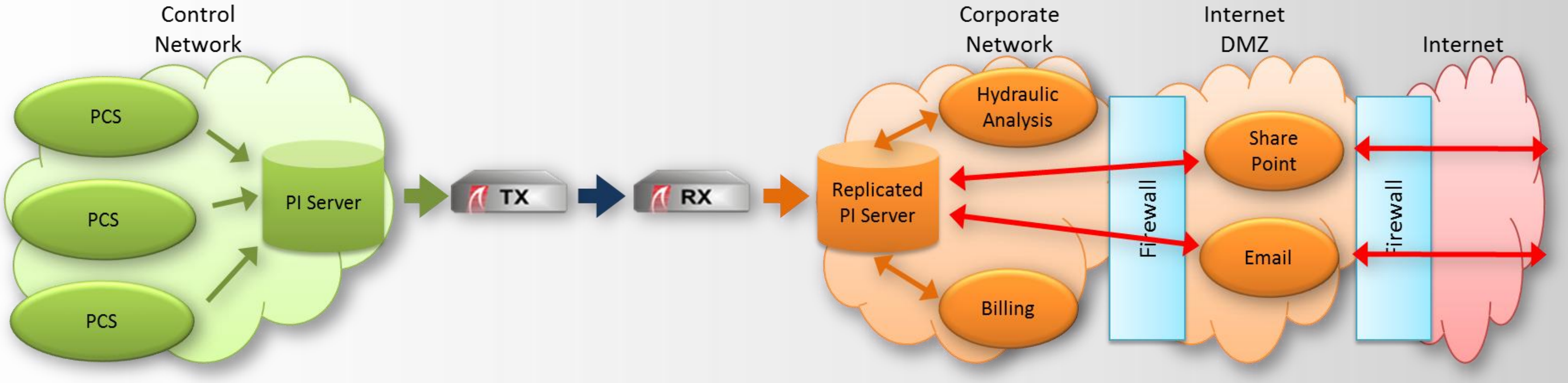
- Third-party-managed HA firewall pair for control network
  - $10,000/month cost
  - Control network originates connections, but traffic is bi-directional
- Many data sources/destinations – "spaghetti code" data flows
- Firewall configuration is opaque – no reviews, no alerts
- Internal audit flagged firewall security as unacceptable



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații în contextul noilor abordări privind securitatea cibernetică.

Waterfall for OSIsoft PI

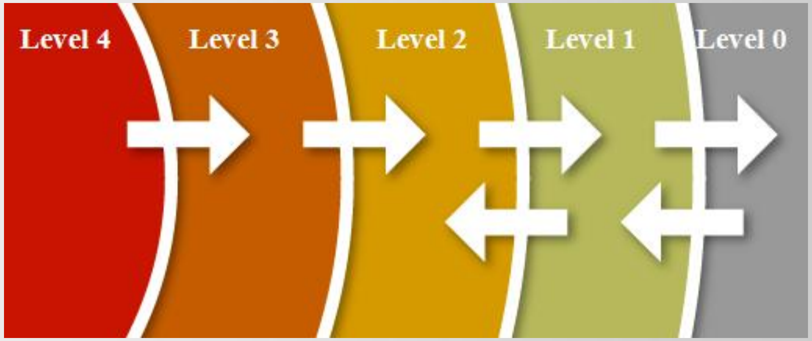
- Deployed OSIsoft PI Server and replica: aggregate all information to be shared with business network
  - All data is available in standard format
  - Adding business applications or data visibility requirements is straightforward
- Unidirectional Gateway solution provides absolute protection from online attacks from external networks



Bucuresti 11 Octombrie 2013 - Infrastructurile critice de informații în contextul noilor abordări privind securitatea cibernetică.

Nuclear Industry

- Deployed at the majority of North American nuclear generators
- Routinely protect safety networks, control networks and plant networks
- Specified in NRC 5.71 and NEI 08-09 regulatory guides



NRC Regulatory Guide 5.71