



WATERFALL

One Way to Connect

"A realistic approach for connecting SCADA/DCS networks to administrative or less secure networks"

April, 2008



Lior Frenkel, Co-Founder and CTO
Waterfall Solutions Ltd.

The material in this document was prepared for the purpose of potential business and is proprietary to Waterfall Solutions Ltd. This document is strictly secret and confidential and is provided with the understanding that it will be held secret and confidential. No part of this document may be disclosed to any third party, copied, reproduced or stored on any type of media or otherwise used in any way without the express, prior, written consent of authorized officers and/or executives of Waterfall Solutions Ltd.



Connecting SCADA networks to external networks

- SCADA 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 SCADA network
- These connections are facilitating *business needs and requirements*
- These connections impose *security risks* to the SCADA network



SCADA networks as the new “cyber-targets”

- SCADA networks are a ***prime target*** for cyber-terror and cyber-crime
 - Nationwide damage – e.g. power outages
 - Media coverage – moral effect and public opinion
 - Huge financial damage
- This is true for all installations, private or governmental, US and worldwide
- Modern SCADA networks 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 networks hacking

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

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

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

The increased connectivity of process control systems to other networks, such as the corporate network and the Internet, further increases the risk of attack from hackers and self-propagating viruses. **Process control systems may be a weak point in your organization's guard against security breaches**

- PA consulting group



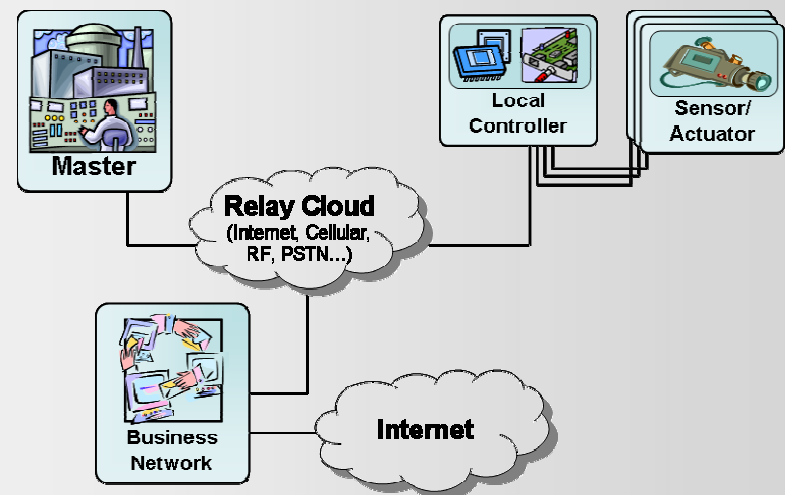
Remote monitoring – Like sleeping with everyone?

- A vendor is remote monitoring its installed equipment, installed at a SCADA network
 - As part of the maintenance agreement (SLA requirement)
 - From one central location
- This vendor is monitoring many *other customers*
 - From one central location
- The SCADA network can be accessed from these other customers
 - Via the central location
 - Other customers' networks may be
 - Less secure
 - Less sensitive
 - Open to the Internet
- A SCADA network commonly has several different vendors remote monitoring its equipment



Connecting SCADA to the business network

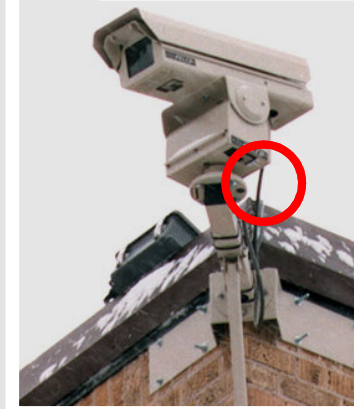
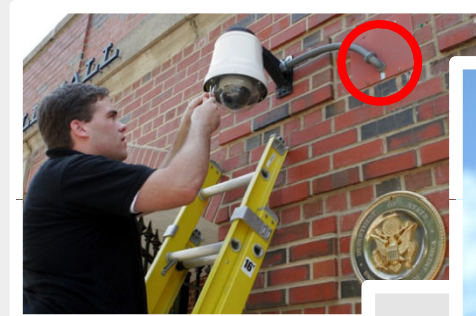
- The SCADA network is required to send online information to the business/administrative networks
 - Production status and statistics
 - Monitoring and status information
 - Etc...
- The business network is commonly connected to other networks, including the *Internet*
- Via these connections, attackers can *gain access to the SCADA network* and facilitate remote, online attacks into it





Surveillance – Who guards the guards

- Modern IP based surveillance devices, such as IP Cameras, are a crucial part of physical security – of the facility and premises
- Deploying IP cameras as part of the surveillance network or via the SCADA network, imposes new threats
- An attacker gaining *access to the IP camera's network cable*, can penetrate the surveillance or SCADA network and commence an attack





External connections

- Connected to less secure networks
 - Business networks, the Internet
 - 3rd Party networks
 - External input devices

- Facilitate remote, online hacking and attacks

- What are the solutions?





The straight forward approach – IT Security

- Deploy standard IT Security means and techniques:
 - Firewalls, Intrusion detection and prevention systems
 - Anti-viruses and Content filters
 - Encryption and digital signatures
- IT Security is not enough here:
 - All IT Security products suffer from software vulnerabilities, bugs and miss configuration – thus, able to be hacked and circumvented
 - Attackers are financially backed up and over motivated
 - Hacking information and know-how is out there
- As a result, more money, resources and effort is, and will be invested by attackers to facilitate an attack on SCADA networks

More than “IT Security” is designed to protect from



The paranoid approach – Total segregation

- Lets keep the SCADA totally and physically segregated 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 network uptime
 - Can not deploy modern IP based sensors
 - Only "analog" devices

Business processes will not work, or will be drastically impaired



The realistic approach – Unidirectional connectivity

- Deployment of physically based unidirectional gateways for all external connections

- As all external connections are, by nature, unidirectional
 - Sending production information to the business network
 - Sending status information to the remote monitoring network
 - Receiving information from IP surveillance devices

- Benefits of the approach - ***A Win-Win situation***
 - Enabling all business needs and requirements (“Straight forward approach”)
 - Top security level – “physical segregation” (“Paranoid approach”)



Why is unidirectional connectivity secure

- Via a physically unidirectional gateway, *data can pass only from one side* (TX side) of the gateway *to the other side* (RX side)
 - No data (not a single bit) can pass the other way around
- This means that between two networks connected via this gateway, there can not be
 - TCP/IP, handshakes,
 - ack's, retransmissions, etc...
- As a result:
 - From the TX side - No online attack can be commenced on the RX side
 - From the RX side – There is no possibility of penetration
- **A physically unidirectional gateway provides full proof security, with no tradeoff for functionality**



Waterfall® - Physically unidirectional technology

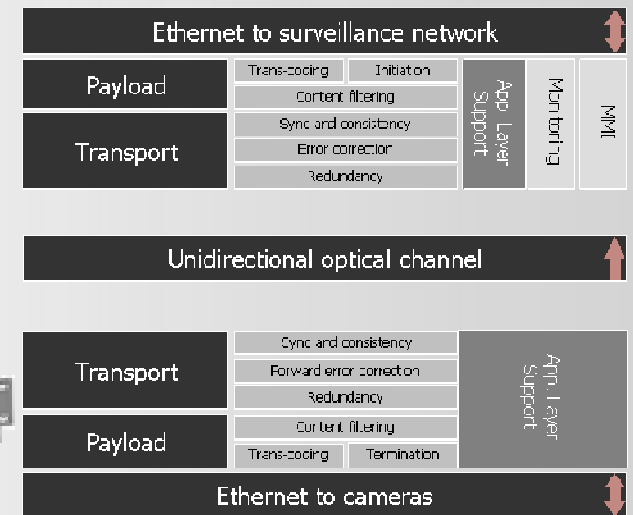
- Field tested unidirectional technology
 - Deployed in large CNI's

- Product family for secure unidirectional:
 - SCADA network monitoring
 - Remote management
 - IP surveillance



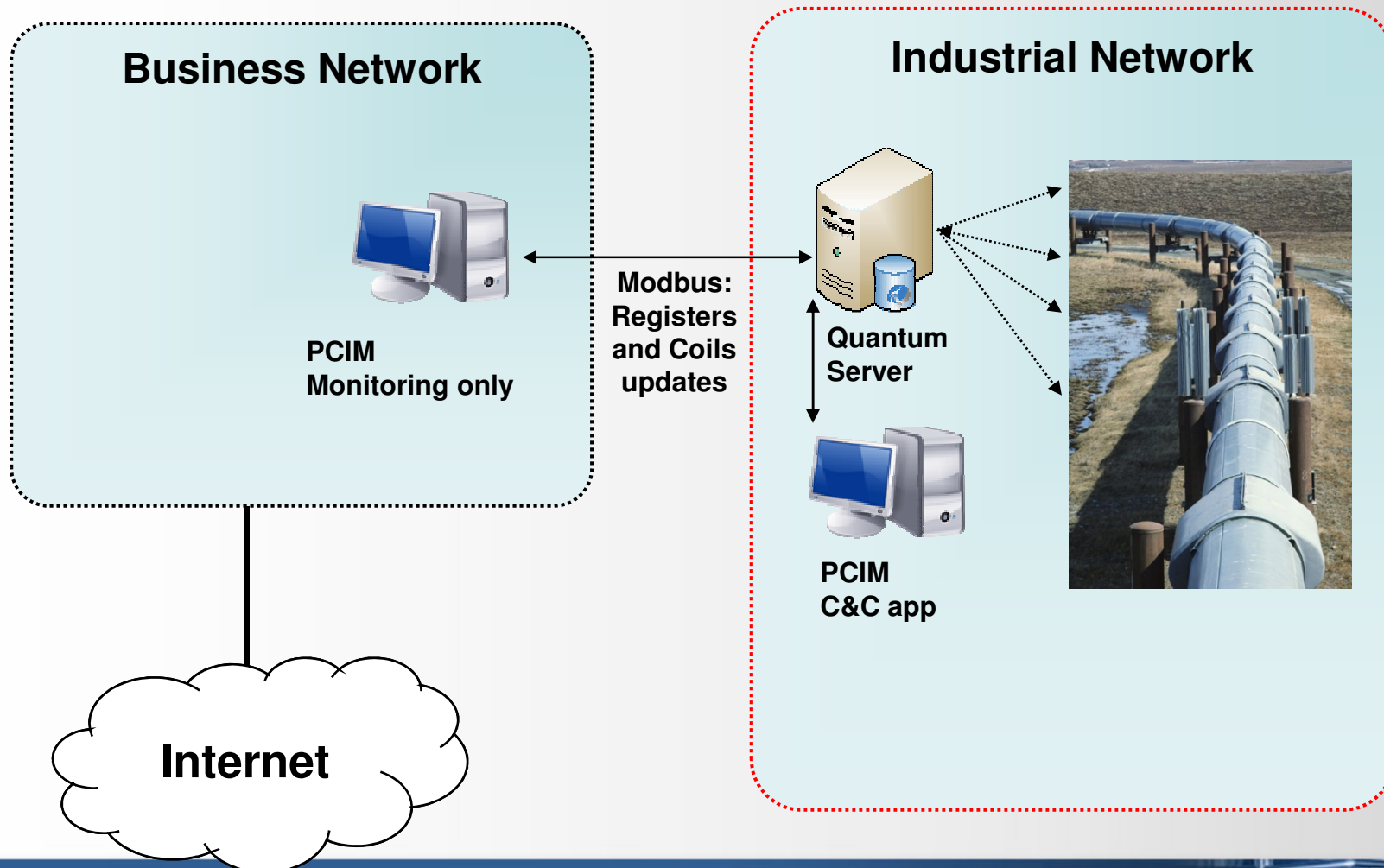
- Support

- SCADA: OSIsoft PI, Modbus, OPC, etc...
- Monitoring: Local/remote FS, FTP, MQ, SNMP, etc...
- Streams: RTSP, RTP, etc...
- 3rd Party: Integral API



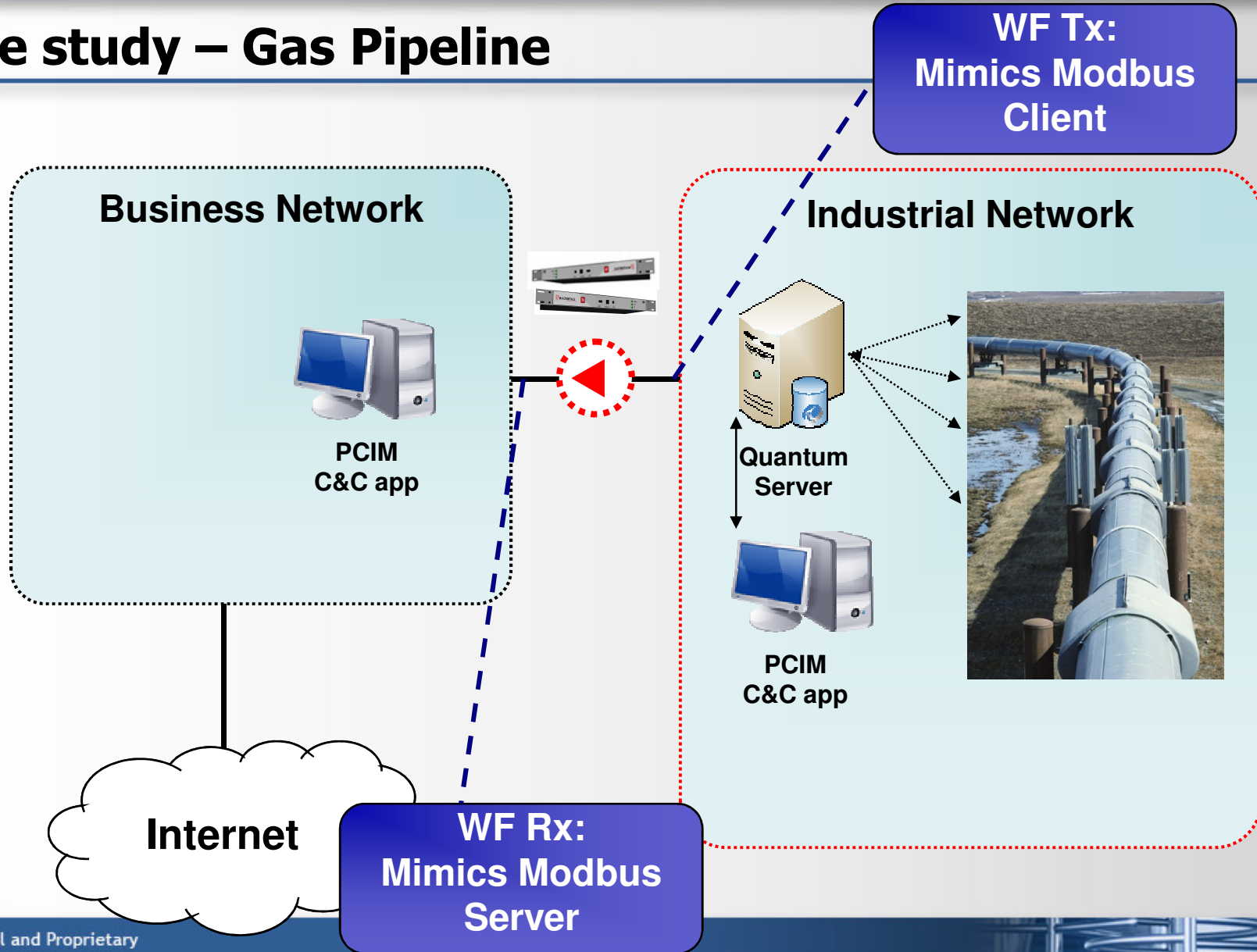


Case study – Gas Pipeline



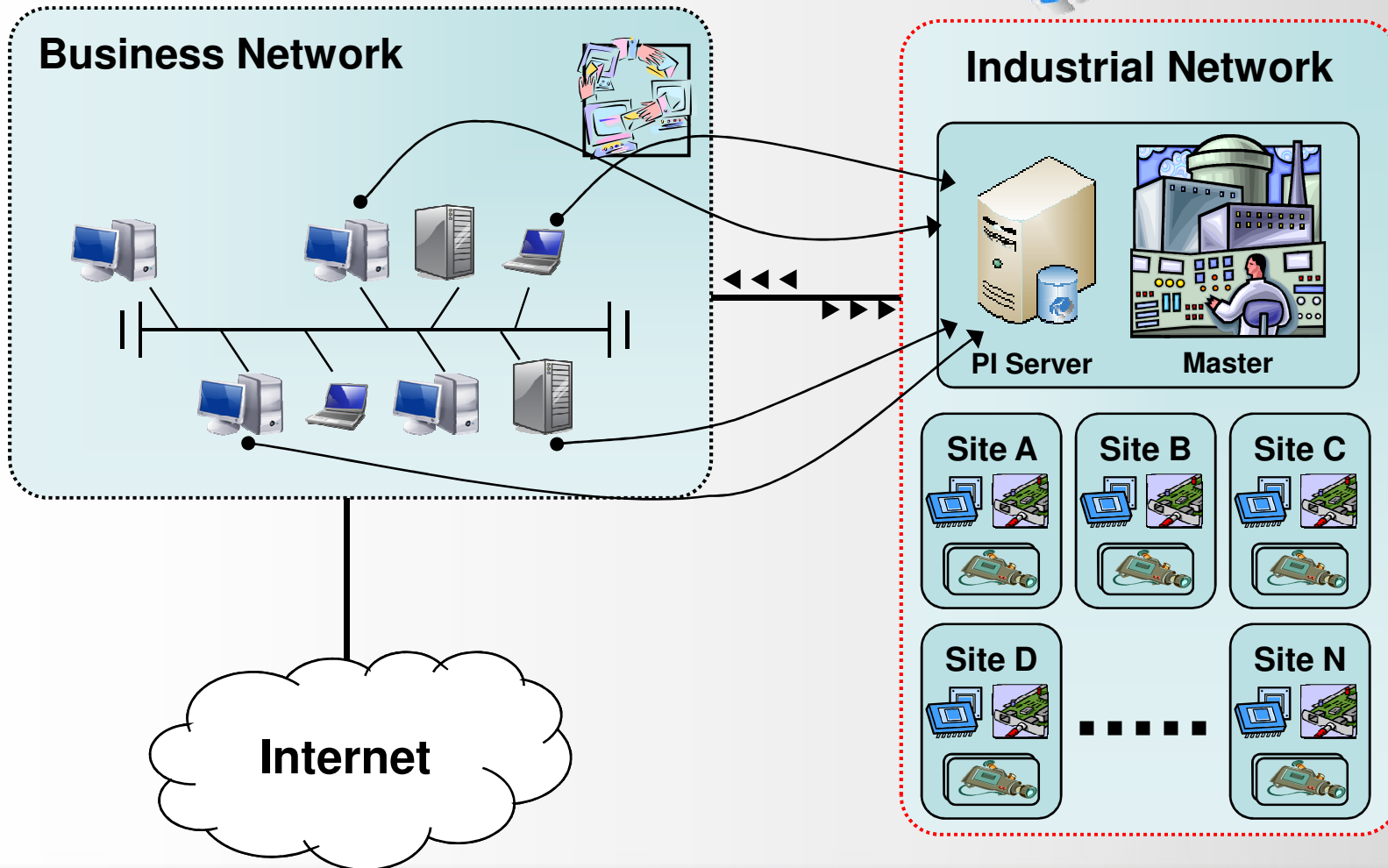


Case study – Gas Pipeline



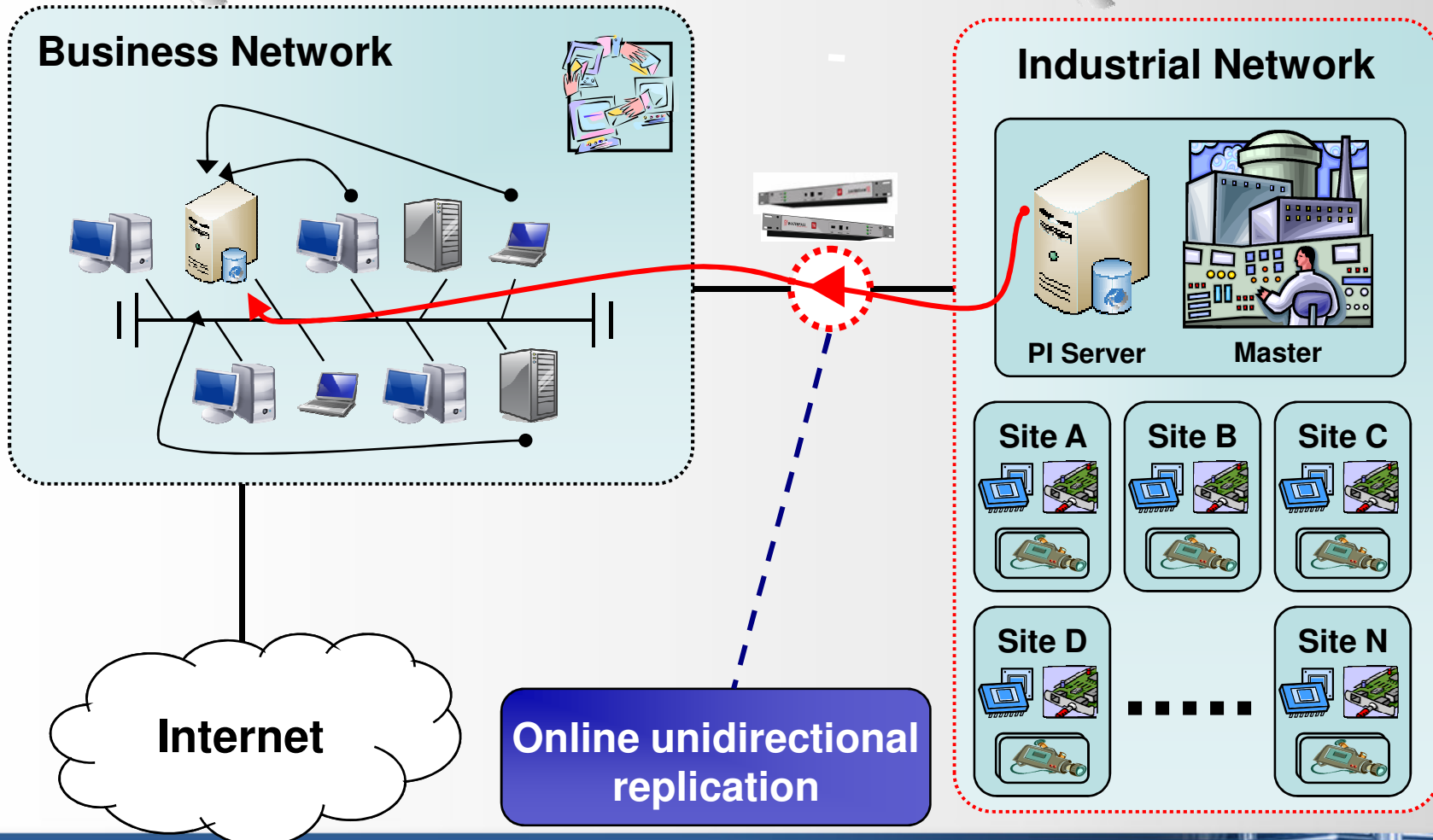


Case study – Electrical power plant



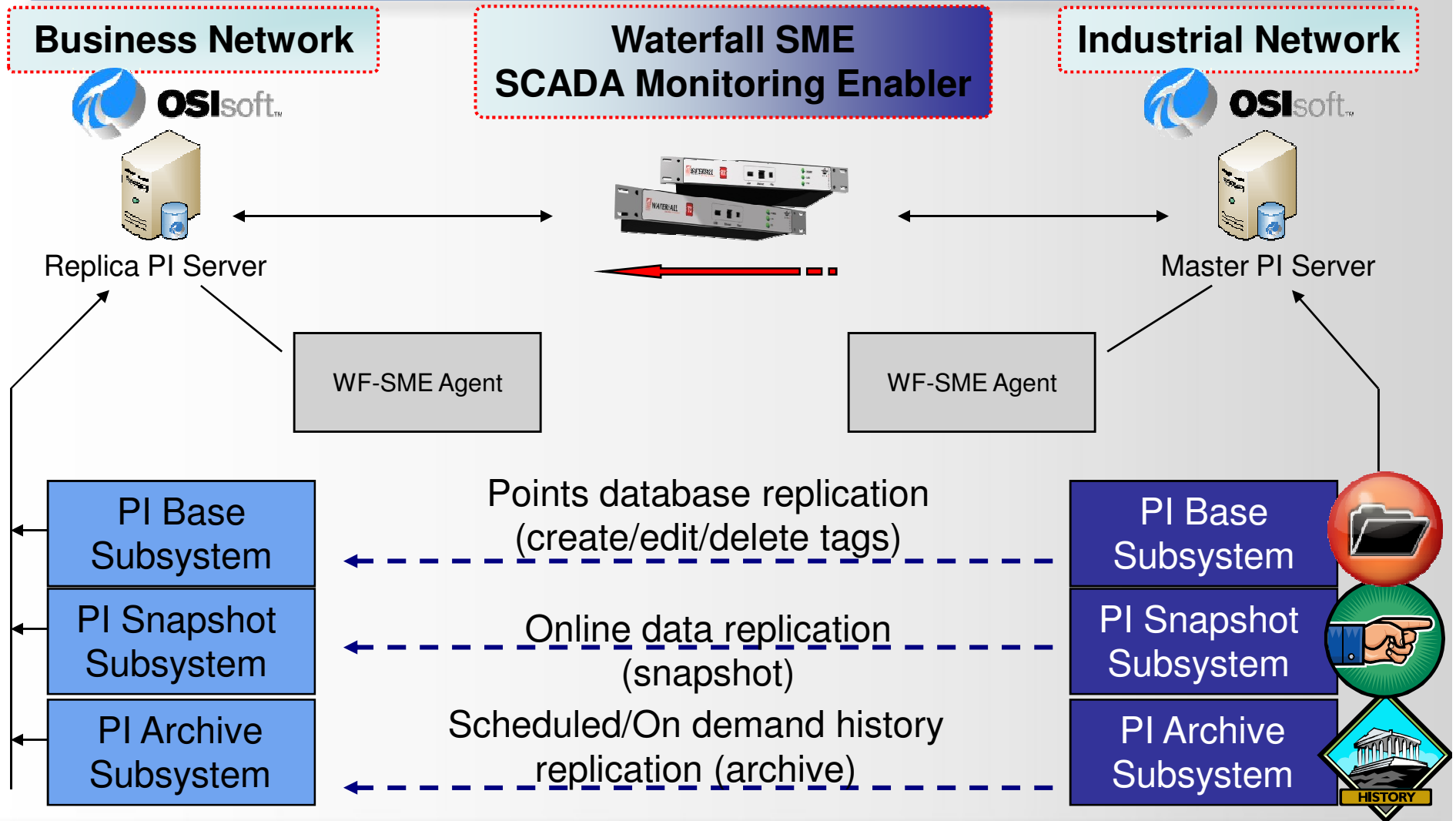


Case study – Electrical power plant





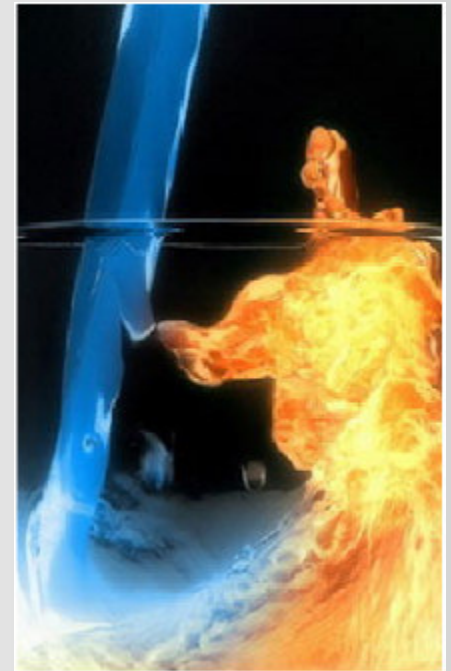
Waterfall – OSIsoft PI Support





Waterfall Solutions LTD

- Waterfall solutions Ltd is the leading vendor for physical unidirectional security products
- Installed based includes large scale CNI's, HLS and Defense facilities, financial organizations, etc...
- Headquarters in Israel, worldwide sales and marketing via channels and strategic alliances





Summary: Secure Security

- SCADA networks are prime targets for cyber-terror and cyber-vandalism
- The damage of a successful attack on such installations is disastrous
- External connections “provide” a relevantly simple way to penetrate and attack the SCADA networks
- Physical unidirectional connections enables SCADA networks to safely use external connections

100% security. 100% monitoring capabilities.

Thank you!

Lior Frenkel, lior@Waterfall-Solutions.com