OSIsoft®

USER CONFERENCE

2008

AMSTERDAM

Empowering Business in **Real Time.**

PI Infrastructure for the Enterprise.

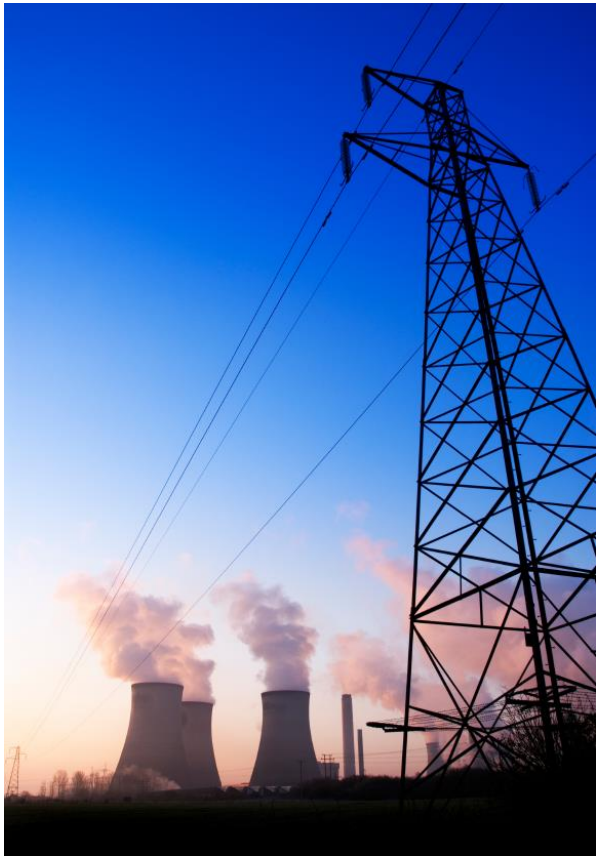
OSIsoft®
USER CONFERENCE
2008
AMSTERDAM

An Ultimate Security Solution for the PI Environment

Gabriel Mazooz

Presentation Agenda

- Israel Electric Corporation (IEC)
  - Some Facts and Figures
- Security Background
  - Cyber Security Threats
- Project Requirements
  - PI System Status
  - The Challenge
- Project Implementation
  - The Players
  - The Working Environment
  - The Process
- Project Summary



Israel Electric Corporation (IEC)

Nazareth, Church of the Annunciation

The Israel Electric Corporation Ltd.

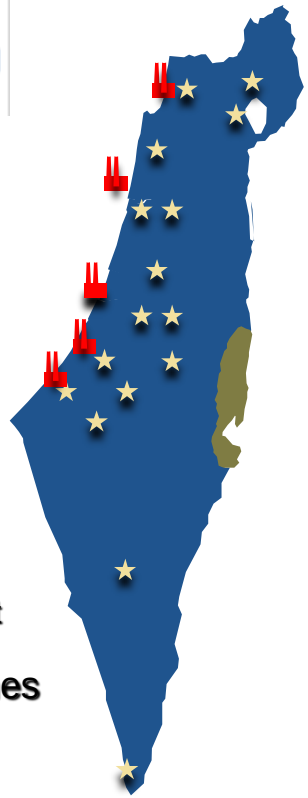
- The Israel Electric Corporation (IEC) - est. 1923
- 99.85% Government owned
- Generates, transmits and distributes practically all the electricity in the State of Israel
- IEC is the sole integrated electric utility in the State of Israel
- One of the largest industrial companies in Israel

IEC – General Profile

- IEC – Main producer (99%) and distributor (100%) of electricity in Israel
- Generating capacity - ~11,000 MW
- Integrated Capabilities – IEC has full design and integration capabilities
- Largest company in Israel with 14,000 employees
- Current government policy calls for the privatization of IEC with competition introduction via Independent Power Producers (IPPs)

The Israel Electric Corporation Ltd.

חברת החשמל



Power plant

Gas Turbines

Israeli Market Operating Statistics 2007	
Capacity (MW)	11,323
Peak Demand (MW)[1]	10,070
Electricity Sales (GWh)	49,323
Population (millions)	7.2
Customers (millions)	2.4
Revenue ($ in millions)	5,009
Total Assets ($ in millions)	17,934

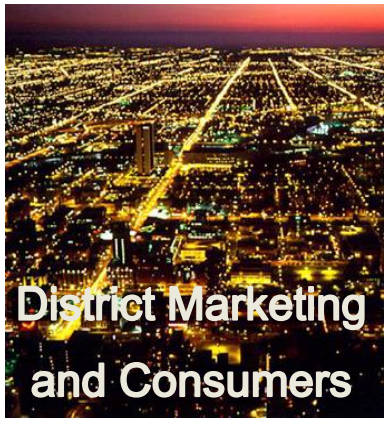
1. **On January 30, 2008 - peak demand of 10,200 MW**

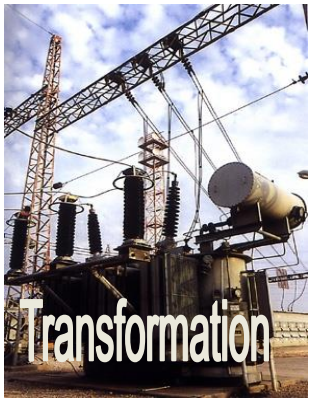
NATIONAL SYSTEM OVERVIEW

SCADA Control System

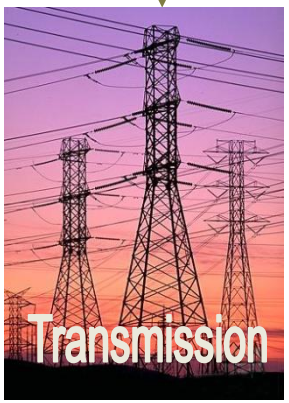
- Ovation
- Bailey
- MAX Control
- ABB
- Siemens

4 District Control Centers





Switching Stations



High Voltage Lines

Generation

Cyber Security – Main Points

- **Critical National Infrastructures (CNIs) are prime targets for Cyber Terror**

- **Process control systems becoming more vulnerable:**
  - **Communication systems converge to IP based networks**
  - **Operating systems with known vulnerabilities are used**
  - **Systems are interlinked**
  - **Growing Worldwide threat environment (more tools, players)**
  - **Remote monitoring and maintenance becoming common**
  - **Interconnectivity with the administrative networks & Internet**

IEC Cyber Security – Main Points

- **IEC is a major cyber-target**
- **IEC is an Electricity island**
- **Strict requirements on availability (essentially 100%)**
- **PI servers are widely in use**
  - **Most of IEC operational data is on PI**

IEC Cyber Security Policy

1. IEC has cyber security policies in effect:
   - Information Security Policy Q1 2008
   - Divisional Policy Q2 2008
2. Cyber security policy is centrally managed by the head of the Generation Division and handled locally by the head of the Computers Dept.
3. The National Information Security Authority (NISA) regulates CNI's networks architectures and cyber security practices & methodologies

Production Division's PI System

- The main information system supplying on-line and real-time data and information on elements and processes of the production division
- Used for making real-time operative decisions by units operators and PI systems users
- Integrated within a great many business process
- Over 500 users system wide
- All-time availability is strictly required

PI Tags Distribution

Alon Tavor	2,000
Hagit	5,000
Ramat Hovav	2,000
Zafit	1,000
Gezer	2,000
National Dispatch	50,000
T & D	50,000
Test	1,000

Total Tags 214,000

Generation Division Headquarters	5,000
Haifa	20,000
Orot Rabin	30,000
Reading	5,000
Eshkol	10,000
Rutnberg 1-2	10,000
Rutnberg 3-4	20,000
Hadera Environment Association	1,000

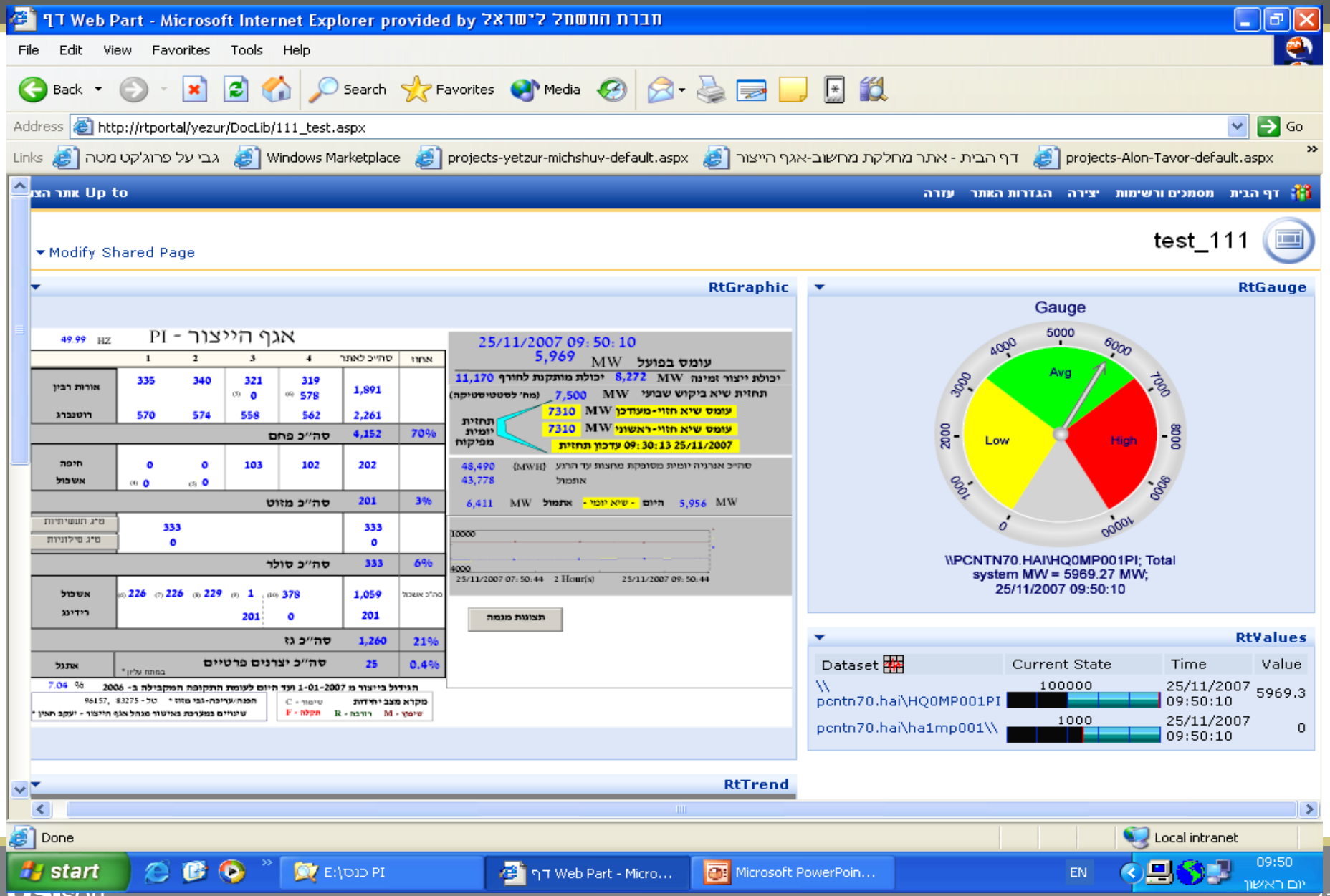
15 Sites

PI System Referent / Administrator

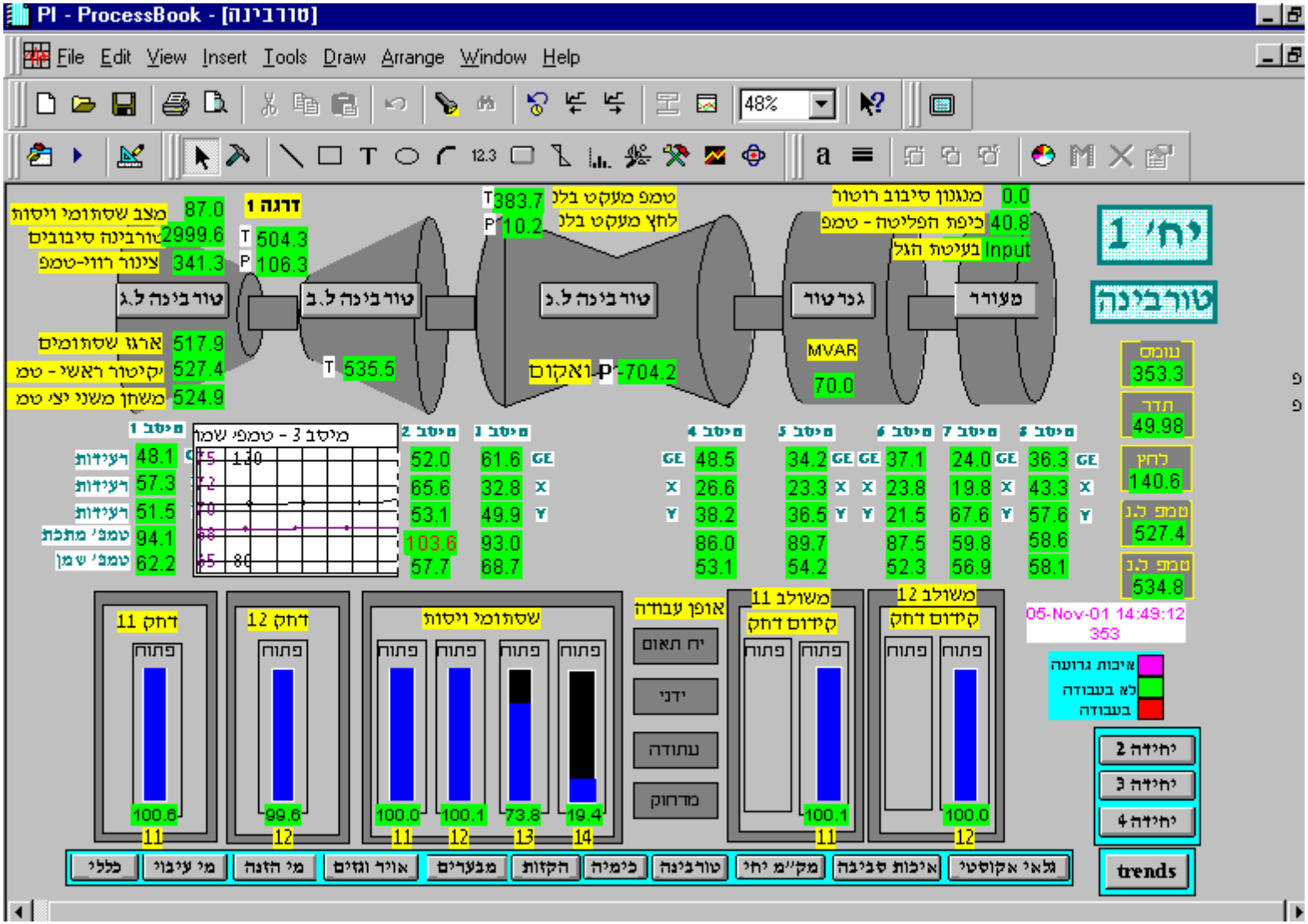
- Responsible for PI system- one at each IEC site
- Operates and maintains on-site PI system
- Develops local applications and displays
- Local Point of Contact for all PI related issues
- Generation Division convenes a PI Referent Forum

Generation Overview - Units Status

RT – PORTAL: Overview - Units Status



Locally developed Application - Example



PI System Expanding

- PI system being used for reporting on the move:

The Challenge

- To arrive at a truly and absolutely protected PI system, while still enabling fully operational PI connectivity with the administrative network
- Quick and easy implementation – minimal downtime
- Minimal cost

PI Security Project - Start to Finish :

Less than a month !!!

The Main Players

- **IEC – Generation Division as the initiator and project leader**
- **Ludan Systems – Solution Developer and Integrator**
- **Waterfall Security Solutions – Solution Developer & Vendor**

Ludan Software and Control Systems - Facts

- Ludan Software and Control Systems - subsidiary of Ludan – Tech Ltd.
- Company activities: Project design, integration. installation and execution of industrial IT and process control projects
- Vast experience in computerized systems and process control large scale projects
- Over 20 years experience integrating PI systems
- Visit us @: www.ludansy.co.il

Waterfall Security Solutions - Facts

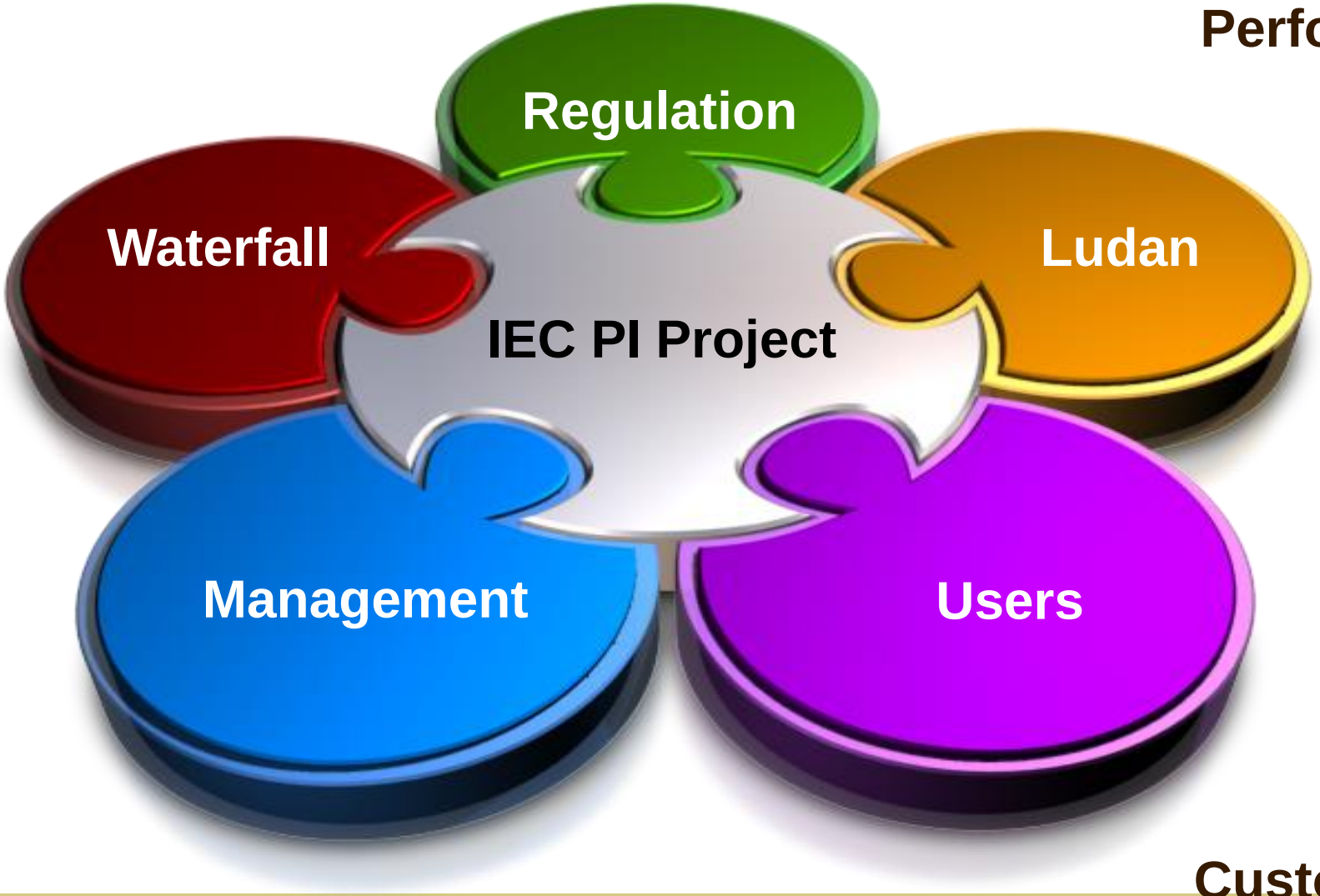
- Privately owned security firm, based in Israel
- Spun-off in 2006, 25 employees, >110 installations worldwide
- Solutions based on unidirectional connectivity harnessed in patented technology integrating hardware and software modules

WATERFALL
One Way to Connect

- Visit us @: www.waterfall-security.com

Overall Project Players

Performers



Customers

Solution Concept – Main Points

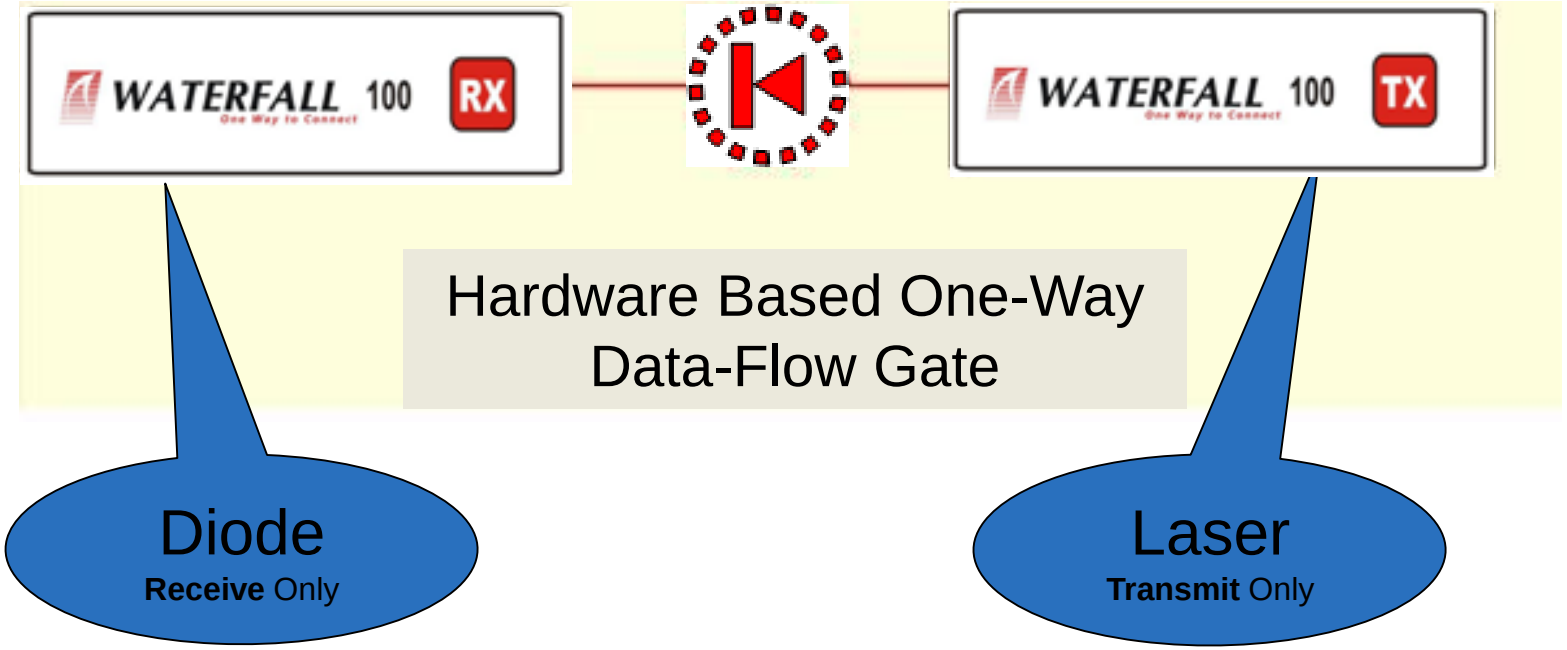
- Segregate PI systems for maximum security
- Allow PI connectivity only via a strictly one-way communications solution (Waterfall One-Way™)
- Use the unidirectional connectivity to replicate PI server information on an external server
- Administrative PI users can only access the replicated PI server

Waterfall Unidirectional Connectivity

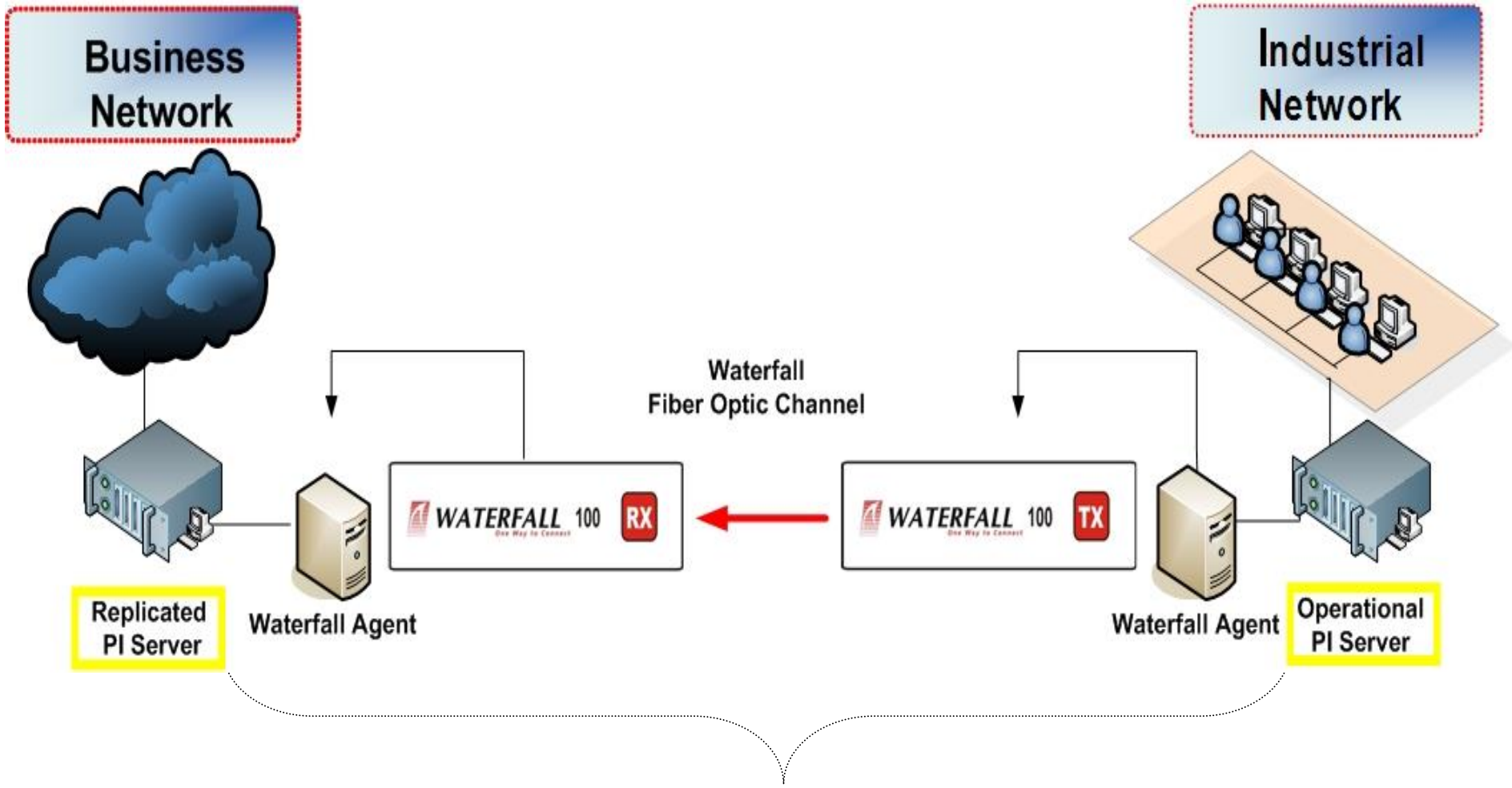
- A novel approach to network and data security
- Deployment of physically based unidirectional gateways for external connections
- Leveraging the unidirectional logic of such connections for:
  - Sending production information to the business network
  - Sending status information to the remote monitoring 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")

Making Truly Unidirectional Connections

- **Realizing absolute unidirectional connectivity in the optical domain:**

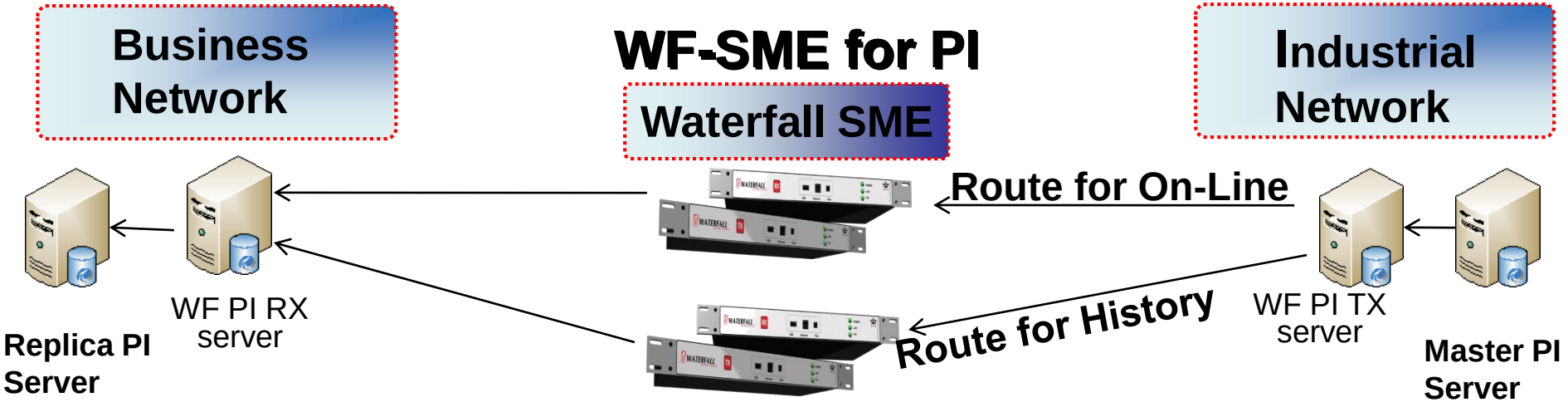


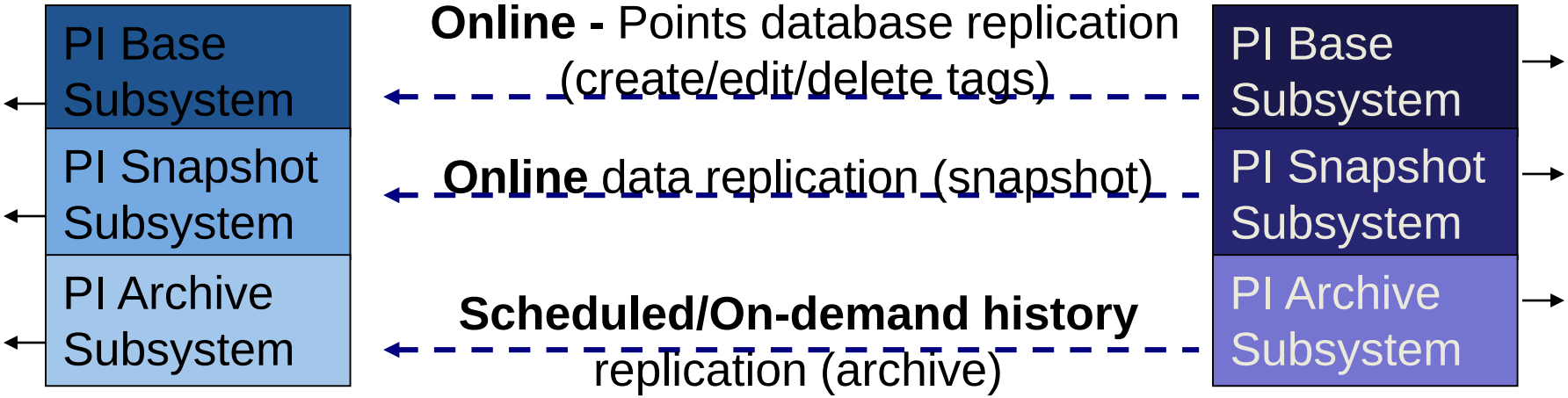
PI System – Solution Components



Innovative W.F. element

WF-SME* PI System – Data Paths

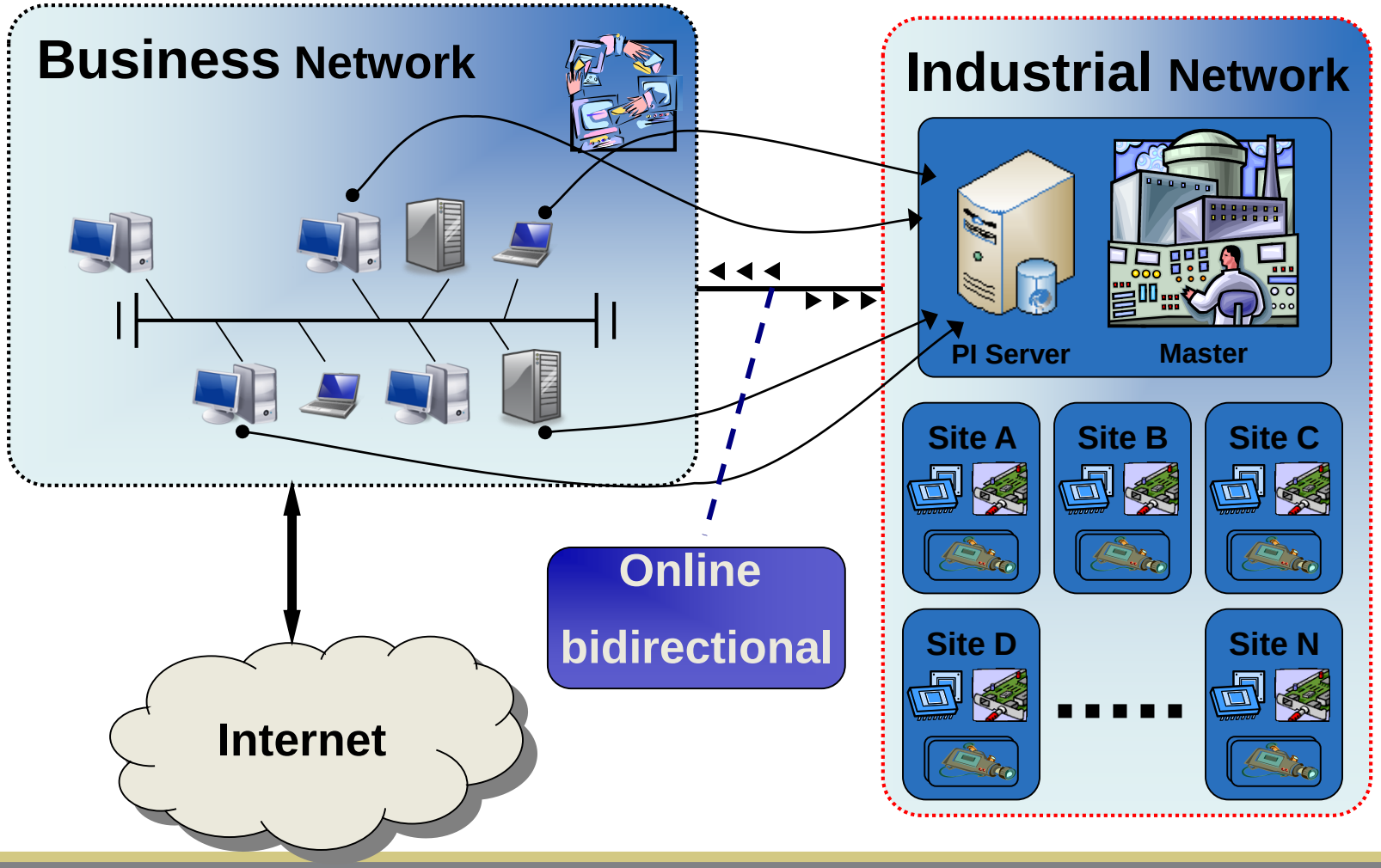




* Scada Monitoring Enabler

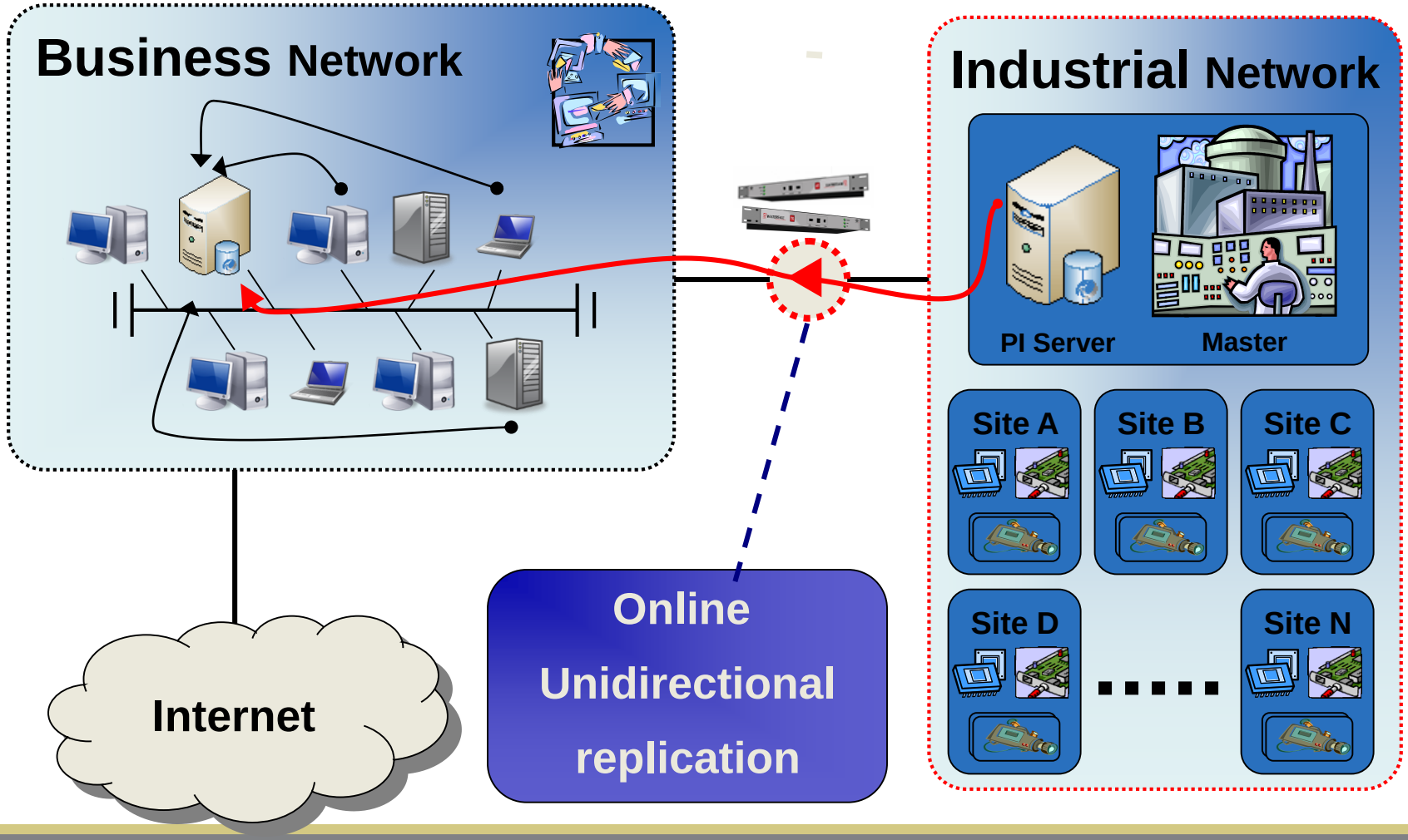
PI System – Before (Insecure)

- **Highly risky architecture**



PI System – After (Secure)

- One way data flow



Project Implementation

- **Process I - Infrastructure**
- **Process II - Sand box installation**
- **Process III - Declaration**
- **Process IV - New server declared operational**
- **Process V – Monitoring**

Project Implementation - Process I

- **Infrastructure:**
  - **Analysis**
  - **Design**
  - **Procurement**

Project Implementation - Process II

- **Sand box installation:**
  - **Original system runs in parallel**
  - **Running 2 or 3 test clients in this period**
  - **Evaluation of performance**
  - **Database and application testing**

Project Implementation - Process III

- **Move Date To New Topology: Declaration**
- **Alert all users & managers**

Project Implementation - Process IV

- New server declared operational
- Referent is coached regarding the new system
- Connection between networks is cut off
- Users are moved to the new system
- Applications and database are rigorously inspected

Project Implementation - Process V

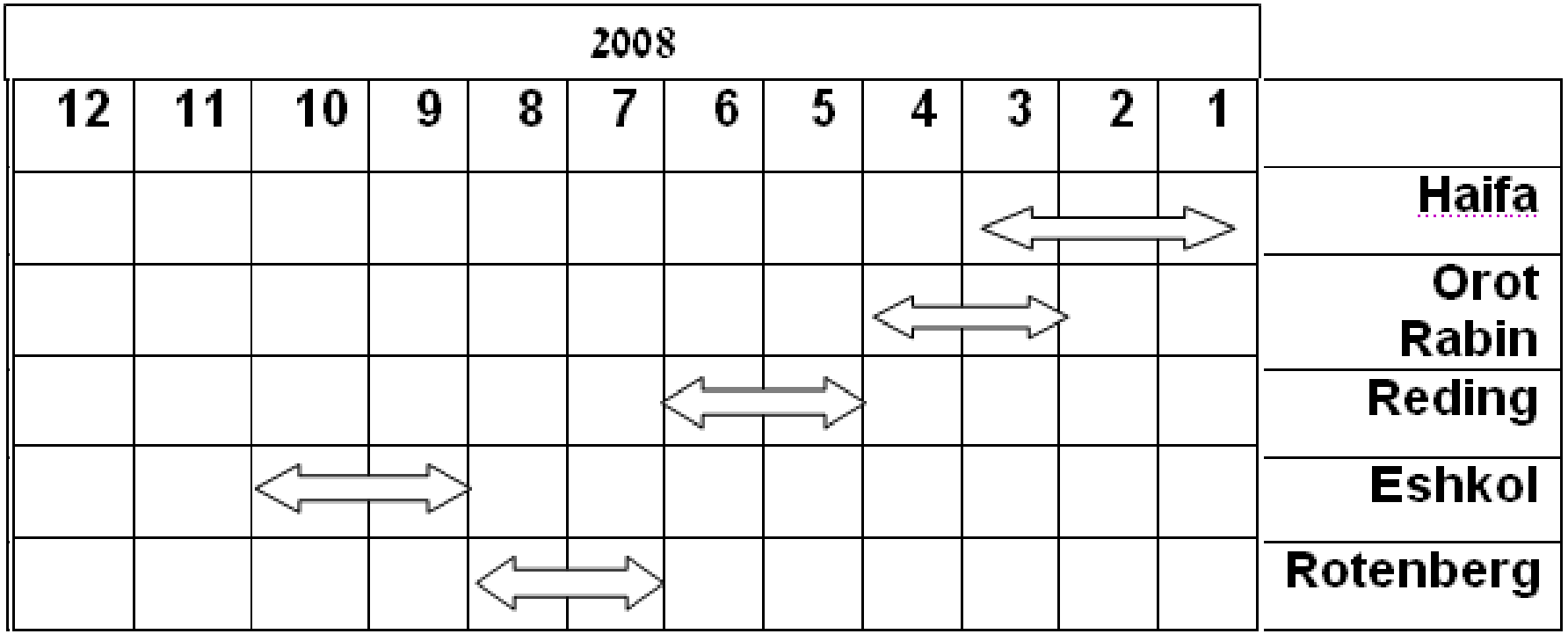
- **Monitoring**
  - **Servers**
  - **Interfaces**
  - **Data**
  - **Users**
  - **Displays**
  - **Applications**

Project Completion

- **Performance - 50k tags**
  - **~ 1 sec. latency end to end.**
- **Uptime 2 years and counting**
  - **0 downtime on all systems installed**
- **User experience**
  - **Seamless passage to the new system**
  - **100s of concurrent users nation wide**
  - **Support *POC is unchanged**
  - ***Point of contact**

Project Management Timeline

Done



Future Prospects

- **Future phases and improvements will include:**
  - **Install base increased to include more turbines:**
    1. **Alon Tavor**
    2. **Hagit**
    3. **Gezer**
    4. **Tzafit**
    5. **Ramat Hovav**
  - **Allow for remote monitoring over unidirectional links:**
    1. **Gezer**
    2. **Hagit**
  - **And in the near future:**
    3. **Alon Tavor**
    4. **Eshkol**

Summary

- State of the art security solution for the PI environment
- “Sleep well at night”
- Project timeline less than 1 month
- PI user experience is unchanged
- Performance is practically unaffected
- Negligible maintenance
- PI Availability is:
  - Stable
  - Reliable
  - Fully Secured

Question Time

OSIsoft®

USER CONFERENCE

2008

AMSTERDAM

THANK YOU