TOTAL FINA ELF

PI

in an IT security

Context

Marc Weinberg

Process Engineering

ATOFINA Research – Feluy (B)

Email marc.weinberg@atofina.com

Marc Souche

ATOFINA DCTI

Atofina Technical Center Lyon (F)

Email: marc.souche@atofina.com

Ref MS/ II n° 22/03Rev 0

TOTALFINAELF GROUP

- World's 5th largest oil company.
- Active in more than 120 countries, organized in over 900 consolidated companies.
- With more than 122000 Employees.
- Structured in 3 branches
  - Upstream : Exploration & Production, trading Gas & Electricity
  - Refining and Marketing
  - Chemistry

ATOFINA

- Chemical branch of the group.
- World's 6th largest chemical company
- With more than 70000 employees more than half of the human resources of the TotalFinaElf Group. (11000 in the US)

Key activities:

- Base chemicals and Polymers: Olefins, Aromatics, Polyethylene, Polypropylene, Styrene, Polystyrene, Elastomers, Chlorochemicals and Solvents, VCM, PVC and Downstream, Fertilizers.
- Intermediates and Performance Polymers: Acrylics, PMMA, Fluorochemicals and Peroxides, Thiochemicals and fine Chemicals Performance Products, Additives, Engineering Polymers, Formaldehyde resins, Agrochemicals.
- Specialties: Rubber-based products (Hutchinson - Mapa Spontex), Adhesives (Bostik Findley), Resins including Photocure Resins (Cray Valley, Sartomer, Cook Composites Polymers), and Electroplating (Atotech).

Corporate Technology Group (CTG)

- **Part of the STRATEGY & RISK ASSESSMENT direction**
- **The CTG is a Network of technologists of all three branches of TotalFinaElf.**
- **Missions :**
  - Promote free access to the Group's technical competencies and help maintain the teams' technical know-how.
  - Raise the Group's technological level by pooling experiences and by formal and informal transfer of information relating to know-how.
  - Promote optimization of the Group's technological resources and exploit the Group's leverage due to size when negotiating with suppliers.
  - Coordinate action with industry and equipment standards organizations.
  - Anticipate the Group's future technology needs.
  - Monitor external technology changes and keep pace with them when appropriate.
  - Manage key technical suppliers relation ship (for ex OSISOFT,…)

PI within TOTALFINAELF

- Over 100 systems installed from refineries to small fine chemical sites
- ATOFINA (hosting most of the PI servers) has a dedicated PI global support team.
- Yearly internal PI User meetings in Europe and US
- Internal Training sessions
- Corporate founding to develop internal PI tools, to test and evaluate new PI features
- Used on all levels of the company… from APC DATABASE to IT network monitoring

TFE & "Cyber" Security

- Standard IT security is today addressed in almost all industries
- Process IT security adds a new dimension to the security: A SAFETY DIMENSION

POTENTIAL PHYSICAL HARM

TO PEOPLE

AND ENVIRONMNET

TFE & "Cyber" Security

- The CTG has launched a working group to address the problem on Group level

- Primary Objectives:
  - Remove any danger for action on plant operation from outside (Internet, Intranet , Corporate LAN).
  - Guarantee System Availability and System integrity

- Secondary Objective
  - Improve confidentiality on information

TFE & "Cyber" Security

Background

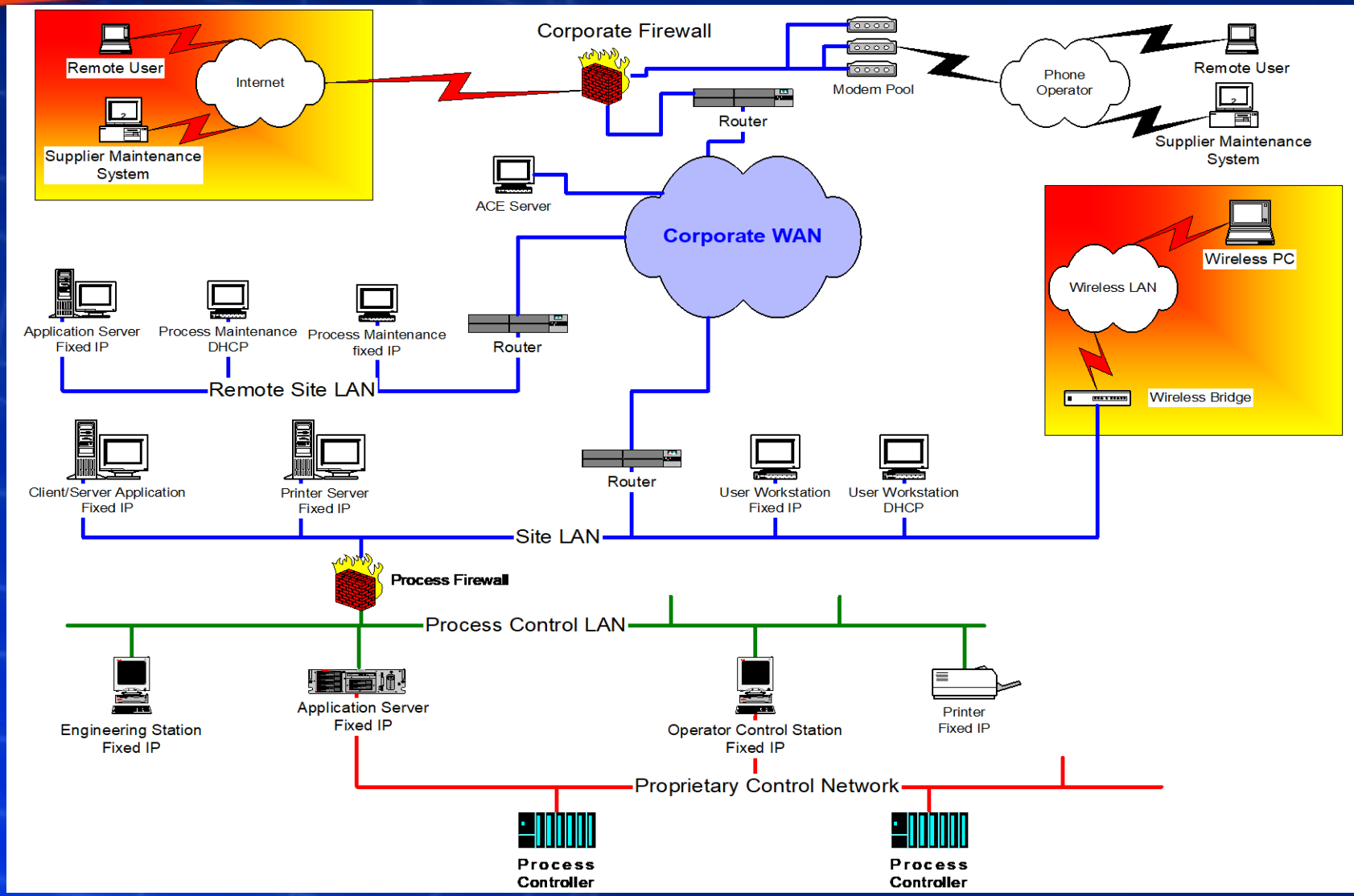
- **Yesterday:**
  - Control systems used proprietary hard and software which gave the system a certain immunity against external attacks.
  - Systems were stand alone applications with (almost) no connections to the external world.
- **Today:**
  - Cost reduction pushed all suppliers on relying more and more on standard hard and software in process control and process control related applications:
    - TCP/IP; Windows NT W2K; wiring and connectors; network structure and elements (hubs, switches, …)
  - Increased demand for information exchange (ERP (SAP), LIMS, RTPDB, ASSET Management) pushed supplier to deliver open solutions, often resulting in weakened security.

TFE & "Cyber" Security

Our project → Goals:

- Establish the interconnection requirements of the sites.
- Study a tailor-made solution for the interconnection of an IT network with a process control network (compatibility with vendor specifications).
- Run one some pilot sites (set-up, functional and intrusion test).
- Define a 'low cost' standard solution which gives a minimal certified and tested solution affordable for all sites.
- Define an implementation guideline for those interconnections.
- Define a corporate standard for the security of process control systems.
- Roll out the standard solution

A Global Picture



TFE corporate process IT security standard

- Today we have defined a corporate security standard for process IT.
- Implementation phase is rapidly ongoing.
- Effects on own personnel and on subcontractor staff (remote maintenance).
- Among effects on all interconnections between ‘office’ IT and process IT there are also important drawback on how to structure, install and locate a PI server in a (our) secure environment.

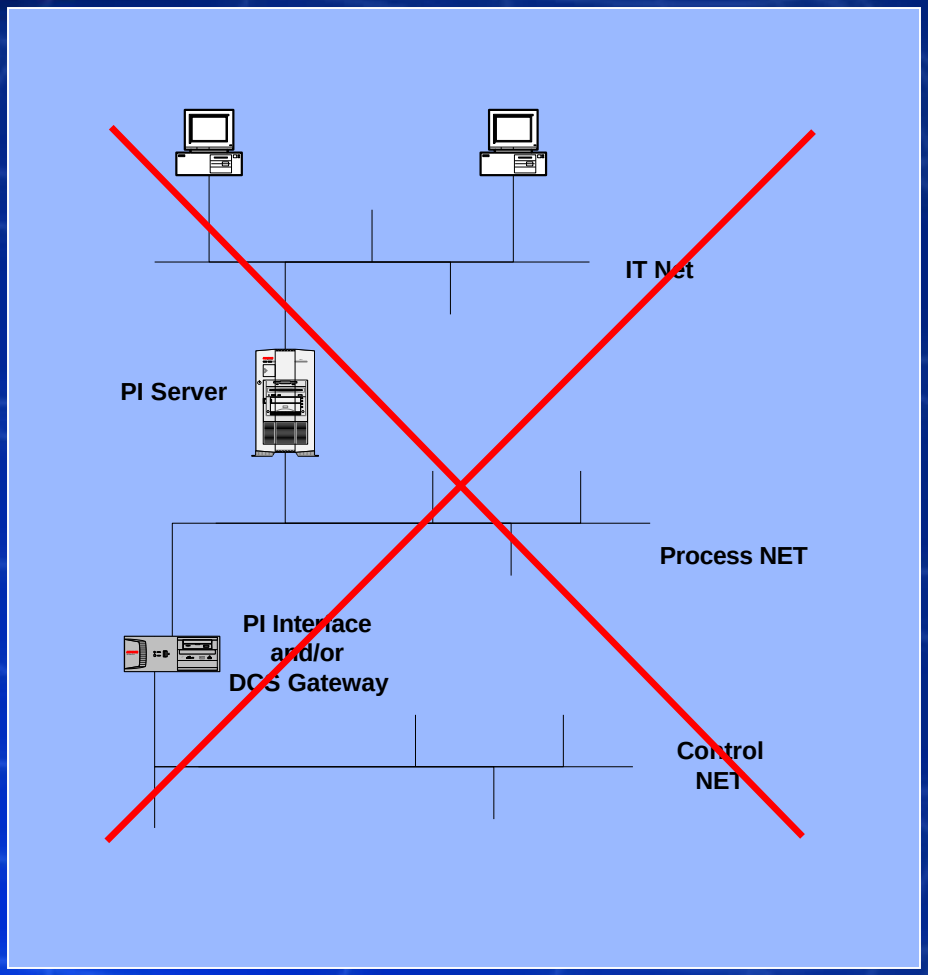
PI & IT security

- Where to put a PI Server ??
  - If it is a server for data consultation : office side.
  - VPN between PI server and Firewall.
  - Use dedicated PI interface on process side.
  - APC PI Servers or PI Servers with DCS write capability on process side. Data transfer to 'Office IT' with PItoPI on separate PC.

PI & IT security

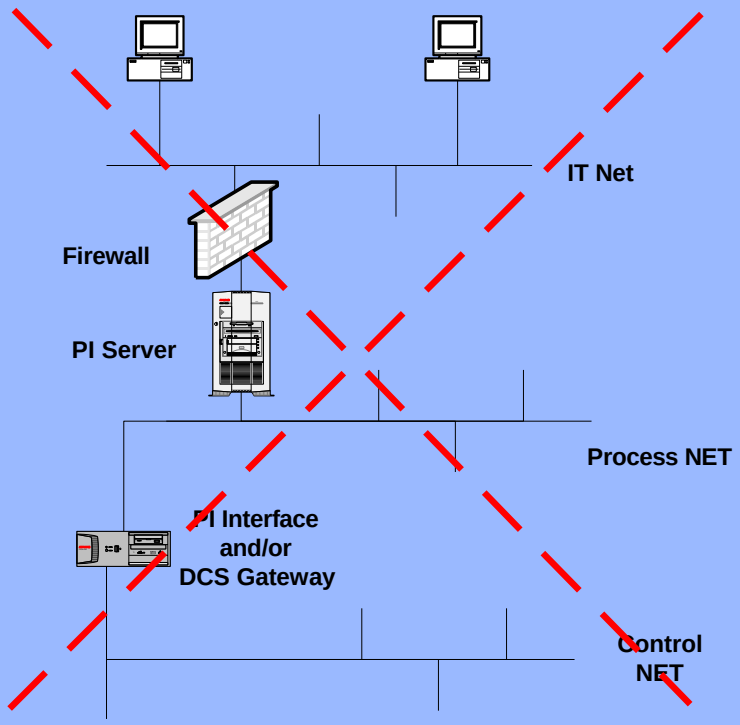
- What to install
  - On Process PI servers or interfaces on process side : nothing
  - On Office PI Servers:
    - Securemote client (VPN) with preshared secret.
    - Service to start tunnel automatically (with no operator interaction)

PI Servers in a secure environment



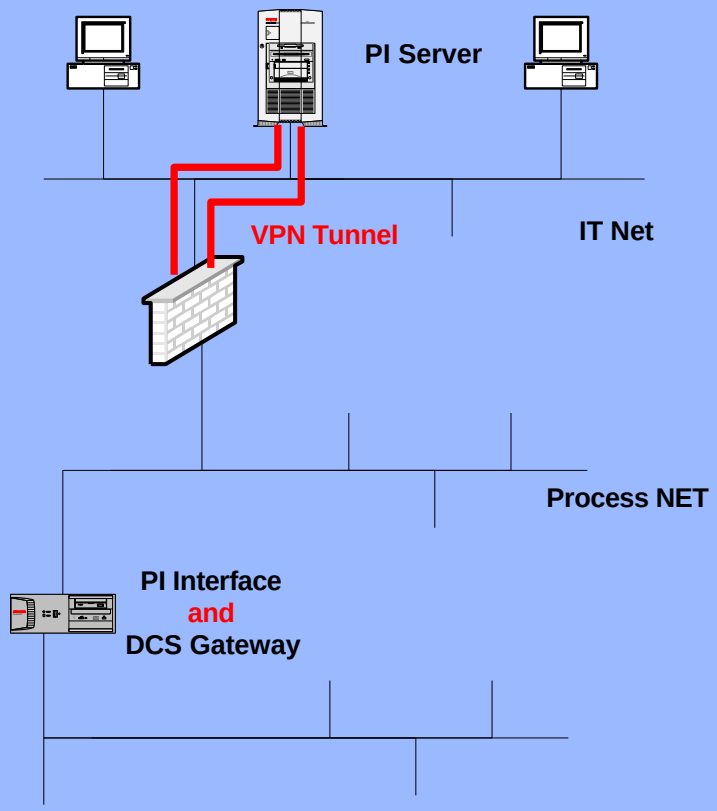
- Recommended OSISOFT scheme witch was used primirlally
- The danger is the vulnerability of the Windows PI Server.
- Once someone has access to the PI server, he has physical access to the Process Net and through the PI interface to the Control Net.
- Potentially dangerous if the PI server has write capability. (Erroneous or malicious change of a tag configuration)

PI Servers in a secure environment



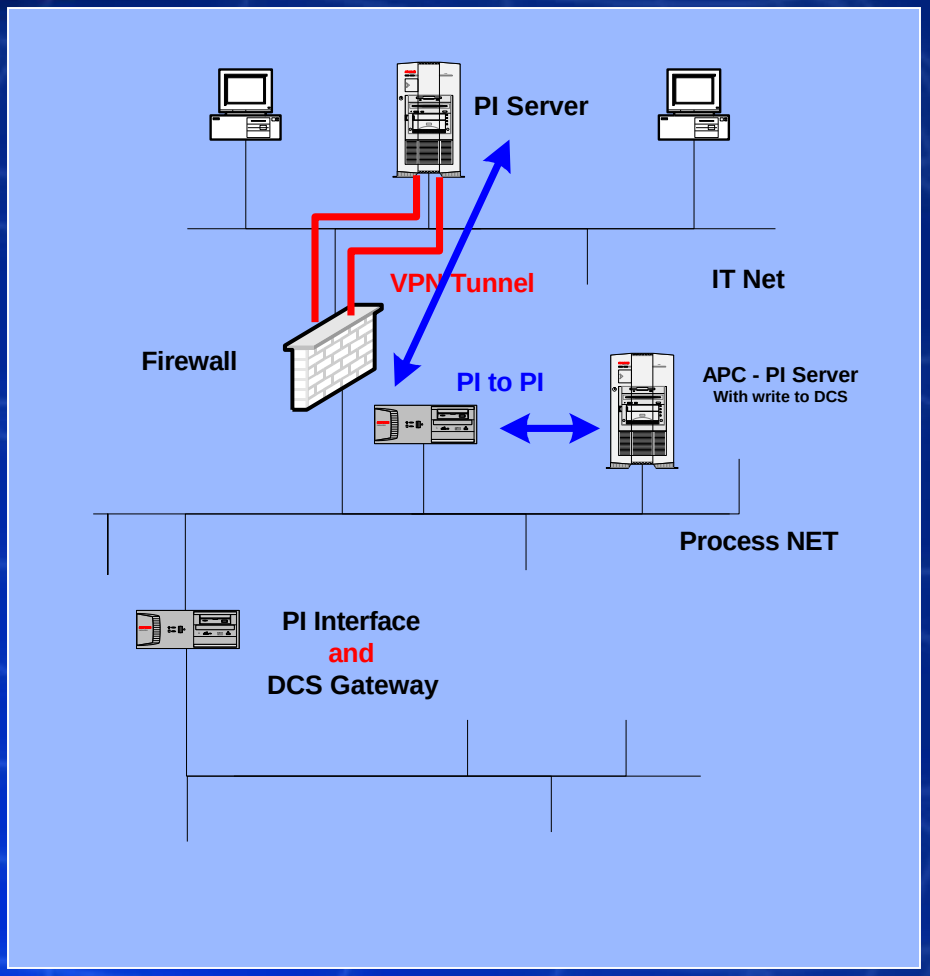
- One possibility is to put the PI server behind a Firewall.
- Access can then be given on an IP address base and PI-Port filtering.
- Disadvantages are:
  - Access list difficult to manage if there is a large number of users.
  - Problems of selectivity in DHCP environments.
  - Impossibility of Server management (Tivoli, ..) in integrated environments.
- Danger if the server has write capability.

PI Servers in a secure environment



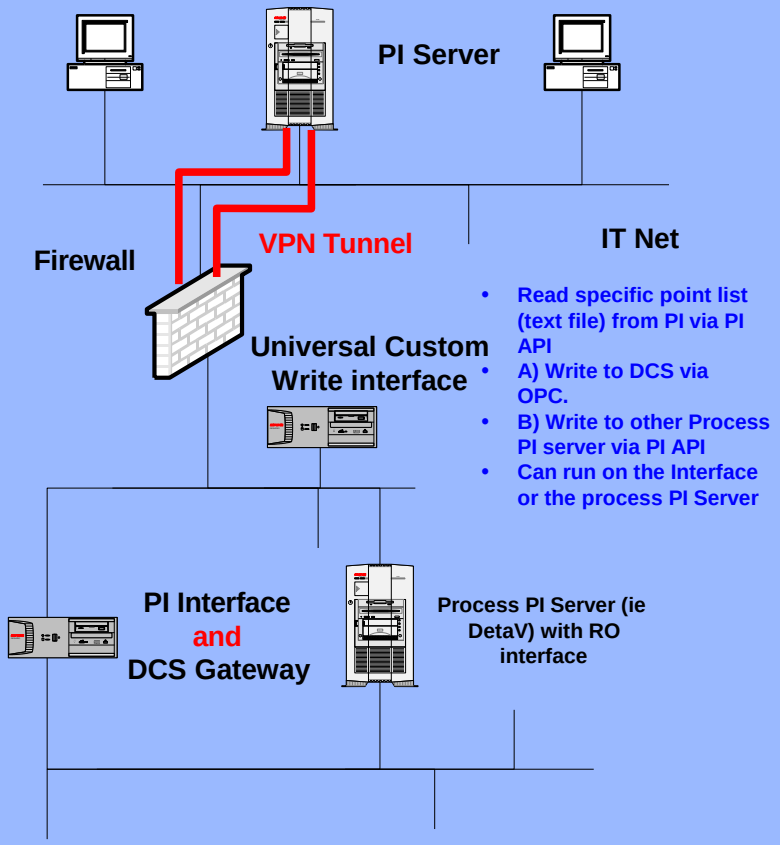
- Standard set up for read only PI Serves
- Process section is protected through Firewall and VPN tunnel (Port filtering)
- Interface runs in read-only mode.
- Access to the interface is only possible from the PI Server through the PI-Port.

PI Servers in a secure environment



- Standard set-up for systems with APC PI Servers (having R/W access).
- Data is gathered on the APC PI Server.
- Data in transferred to the “Office” PI Server through a PItoPI interface.
- The PItoPI interface runs on a separate machine.
- The “Office” PI Server has only access to the PItoPI interface (VPN + PI port). This eliminates rebound possibilities.

PI Servers in a secure environment



- Future set-up for a “office” PI Server with write access.
- A special write interface (internal development), isolated from the IT Net, reads write data from the “office” PI Server.
- Then it writes the data to DCS via OPC.
- Tag list is handled as an encrypted local configuration file which can be managed by DCS administrator (if different from PI administrator)
- This interface can also run on the PI-interface node.

Wishes for PI security

- Interfaces : improve the yes /no mechanism for writing to DCS's. (possibility to filter DCS tag reference for writing). This would eliminate the special interface described before
- Use Strong Authentication for PI administrators
- Have access to the firewall table remotely and securely as it is possible now with PI trust table
- Increase PI buffer size because PI server not directly on the DCS network

PI in an IT security context.

Questions ?