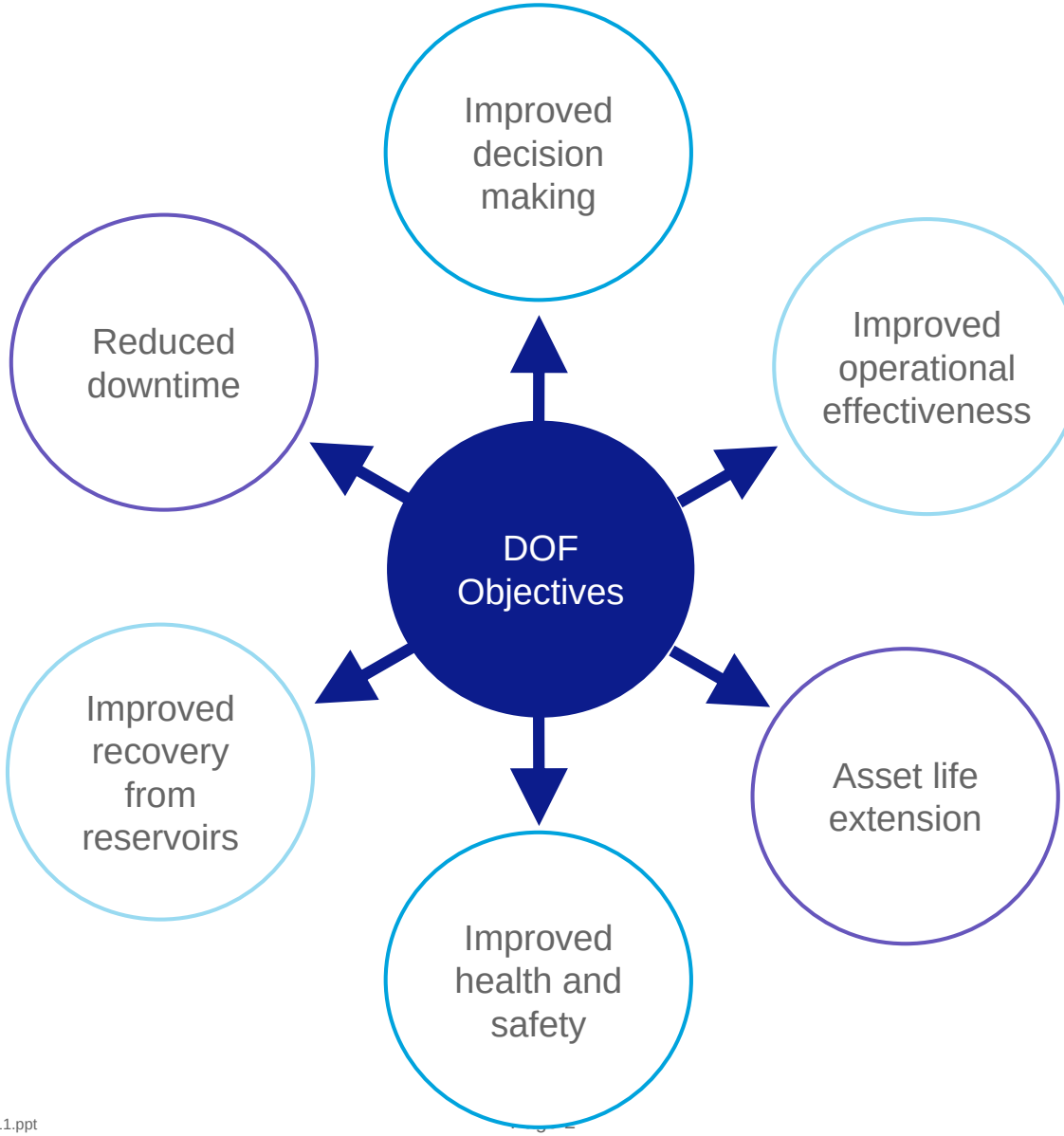
Enabling Digital Oilfields through effective cyber security

IDOC 2011

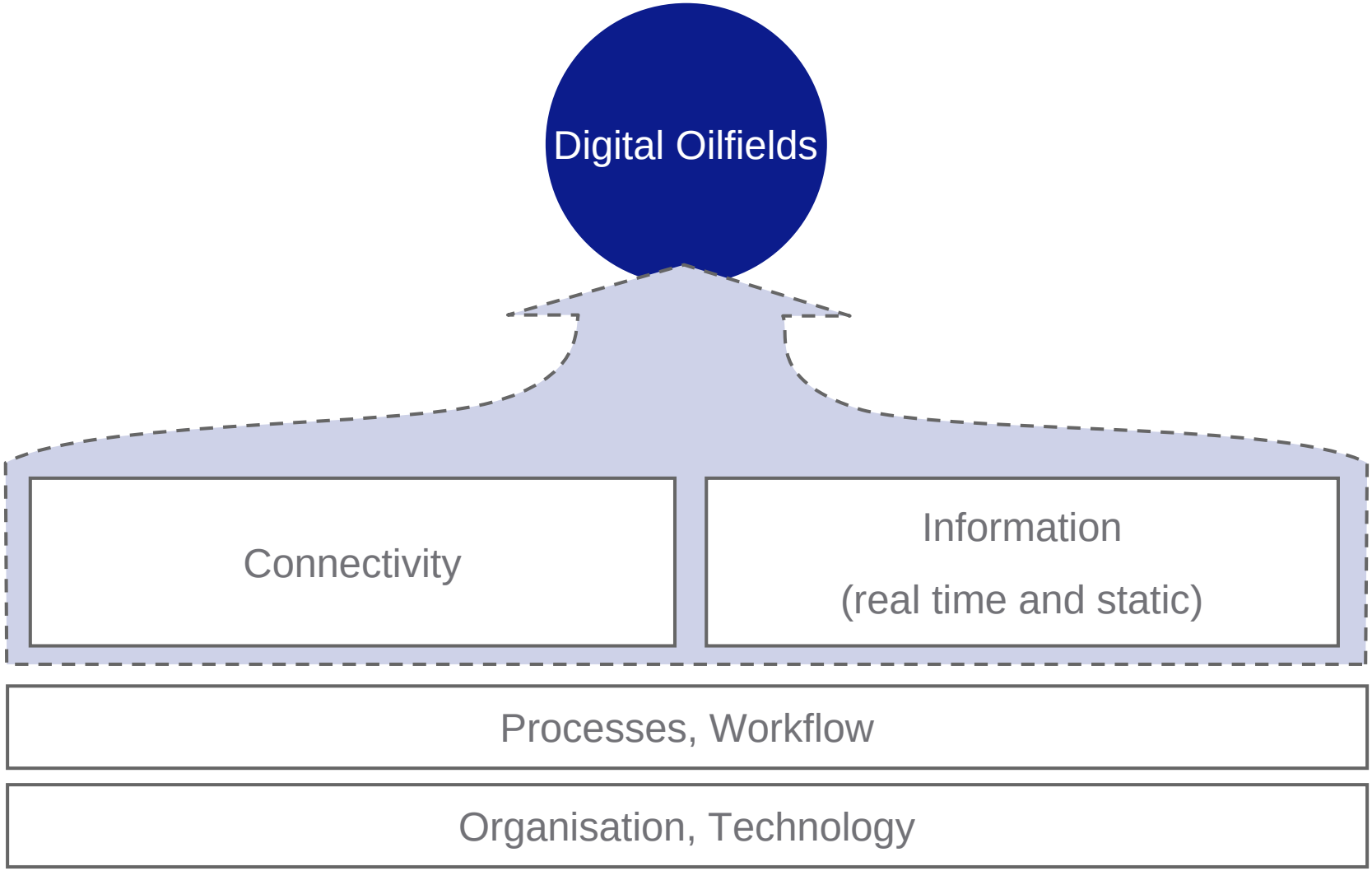
Justin Lowe

What are DOFs trying to achieve?



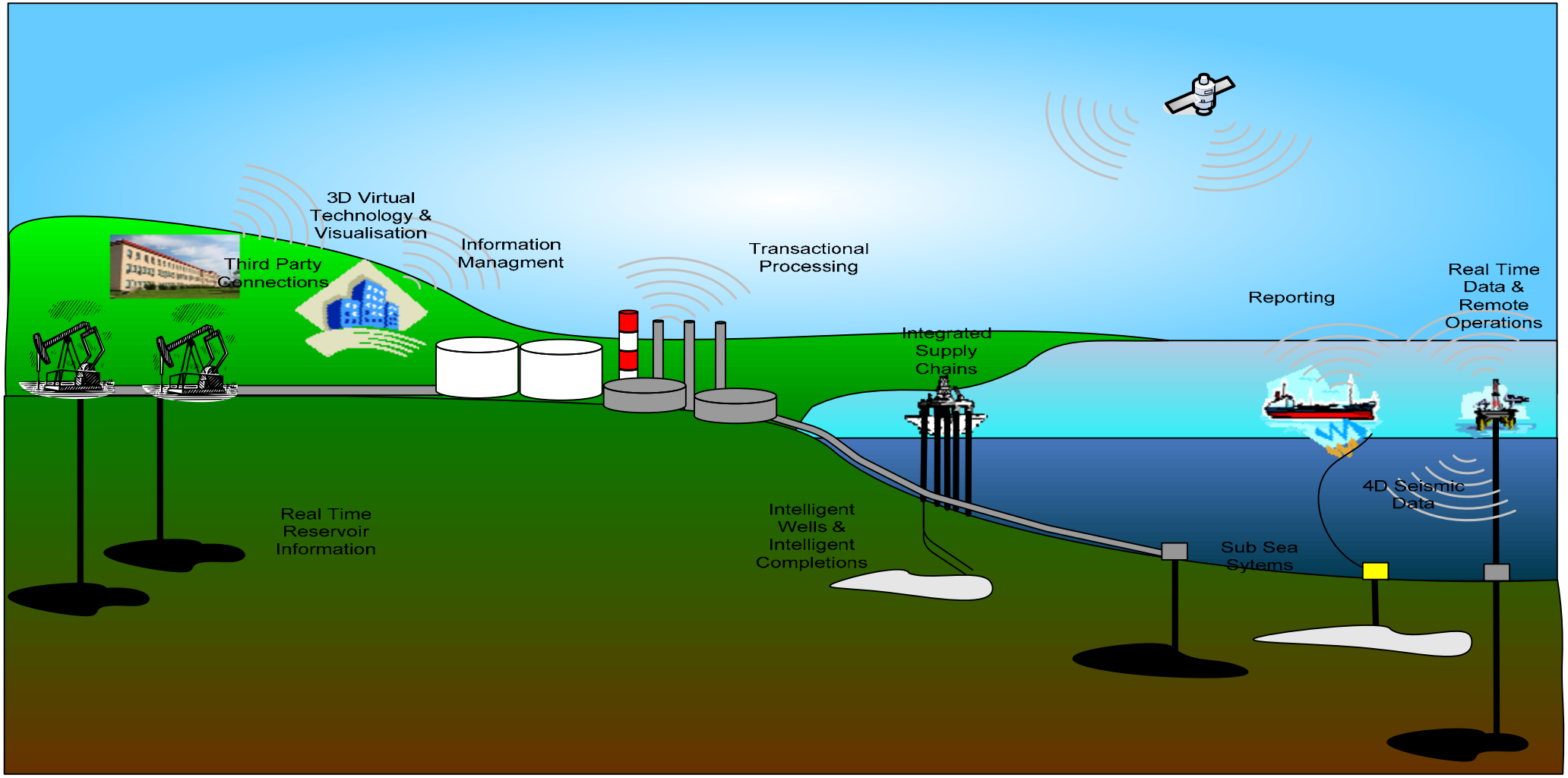
PA Consulting Group

What are the DOF enablers?



PA Consulting Group

Connectivity – a key enabler for digital oilfield

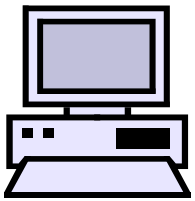


PA Consulting Group

Traditional drilling information exchange

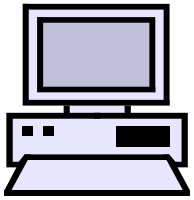
Rig Site

Drilling Control Management System (DCMS)



Mud Logging

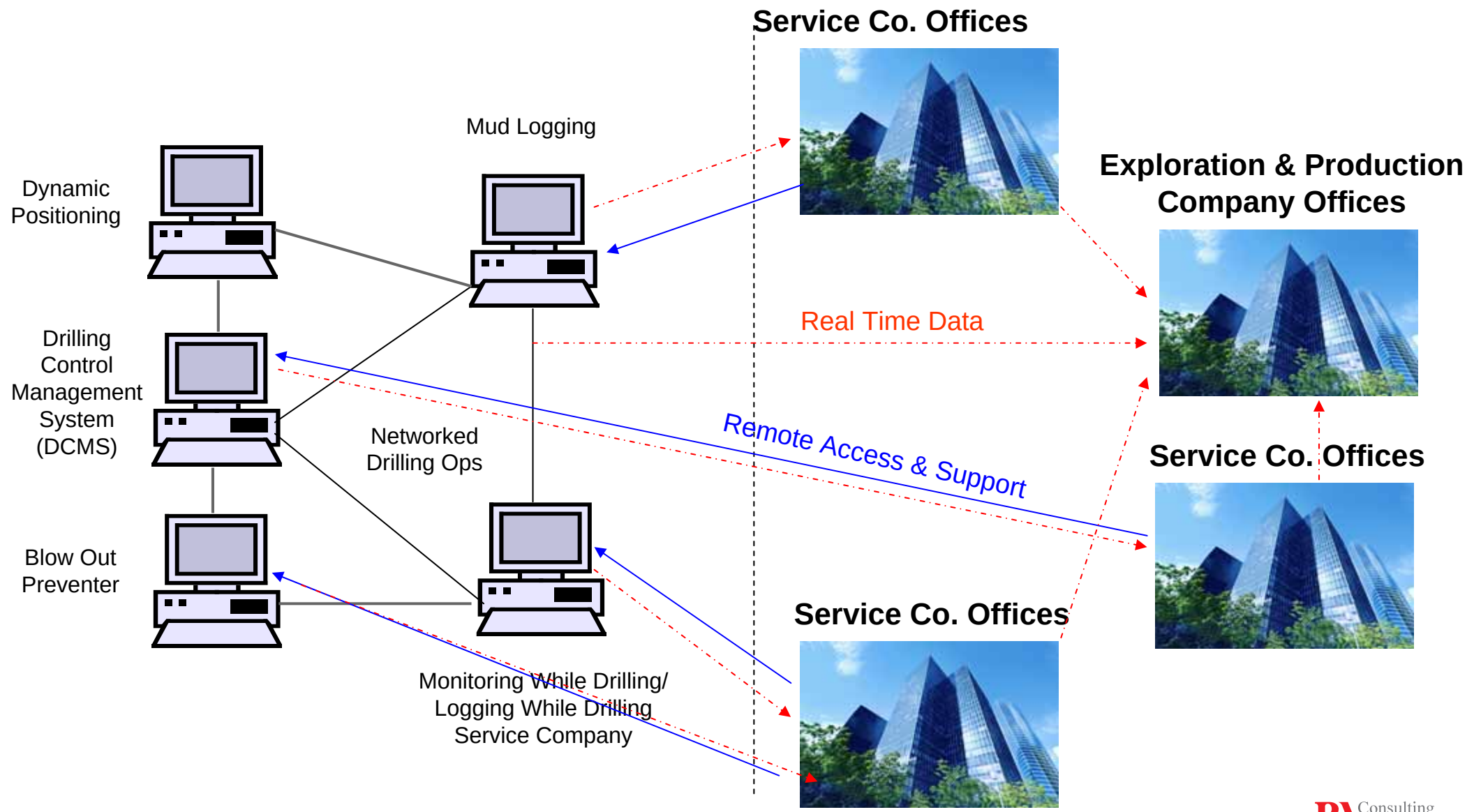
Manual Data Transfer



Monitoring While Drilling/ Logging While Drilling Service Company

Company Offices

There is an significant increase in demand for remote connectivity and real time information



PA Consulting Group

Cyber security can be a barrier to digital oilfields

- Systems are often difficult to integrate or link up
  - Insecure industrial systems which were designed to operate stand alone
  - Silos of information
  - Difficult to integrate between organisations
- IT and security not aligned to DOF
  - IT and security policies not designed for the industrial operating environment
  - IT and security personnel that don't understand the operating environment
  - Standard IT solutions don't fit – different technologies
- Some DOF systems are sensitive and need careful handling
  - Confidentiality – e.g. tight hole data
  - Integrity – e.g. fiscal metering
  - Availability – e.g. process and drilling control systems

Cyber security incidents can have a real impact in the digital oilfield

- Virus disrupts drilling rig dynamic positioning system
- Worm disables mission and safety critical drilling control system
- Poor security causes confidential drilling information to be released to wrong client
- Worm disables fiscal metering system
- Disgruntled employee disables pipeline safety monitoring system
- Virus impacts drilling system through USB stick
- Malware infection causes denial of service on VSAT communications
- Poor configuration management causes oil spill
- Worm causes loss of view and loss of control of major oil and gas plant control system

Night Dragon – targeted cyber attacks against global oil and gas and companies

The Night Dragon attack was sustained attack to designed to obtain sensitive information from organisations using commonly available tools

Attack initiation used multiple attack vectors to gain access to systems:

- SQL injection of extranet web servers
- Spear-phishing attacks of users
- Compromising corporate VPN accounts

A highly sophisticated attack

- **Disabling Internet Explorer proxy settings** to allow direct communications from infected machines to the Internet
- **Malware** used to obtain local and AD account information
- Network servers accessed and **Remote Administration Tools (RATs) installed** on the servers
- **Surveillance carried out** using RATs
- **Data stolen** from the servers.

Impacts.

- Loss of sensitive proprietary operations information
- Loss of project financing information
- Loss of information relating to field bids and operations

Stuxnet – a worm specifically targeting an industrial control systems

The *Stuxnet* worm is designed to reprogramme and disrupt specific industrial systems

***Stuxnet* is one of the most highly engineered and technically complex worms yet seen**.

- Exploits **multiple Windows vulnerabilities** (**including zero day**), as well as **sophisticated exploits within Siemens systems**
- **Spreads via multiple replication mechanisms**: USB sticks, LANs, infected PLC project files
- **Inserts malicious code in PLCs** - infected machine will automatically search for and compromise Simatic WinCC, PCS7 and STEP7 stations
- **Detection is difficult** - Stuxnet replaces the STEP7 DLL
- **Modifies its behaviour** to avoid detection by AV software
- **Establishes P2P connections** for instructions and updates
- **Uses stolen certificates** from major hardware manufacturers
- **Hides the unauthorised code**

The potential consequences to industrial control systems are severe:

– Non-targeted impacts such as slowing of system communications could be catastrophic in safety and control systems

– Targeted take-over of specific PLCs could allow malicious control of a process

– It should be noted that multiple payloads appear to be propagated, the purpose of some of these is unknown. Recent research has shown at least two payloads is specific to particular Uranium enrichment centrifuges.

It could have been much worse though.

The game has changed…

The old days

- Viruses from CDs floppy disks
- Worm infections from corporate network
- ‘Accidental’ incidents

The future challenges

- Its no longer about protecting against standard IT attacks
- There are people out there targeting oil and gas companies
- There are people out there attacking industrial control systems
- These attacks are using highly sophisticated attacks
- Zero day attacks
- Increased insider threat

Simply separating the control and business network domains is not enough – an integrated security framework is needed.

Industrial control systems are still vulnerable

- Much work has been done by ICS vendors to improve security
- However ICS still have some fundamental security vulnerabilities
  - e.g. key stuxnet vulnerabilities still not fixed – a year on
- More and more vulnerabilities are being found
  - There is now much more interest in finding security vulnerabilities in control systems
  - The good guys are looking for vulnerabilities
  - But so are the bad guys….

Cyber Threats and Vulnerabilities Against SCADA Systems

Vulnerabilities:
****
1. Solar Magnetic Storm Impact on Control Systems
2. Advantech/Broadwin Webaccess RPC Vulnerability
3. Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink
4. Gleg Agora SCADA + Exploit Pack
5. Wonderware InBatch Client Activex Buffer Overflow
6. Honeywell Scanserver Activex Control
7. ICONICS GENESIS Multiple Vulnerabilities
8. RealFlex RealWin Multiple Vulnerabilities
9. 7-Technologies IGSS ODBC Remote Stack Overflow
10. 7-Technologies IGSS Multiple Vulnerabilities
11. Samsung Data Management Server
12. Samsung Data Management Server Root Access
13. Advantech Studio ISSymbol Activex Control Buffer Overflow Vulnerabilities
14. ICONICS GENESIS32 and BizViz Activex Stack Overflow

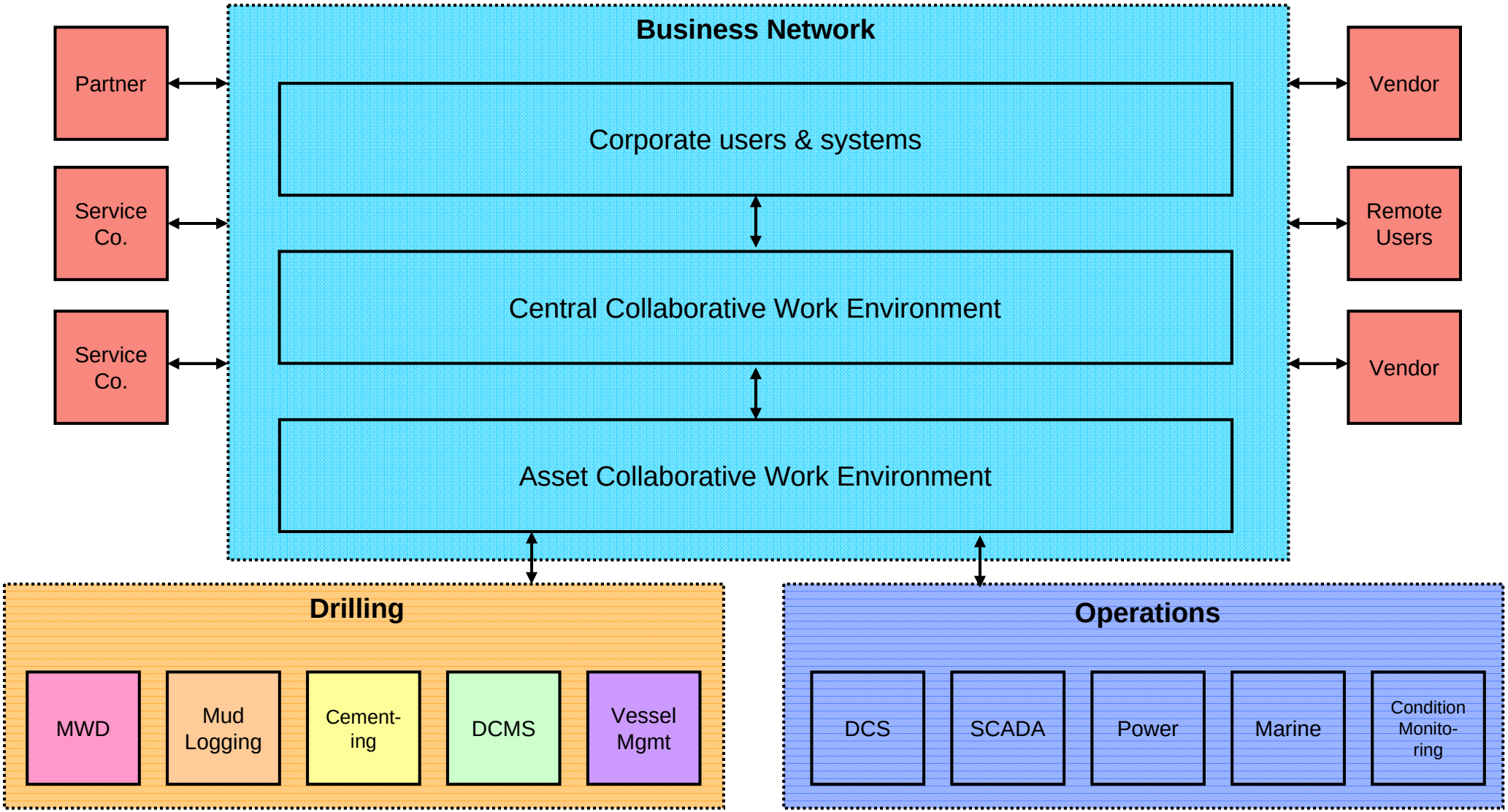
What is the impact of digital oilfields?

- DOFs are reducing operational risks in many ways
  - Reduced travel
  - Remote operations
  - Better decisions
  - Integrity monitoring
- But in some ways they are increasing operational security risks
  - Connectivity
    - IT to plant
    - Interconnectivity between vendors and suppliers
  - Increased field technology
    - Smarter devices closer to plant

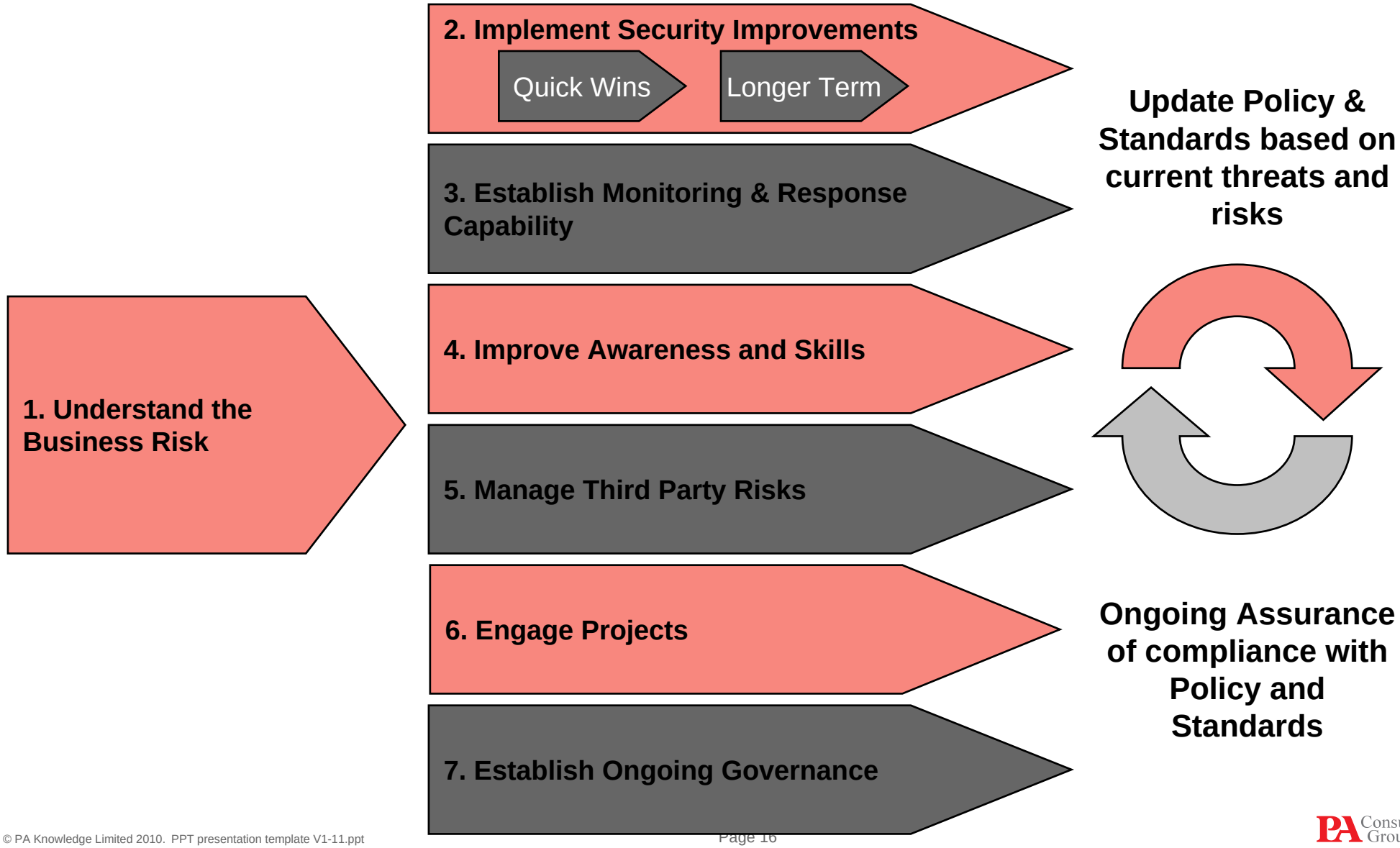
So how can DOF security issues be addressed?

- Need an end to end approach to DOF security
- Need aligned teams:
  - Engineering / Operations / IT / Telecoms / Security
- Comprehensive end to security framework and management regime
  - Understand DOF objectives
  - Understand risks
  - Systems involved and architecture
  - Data and information architecture
  - Integration architecture
  - Technical security measures
  - Ongoing support and management

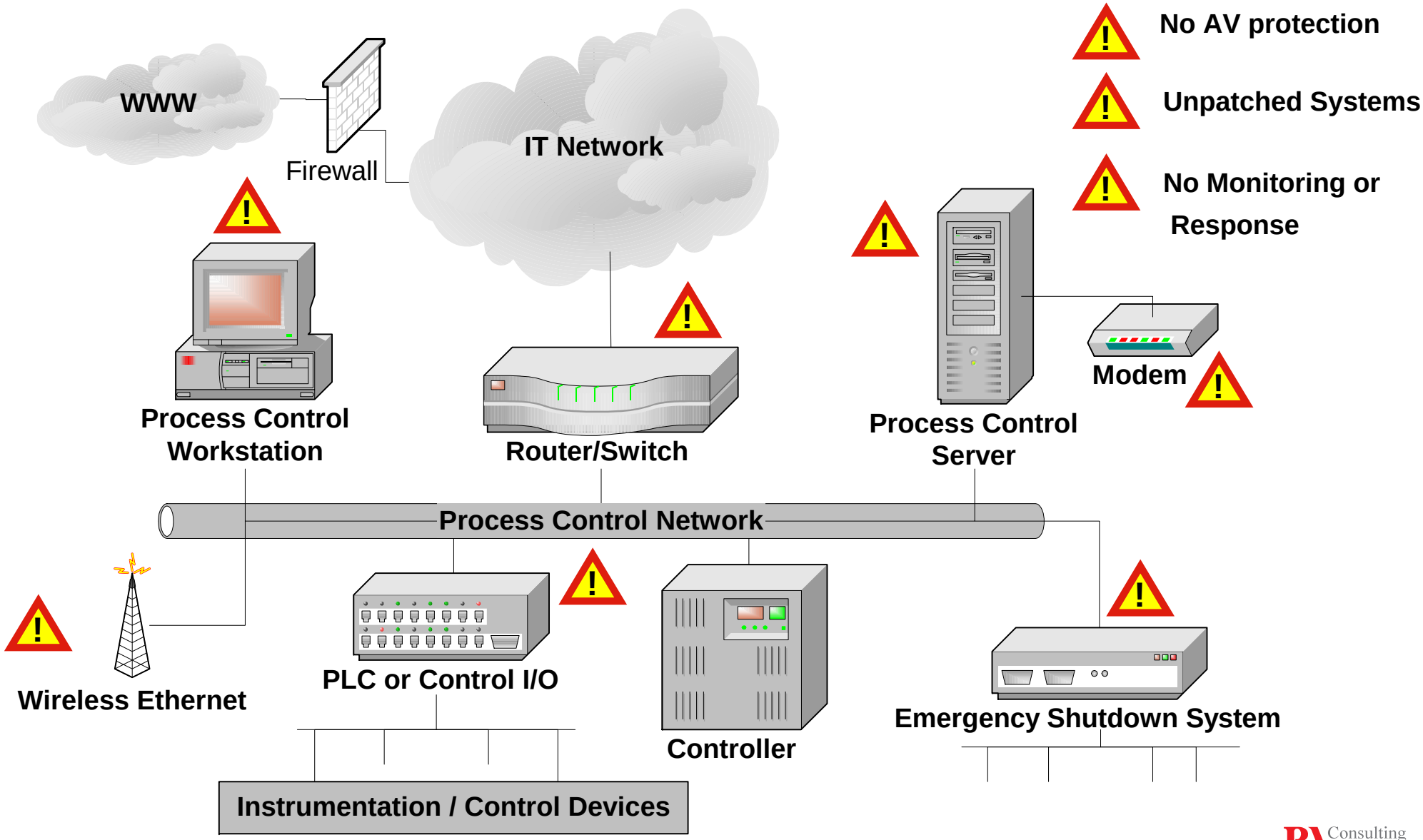
There are many different parts of the DOF that need to be addressed



Developing a security framework for DOFs

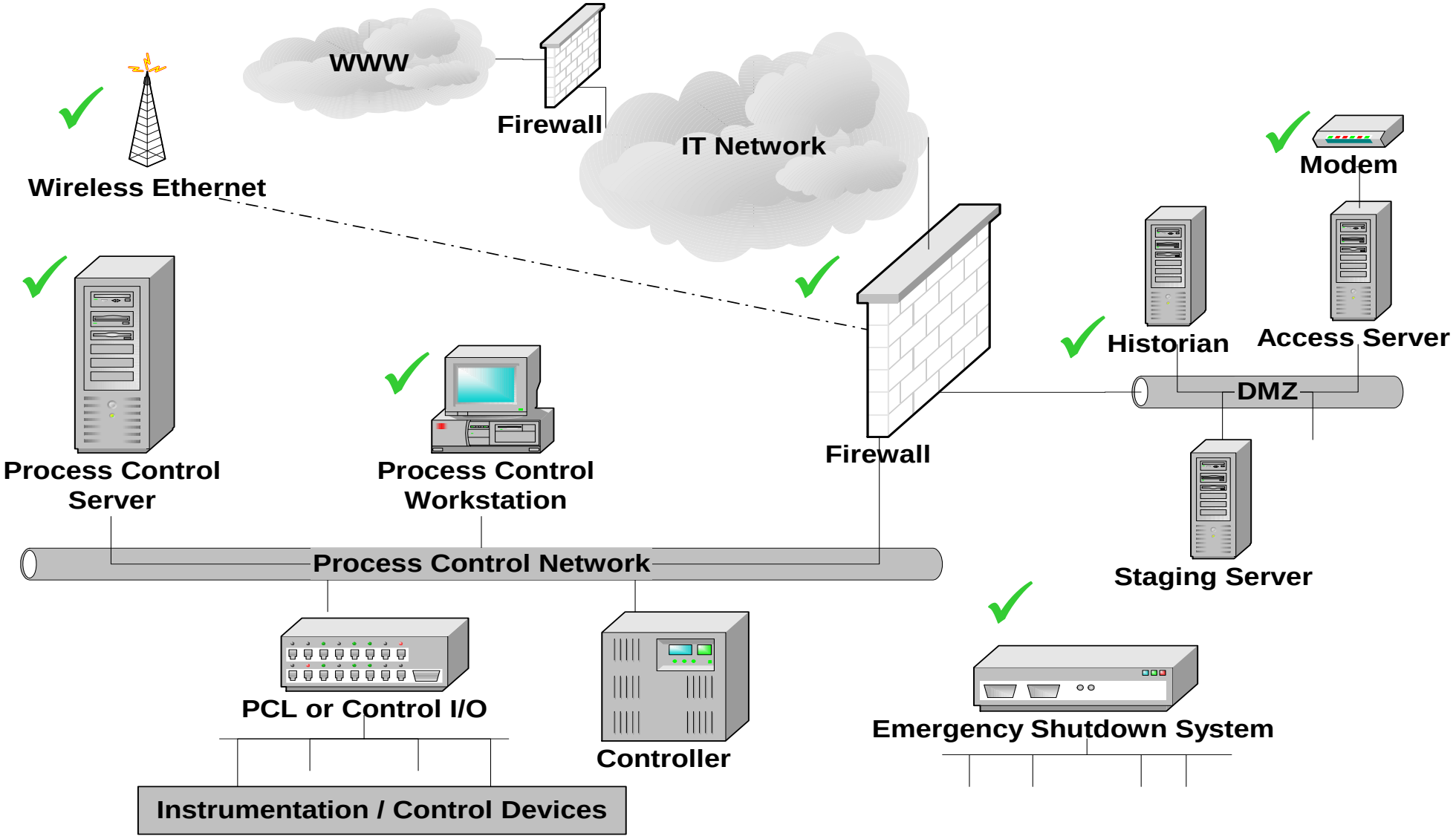


DOF control system vulnerabilities



PA Consulting Group

Security improved control system



All Nodes are Patched and AV protected

24/7 System monitoring & response capability

Enabling digital oilfields through effective cyber security - Examples

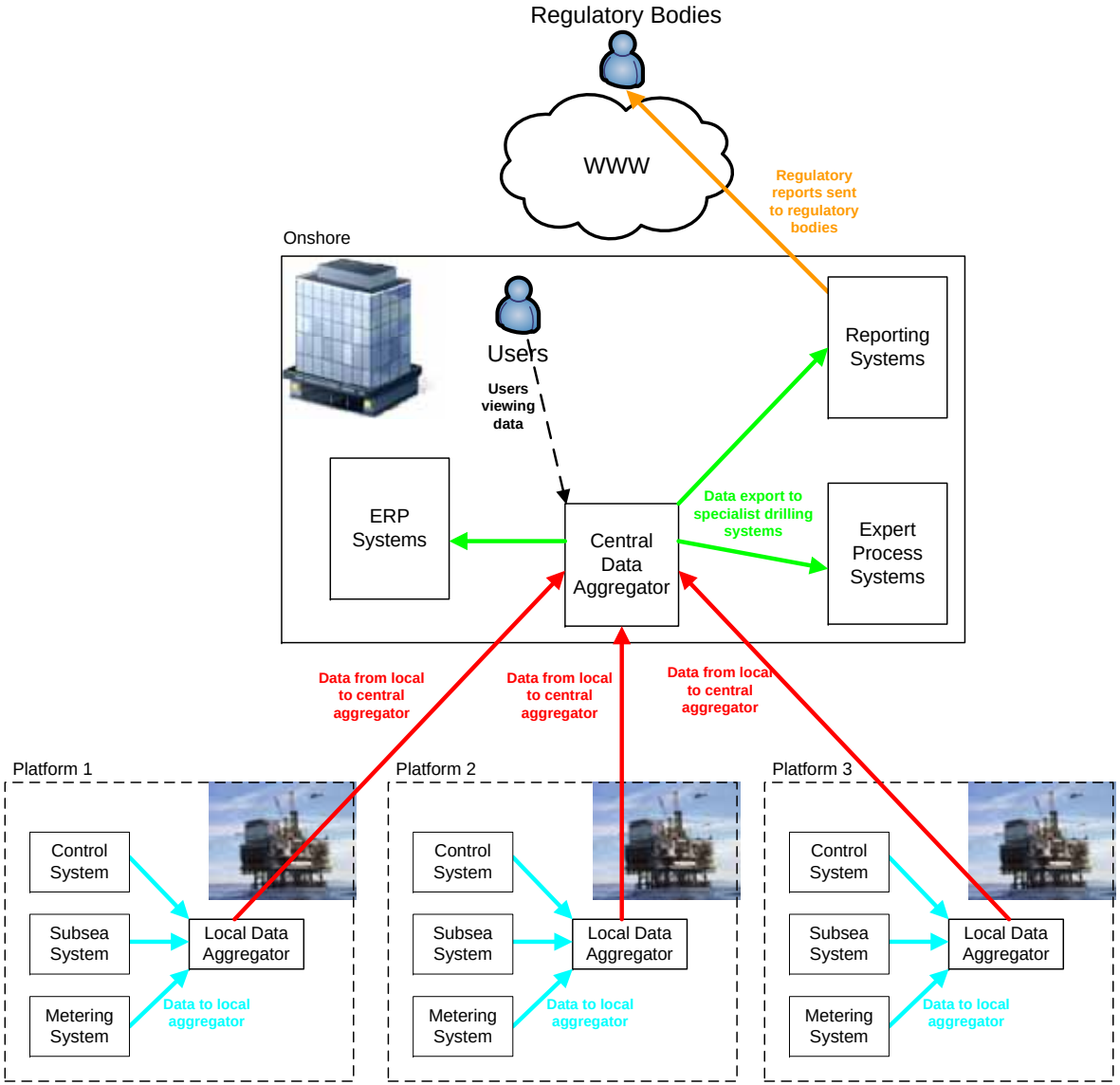
A properly designed DOF security framework can be a significant enabler for DOFs

- Access to stranded data
- Remote access
- Protection of sensitive systems
- Protection of sensitive data
- Enabling collaboration
- Enabling secure remote support

Examples

- Real time production information
- Real time drilling information
- Secure remote support
- Real time remote condition monitoring

Improving asset management and operations through process and sub-sea real-time information



Objectives

- Provide real time process information to corporate users
- Provide real time information to expert process systems

Benefits

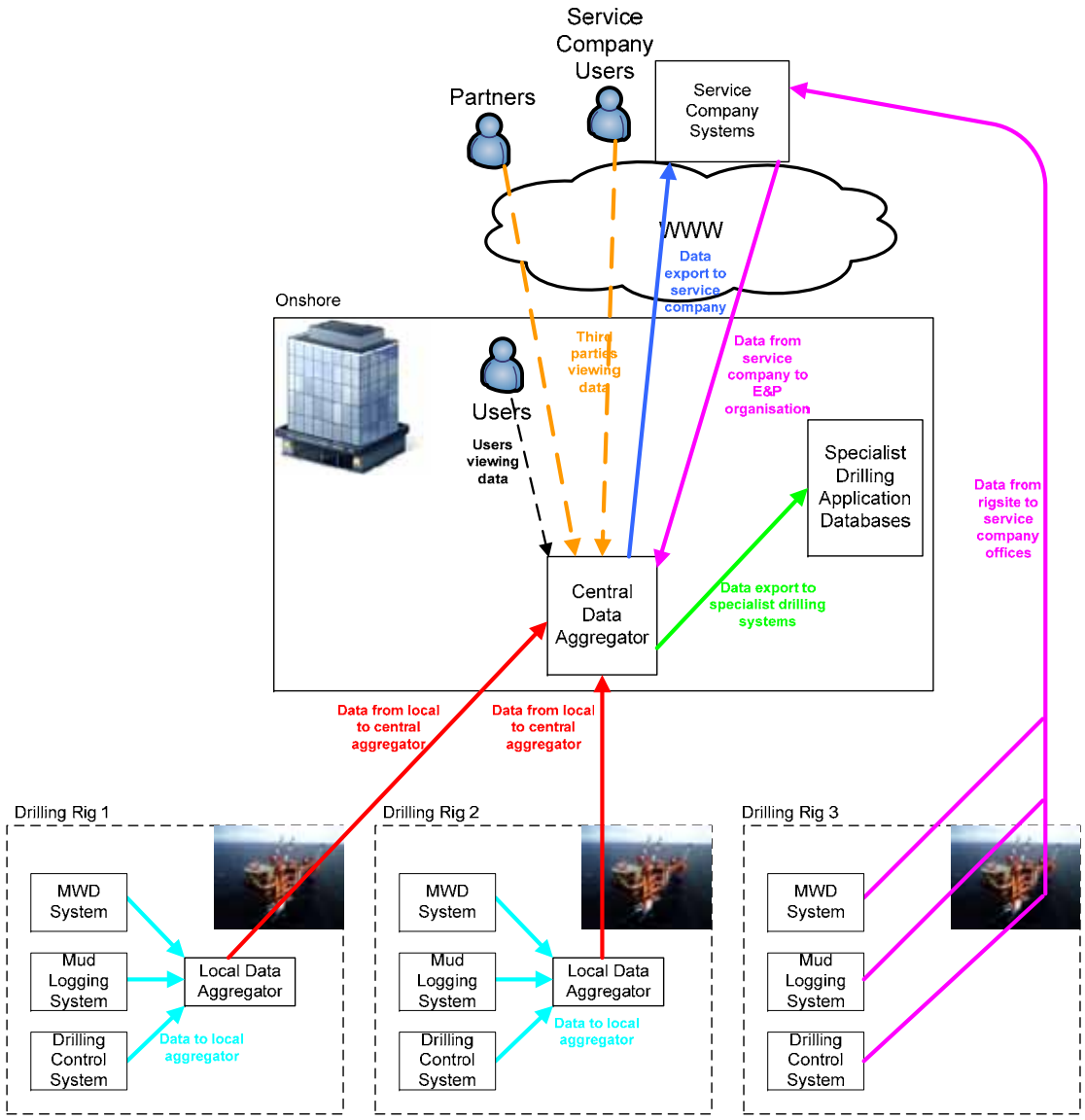
- Real time information widely available throughout the corporate environment
- Information can be shared with other systems (e.g. advanced historians, reporting tools)
- Benchmarking between assets easier
- Increased collaboration possible
- Scalable

Challenges

- Information flows to the corporate environment not the priority of the process environment
- Information ownership unclear
- Different business drivers can lead to different solutions
- Vendor systems need to meet/exceed company IT security requirements
- Connection of the corporate environment to the plant environment
- Support boundaries become blurred

PA Consulting Group

Improving drilling operations through using real-time information



Objectives

- Provide real time data from drilling related systems to company systems at the rigsite

Benefits

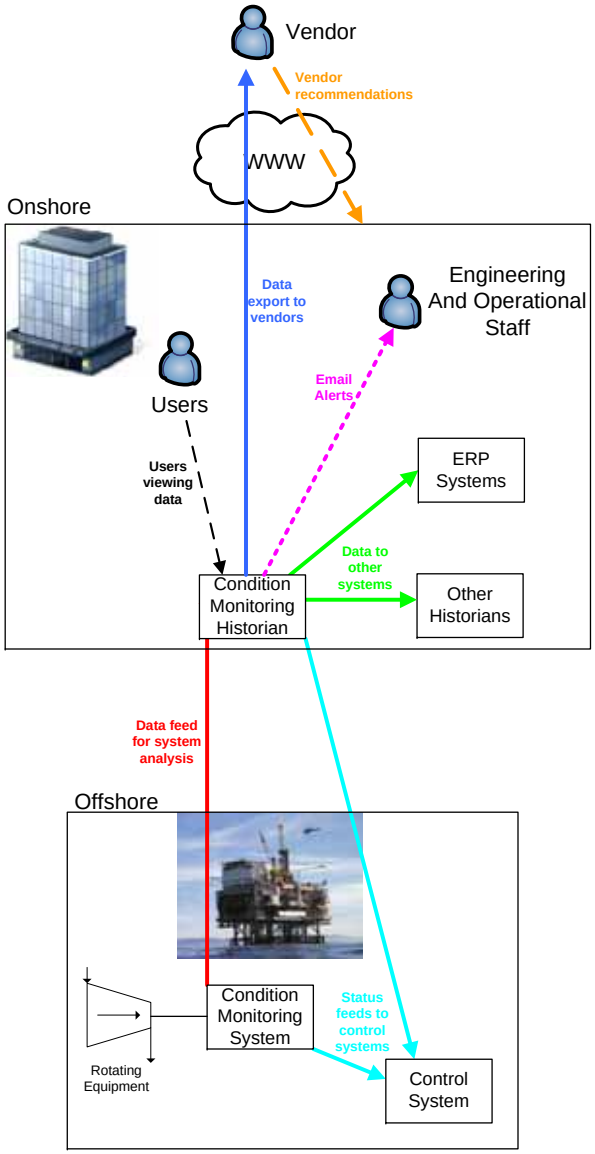
- Real time drilling information is widely available across the corporate environment
- Real time information can be provided to other drilling applications
- Ownership of the data is with company not the service company
- Scalable

Challenges

- Systems need to be resilient
- Connection of service company systems to company networks
- Standard communications (e.g. WITSML) are relatively new to the industry
- New ways of working for both company and the vendor
- Often need to work in parallel with data feeds to the service company systems
- Rigs may not be company owned

PA Consulting Group

Improving production operations – remote condition monitoring for rotating equipment on offshore platform



Objectives

- Real time condition monitoring information for rotating equipment

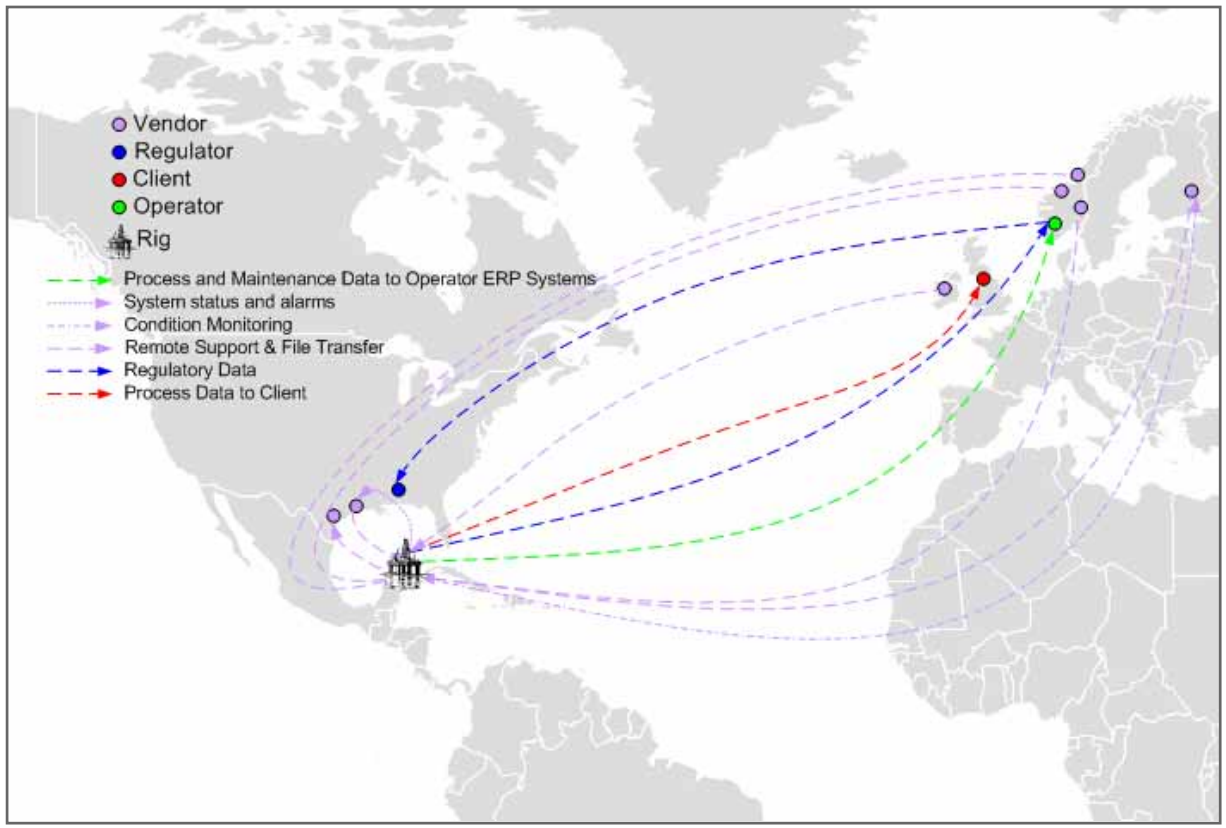
Benefits

- Decisions based on real time information not monthly reports
- Information can be shared with other systems
- Alerts can be sent to appropriate personnel using standard corporate systems (e.g. automated emails)

Challenges

- Not all vendor solutions capable of supporting this type of solution
- Vendor systems need to meet/exceed company IT security requirements
- Connection of the corporate environment to the plant environment
- Support boundaries become blurred

Smarter asset management for deep water drilling rigs through remote monitoring, support and reporting



Objectives

- Allow third parties and other support staff to:
  - Remote support
  - Remote expert analysis and advice
- Transfer of regulatory data
- Transfer of process and maintenance data

Benefits

- Increased uptime. Decreased issue resolution time
- Support staff do not have to be based at the asset
- Support staff can be shared by assets
- Removal of staff from hazardous locations (e.g. offshore)

Challenges

- Systems need to be resilient and secure
- Connection of third party networks to company networks
- New way of working for both company and the vendor, high level of trust
- Procedures need to be changed to meet the new ways of working

PA Consulting Group

www.paconsulting.com