

The Industrial Data Centre

Delivering secure visibility over industrial IT infrastructure

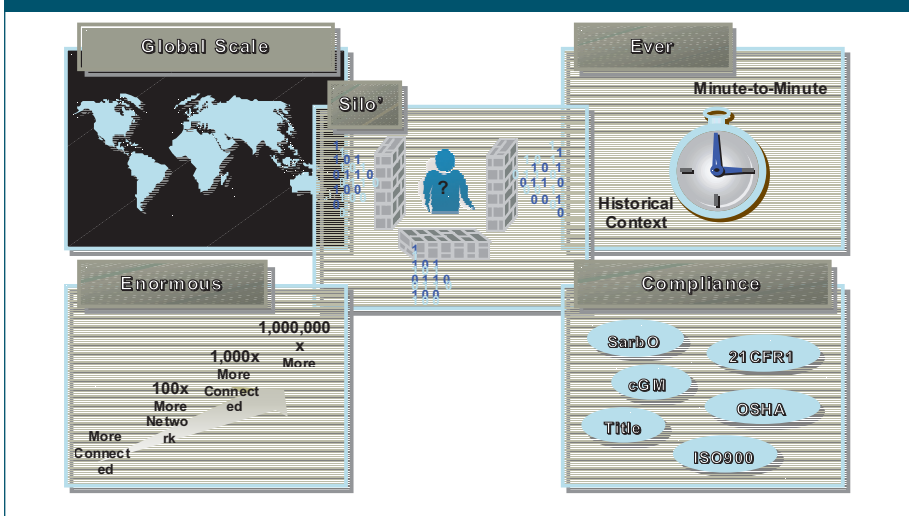
The data centre is increasingly the life support system of any enterprise. It allows collaboration, interaction and creative relationships to flourish between partners, employees and customers. However, many data centres fall short of providing users with optimal benefits. This is for a number of reasons, not least of which is the historical development of disparate infrastructures to support applications that operate in standalone environments.

For manufacturing companies, the data centre is increasingly linked to the process control network that delivers business critical information from industrial installations. Being able to make better business decisions more effectively requires information to be available at the operational, divisional and enterprise levels of the organization. And the speed with which business operates means that data has to be available to support decision making in a much shorter timeframe

However, whilst the transparency of operational information is vital, the configuration of the process control network (PCN) with the corporate network is a demanding task. In particular, connecting the PCN to the business network with the maximum levels of security represents a major challenge. In short, the balance between visibility of data and security of the network is critical.

To address this challenge Cisco and OSIsoft have developed the Industrial Data Centre (IDC) that is designed to optimise the balance between data visibility and security in connecting the PCN to the business data centre.

Figure 1: Business Challenges



Business Challenges Facing Oil and Gas Companies

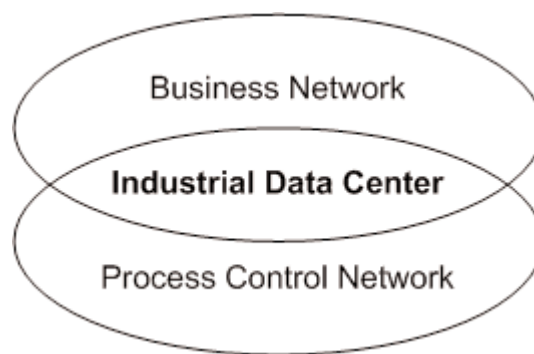
There are a number of specific business challenges that oil and gas companies need to confront:

- Organisation-wide security
- Maximising operational efficiency
- Acquiring, distributing, reporting and managing data in real time
- Remote management, maintenance and scheduling of offshore platforms
- Global scale
- Integrating the requirements of all business units
- Business continuity and transparency through the creation of simplified and secure integrated data centres
- Responding to the regulatory burden imposed in the post Sarbanes Oxley environment

Simplifying real time performance management

The process control networks that provide access to operational data exist in a complex environment. Multiple interfaces and connections need to be managed into one, streamlined system that both maximises the visibility of information where and when it is needed and simultaneously provides high levels of security.

Figure 2: Industrial Data Centre Concept



What is the Industrial Data Centre?

Industry estimates suggest that as much as 70 per cent of IT budgets are spent on simply maintaining existing application environments. In response to this, the IDC has been developed to provide corporates with an infrastructure that allows them to improve operational efficiency, optimise utilisation of data centre resources and release funds for innovative new IT projects that generate revenue.

The IDC provides a platform for the consolidation of data centre, storage and server requirements as well as virtualisation of computing and storage allowing for more efficient use of existing resources. At the heart of the IDC is an Intelligent Information Network (IIN) infrastructure that provides secure user access to data centre services,

as well as the flexible and scalable deployment of components as required, including applications, servers, mainframe computers, appliances and storage.

The IDC is designed to support the need for consolidation and at the same time provide the security and reliability to ensure that business continuity is not impaired. Using the design principles contained in the IIN architecture, the Industrial Data Centre has been specifically evolved to provide a holistic view across both Networks of real-time data and secure and reliable connection between an industrial process control network and the business network that allows for greater oversight of critical data at the corporate centre.

Connecting these 'islands' of information to a corporate centre is increasingly vital for oil and gas businesses. However, the security of these connections cannot be overemphasised. Any breach in that security could have disastrous consequences. And the number of attacks on corporate data centres is increasing all the time. One estimate suggests that there are nine million attacks on corporate data centres from hackers and other malicious operators every day.

Operational data is not only needed to improve performance, it is increasingly part of a business's governance obligations. Since the implementation of Sarbanes Oxley and related regulatory initiatives, the collection and storage of information has taken on a new urgency for business. So, in addition to business imperatives driving the need for operational visibility, regulatory pressures are also now increasing that pressure.

Achieving Maximum Visibility with Maximum Security

Threats to the process control networks come from a number of directions and in a number of forms. Malicious attacks, the deliberate or inadvertent introduction of worms or viruses are but two of the most obvious. Other threats include incorrect programming of a PCN device, or the introduction of unauthorised devices.

The integration of business and industrial installations mean that the closed systems of the PCN which have not previously had to be concerned with security are now open to the same vulnerabilities that have the potential to damage all corporate networks which are not adequately protected. These threats include:

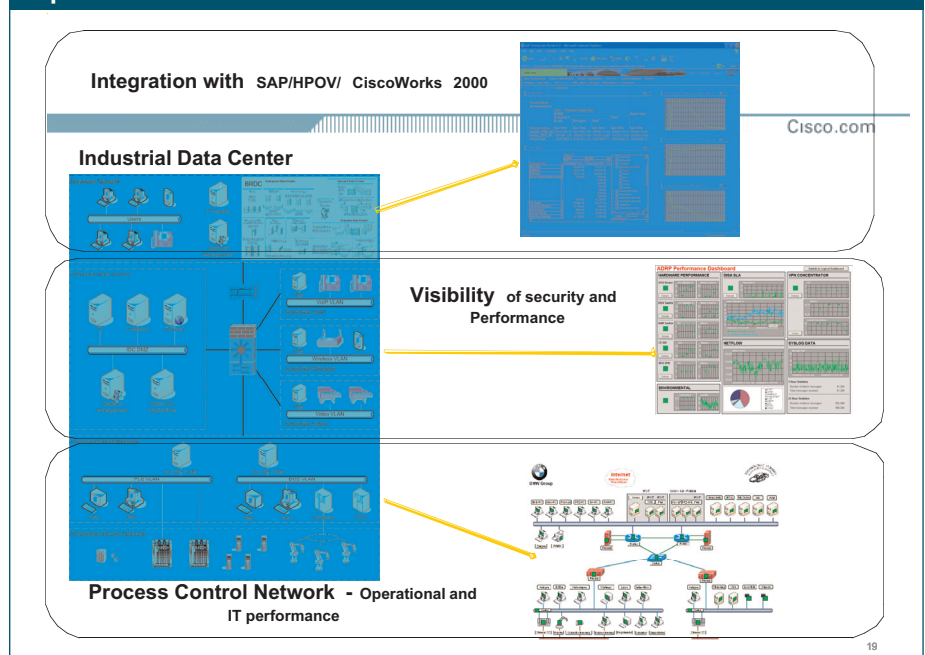
- Worms and viruses
- Unauthorised and unknown access
- Malicious attacks

In addition, PCNs have specific challenges that further complicate their integration into the business network. Because they have always operated as closed systems, legacy protocols used on the PCN have no inherent security. For oil and gas companies this problem is compounded by the existence of multiple networks in globally dispersed sites

In response to this security challenge, the IDC is a specifically designed set of software, hardware and best practices that allow safe and manageable connections between the PCN and the business network. The heart of the IDC is a dedicated LAN, comprising PI Server or other servers allowing access to the PCN, called the Demilitarised Zone (DMZ). The DMZ is a region controlled by enterprise IT where standard IT practices such as anti-virus and patch management can be applied without the risk of interfering with operational systems. The IDC simplifies security management by ensuring that all operational data that flows between the PCN and the Business Network must pass through the IDC PI Server.

Figure 3: Figure 3: IDC Reference Architecture

The IDC DMZ contains a PI and IT Monitor server which connects data from the PCN to the business network. PI interface nodes on the PCN collect operational data and store it in the IDC PI server.



The Process Control Network

Operational information is collected from PCN systems by PI interface nodes including:

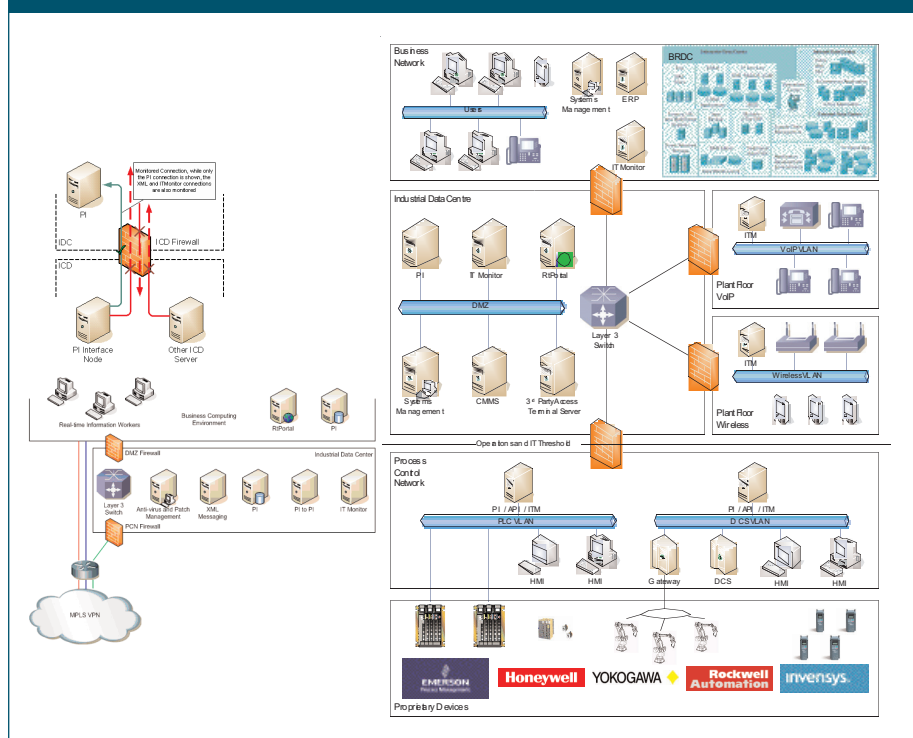
- DCS – eg Honeywell, Yokogawa, ABB, Emerson, Foxboro
- PLC eg Rockwell, GE, Modicon, Modbus, Modbus+
- SCADA eg Siemens, GE, Wonderware
- Open Standards eg OPC, ODBC, OLEDB

By using the security that the IDC PI server offers, operational data can be collected and devices within the process control network monitored in a completely secure way.

In this way the business network's users and applications have secure and real time visibility of operational data without compromising the performance of any aspect of a Converged Ethernet Network.

In addition to business users, third parties such as suppliers or partners may need to access information from the PCN. By placing a VPN Gateway like an SSL Gateway based on the VPN3K within the IDC DMZ, third parties can have secure remote access over the Internet using corporate VPN. Vendors of specific industrial equipment may also need to access devices attached to the PCN in order to monitor performance. Securing these systems – which commonly use dial up access –has in the past been problematic. The IDC creates a more manageable approach to secure third-party access by introducing an application gateway that controls all access to the PCN, thus eliminating the risk of 'infection' from a third party's computer. When a third party connects – either via the Internet or connected intranet - an audit trail of connections via the application gateway is produced which further enhances security.

Figure 4: Integrated IDC



IT Monitor – Real-Time Infrastructure Monitoring

The integration of real-time data into the enterprise network delivers key benefits to performance management and planning, but at the same time the reliability of the data

flowing from industrial installations becomes increasingly critical. Any downtime in availability or poor performance can have serious implications, creating missed opportunities and loss of revenue. As part of the IDC Solution, IT Monitor enables complete visibility of the end-to-end infrastructure from the enterprise centre to the factory floor, ensuring that the flow of information around the entire infrastructure, the availability and performance of applications and services can all be monitored to ensure optimal operational efficiency.

IDC: Ready and Secure for New Technology

Extending the use of new technologies is of course an attractive option for all businesses, allowing them to increase both productivity and efficiency. The use of Voice over IP (VoIP) offers many such advantages, as does the use of wireless technology to make real time point of activity computing possible. Video over IP means that industrial installations can be kept under surveillance by any appropriately authorised user in any location. However, their adoption in industrial contexts has often been hampered by concerns about security.

The IDC suite of technologies and best practices is specifically designed to address those security concerns by allowing advanced technologies to be introduced securely. So, for example, mobile users can access information from the IDC without compromising the security of the installation.

Conclusion

Energy businesses operate in a climate that continually generates unique challenges. The scale, extent and globally dispersed nature of their installations exceed those of most other industry sectors. However in common with other sectors, energy businesses face similarly critical issues of information availability, regulatory pressures and the need to ensure that productivity is maximised in the most efficient way possible. The Industrial Data Centre is designed to help them address those challenges and meet their business goals.

Corporate Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (6387)
 Fax: 408 526-4100

European Headquarters
 Cisco Systems Europe
 11, Rue Camille Desmoulins
 92782 Issy-les-Moulineaux
 Cedex 9
 France
www.cisco.com
 Tel: 33 1 58 04 60 00
 Fax: 33 1 58 04 61 00

Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-7660
 Fax: 408 527-0883

Asia Pacific Headquarters
 Cisco Systems Australia, Pty., Ltd
 Level 9, 80 Pacific Highway
 P.O. Box 469
 North Sydney
 NSW 2060 Australia
www.cisco.com
 Tel: +61 2 8448 7100
 Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
 Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
 The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
 Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005, Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company (0403R)