
# SPE 112279

# IT Security and Architecture for Integrated Operations: Examples from Deliveries to Ormen Lange and Draugen

Marius F. Aarset and Olav Mo, ABB A/S



This paper was prepared for presentation at the 2008 SPE Intelligent Energy Conference and Exhibition held in Amsterdam, The Netherlands, 25–27 February 2008.



## Abstract

The introduction of Integrated Operations causes a demand for integrating process control systems with office systems. A secure and reliable connection between these systems enables considerable cost savings related to:

- Process Optimization
- Maintenance
- Collaboration
- Remote support

Shell operates two oil fields on the Norwegian Continental Shelf; Draugen and Ormen Lange. Draugen is an established oil-field having been in operation since 1993. Ormen Lange is a new gas-field based on subsea installations remotely operated from an onshore process plant.
In implementation of a technological basis for IT Architecture and Security supporting Integrated Operations, certain products and services are essential for achieving the ambitious expectations. The technological basis may be separated in three fundamental areas:

- Establishment of plant Security Policies, a management tool for establishing plant security.
- Design of a Plant Network, which will facilitate communication between the office and process control networks, and communication with other subsystem networks.
- Implementation of Remote Services, a solution for a secure connection between the Plant Network and the office network.

IT security is a major issue when integrating office systems with process control systems. Corporate, national and international standards must be adhered to, and good technical and procedural solutions must be developed. The technological nature of the underlying process control systems must be addressed when an architecture for integration is created.

Both Draugen and Ormen Lange have recently been designed to facilitate Integrated Operations according to Shell requirements, integrating information from various subsystems and making real-time data available in Shell's newly developed collaboration centre in Kristiansund, Norway. The collaboration centre will provide operational support to Draugen and Ormen Lange, and is part of a collaboration network in Shell Europe. Remote services are established enabling remote access towards vendor support centers, as the ABB remote operations rooms for Ormen Lang and Draugen.

## Introduction

In the year 2000 it was stated by a Norwegian governmental committee (Norwegian Ministry of Justice, 2000) that the division between open office and enclosed process control networks was a characteristic of the IT infrastructure of the Norwegian oil and gas industry. This division was said to increase robustness and reduced the vulnerability of the process control systems. It was also stated that there were very few functional dependencies across this boundary. This reality is being challenged with the introduction of *Integrated Operations*;

In recent years the implementation of Integrated Operations is seen as the third efficiency leap on the Norwegian Continental Shelf. Integrated Operations is all about improving operation and maintenance of oil and gas installations through employing

new technical solutions in combination with better work processes. Sharing of data and information through integration of process control systems is a corner stone in the strive towards implementation of Integrated Operations.

Process control networks will no longer be fully separated from other networks, and as long as networks are not physically isolated there will always be a possibility that unwanted traffic is let through the connection point between the networks. The design of this connection to the process control system and other subsystems, and the procedures for operation of the inter-connected systems, will decide how secure and reliable this integration will be.

## The Challenge and Solution of Integration

### Integration Demands

The strongest demands for integrating process control systems with office systems come from the introduction of Integrated Operations. Integrated operations include work processes and activities like:

- Process Optimization
- Maintenance
- Collaboration
- Remote support

### Integration Challenges

IT security is clearly a major issue when integrating office systems with process control systems. Current and emerging national and international standards as well as corporate standards must be adhered to, and good technical and procedural solutions must be developed.

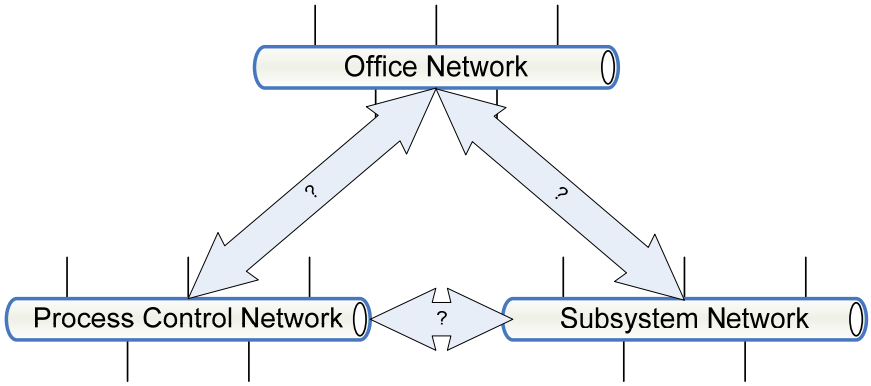


**Figure 1 Integration challenges**

Another issue is of course the integration itself. There is no prevailing standard for data communication between the office and the process control systems that is embraced by both camps. The de-facto standard for integration between process control systems is OPC. However, the most widely adapted OPC implementation is using a communication protocol that is difficult to pass between networks. Also, the OPC standard does not address how data should be organized.

Integration is not only about communication. Other important issues must also be addressed:

- Formatting and organizing
- Data quality
- Data integrity
- Reliability
- Availability

If not done properly, connecting the process control system to the office network to enable Integrated Operations may cost more in security incidents than you will ever gain on introducing Integrated Operations in the first place.

### Technical Solution

Individual solutions to the integration challenge are needed since no process control network and no office network are equal. However, the principles of connecting the office and process control networks can be based on the same best practices and guidelines.

The solution to the integration challenge considered in this paper focuses on three main elements to achieve successful integration:

1. Establishing a Security Policy
2. Introducing a Plant Network
3. Implementing Remote Services

***Security Policy***

The plant security level should be well defined throughout the lifecycle of a plant. Security Policy is the tool to define the plant security level, where it must clearly state what is allowed to do and what is not. Security can in many ways be seen as the HSE (Health, Safety and Environment) part of computing. Without a security policy in place it is up to each individual to define what an acceptable risk is. It is important to put security awareness on the agenda, and when the security policy is in place it must be communicated to all personnel working in the plant.

The security policy must cover every aspect of the security on different levels:

- Physical security
- Computer security
- User security

A security policy should be based on an analysis and assessment of the functional needs and security objectives of the organization, current and planned network structures and information and control flows, risks in terms of probability of different types of attack and potential consequences, and available technical security solutions.

The security policy must be used as basis for every security measure taken for the plant. The security measures are in turn tools to implement the policy.

It is important to create the security policy in the early phases of a project to make every project member aware of the security issues.

The security policy should be developed as a joint effort performed by all the involved parties in cooperation:

- Plant operator
- Engineering contractor
- Process control system supplier
- Subsystem suppliers

The plant operator and the engineering contractor in cooperation will be responsible for the project phase. The plant operator will be responsible for the operational phase. The control system vendor is in general responsible for the control system delivery and other suppliers are responsible for their deliveries

***Plant Network***

The Plant Network is introduced in order to facilitate remote communication to the process control system through a Remote Services solution and communication between the process control system and subsystems connected to the Plant Network. See Figure 2 for an illustration of the Plant Network.

There are three classes of networks that are connected to the Plant Network:

- Office network
- Process control network
- Subsystem network

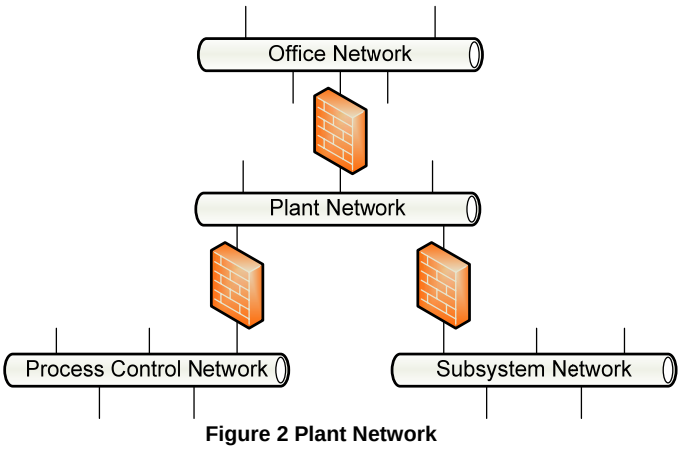


**Figure 2 Plant Network**

The principles for the Plant Network are:

- Firewalls are used for all networks connections to the Plant Network to provide sufficient segregation
- All connections through the firewalls are terminated on the Plant Network
- Security patches are installed on all computers on the Plant Network as soon as they are available
- The operating system on all computers on the Plant Network is hardened meaning that all services not specifically used are removed.

Developing the guidelines and specifications for connecting these networks with each other is not a trivial task since the process control system and subsystems might be old, poorly documented and complex. Even if they are not, connecting this side will typically be more challenging than connecting the office side.

***Remote Services***

The Remote Services solution is used to create a secure connection between the Plant Network and the office network. Through this solution users on the office network are able to connect to computers and systems on the Plant Network, the process control network and other subsystem networks.

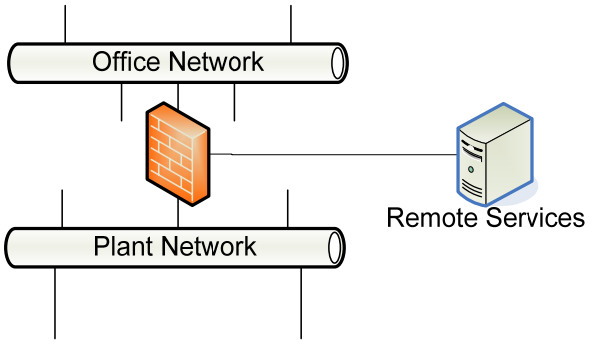


**Figure 3 Remote Services from the Plant Network**

Large oil companies often have a solution for connecting a Plant Network to the Office Network. Through this solution services required by computers on the Plant Network as well as computers in the process control system and subsystems can be made available. If the company does not have a Remote Services solution a solution design must be established.

The Remote Services solution must provide or support the following security related services:

- Authentication and access control
- Anti-virus update
- Operating system patch distribution

And the following remote operation and maintenance services:

- Interactive remote access
- File transfer

The Remote Services solution may utilize functionality already available in the office network and may be shared between multiple Plant Networks at different sites.

***Individual Asset Adaptations***

From the three solution building blocks described above, a solution must be compiled for each individual oil and gas site asset. Variations that must be taken into account for individual adaptations are:

- Technical state of the site
- Corporate standards of the asset owner
- Local governmental rules and regulations
- Vendor best practices
- Actual integration demands

**Norwegian Oil Industry Association (OLF) Guideline No. 104**

Because of the introduction of Intergrated Operations the Norwegian Oil Industry Association (OLF) developed a security guideline in 2006; OLF Guideline number 104 (OLF, 104) applies to plant operators on the Norwegian Continental Shelf. It consists of 16 controls funded in ISO/IEC 27001:2005, adapted to the oil and gas sector.

The Information Security Baseline Requirements (ISBR) in the guideline consists of both administrative and technical controls:

- Administrative controls are establishing and enforcement of a security policy, risk management, business continuity planning, change management, patch management, education of personnel and documentation of work procedures, network topology, service documents, incident handling, etc.
- Technical controls are network segregation, default deny, host/system hardening and anti-malware tools.

The guideline can be downloaded from OLF (http://www.olf.no/hms/retningslinjer/).

## Project Experiences

In this paper two oil and gas assets on the Norwegian Continental Shelf operated by A/S Norske Shell are addressed. The two assets, Draugen and Ormen Lange are different in nature:

- Draugen is a fixed offshore concrete oil production platform, located outside of Kristiansund, Norway and has been in operation by Shell since 1993.
- Ormen Lange is a newly developed gas production subsea installation remotely operated from an onshore process plant located at Nyhamna, Norway. Ormen Lange has been producing gas since October 2007.

Both Draugen and Ormen Lange have recently been designed to facilitate Integrated Operations according to Shell requirements. Through the integration solutions established, both assets have been integrated with a newly developed Shell collaboration centre in Kristiansund, Norway.

In the following Sections we will look into the experiences from establishing integration solutions based on the *three main integration elements* for the two assets of such a different nature. The solutions have been established in co-operation with the operating oil company A/S Norske Shell and the companies in charge of the field development of Ormen Lange.

### Ormen Lange Experiences

The plant operator for Ormen Lange in the production phase of the plant is A/S Norske Shell. A different company, Norsk Hydro ASA, was the plant operator for the construction phase. The main engineering contractor was AkerKværner, but even in this role there was a split responsibility with Vetco Aibel as engineering contractor for a part of the plant. This role division created some challenges. Fortunately Shell has been proactively involved from the early phases. The main ABB project was performed for AkerKværner, but ABB has been running smaller side projects for Shell to ensure compatibility to Shell company standards.

#### *Work process*

Our very first work on Ormen Lange from an IT security and architecture perspective was the Remote Access Study which was finished in February 2004.

This was followed by a preparatory work for the Shell Remote Services solution for Ormen Lange that was started in July 2005. A working group consisting of AkerKværner, Hydro, Shell and ABB had regular meetings for one year. During that period a preliminary test was performed in November 2005 and a final test in May 2006. The final test was performed on the actual Ormen Lange delivery system installed for staging in ABB's offices in Oslo.

An OPC Security Test of the process control system was initiated in September 2005 as a preparation for using OPC interfaces to communicate with third party subsystems. Some findings were done in the process control typicals that needed to be addressed. As a continuance of the OPC security test a Process Control System User Access specification was prepared in December 2005.

The design process lead to the introduction of a *Plant Network* and *Remote Services* through the Shell managed Process Control Access Domain (PCAD), compliant with Shell regulations. See Figure 4 for illustration of the Ormen Lange network topology.

The Ormen Lange Plant System IT Design Specification was finished in January 2006 after some iterations with the engineering contractor. The implementation work for the Plant Network was started shortly thereafter to be ready for the final test of the Remote Services solution.

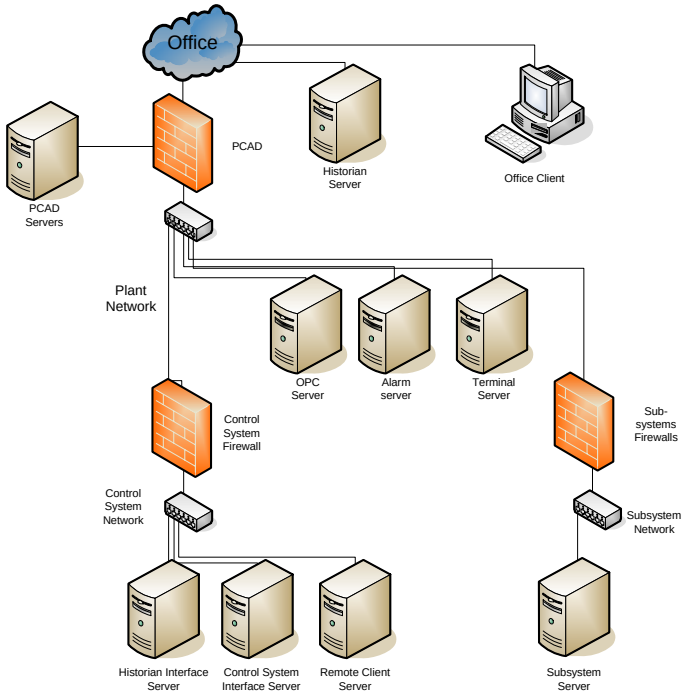


**Figure 4 Ormen Lange networks integrated through Plant Network**

In retrospect it can be pointed out that no Security Policy as such was specifically developed for the project. However, as seen above and in the following section about system start-up, a lot of work was done on the field of IT Security during the project. The plant operator also brings in considerable corporate security measures. Together, this would cover most aspects of a Security Policy. In coming projects we will place emphasis on creating the Security Policy in the early project phases.

***System start-up***

Site installation of the Plant Network was done in the fall 2006. The Remote Services system was simultaneously installed by Shell. A site acceptance test of the connection to the Ormen Lange Plant Network was performed in January 2007.

Currently many ABB and Shell users have access to the Ormen Lange SAS system through the Remote Services solution. In addition many more users have access through the third party- or subsystems connected to the Plant Network.

Two persons have been engaged on a 2 weeks on – 3 weeks off rotation for more than a full year to install the Plant Network and to assist the installation of the process control system on networking and IT security issues. These activities have been covered by the site team:

- Backup and Restore
- Security Policy
- Computer and User Administration
- System Operation
- Remote Access
- VirusScan setup
- Black Startup Procedure

***Solution compilation and Remote Services solution integration***

The Plant Network consists of five firewalls with a total of 20 connected control and subsystems in addition to several servers. One server on the Plant Network is dedicated for communication of real-time process data. Another is used for alarm and event collection and analysis. A terminal server has been set up for providing access to subsystem rich client applications which need specific software installed.

Backup of the servers on the Plant Network and the process control network is managed by a two-step procedure:

- Scheduled image backups of all computers are saved to the Backup servers in the systems.
- The contents of the Backup server hard drives are regularly saved to tape.

Interactive remote access from the Shell office network and the Third Party Access system is passed through the Shell PCAD system. Commonly used remote desktop solutions like pcAnywhere, VNC and RDP can be used to connect to control

and subsystem hosts. Authentication and access control is performed both by the remote services solution and the process control system and subsystems.

PCAD provides a secure solution for transferring files to and from the process control system and subsystem hosts. Anti-virus updates are also provided, with automatic updates set up on the Plant Network, process control and subsystem hosts. The anti-virus scanning on the process control system is set up according to ABB guidelines (ABB, 2007) to not impair the functionality of the process control system.

Windows patch management is handled by local Windows Server Update Services (WSUS) servers. These servers will be set up to upload patch information through PCAD. The WSUS servers are currently updated through a manual process.

**Draugen Experiences**

The Draugen platform has been in operation since 1993. The process control system at Draugen has been through several upgrades since the early start-up. As a result of this long operating history, the process control system consists of various technologies, where some parts differ from the technologies applied at the new field Ormen Lange.

***Work process***

To provide better support for the operation of the platform there was seen a need for more efficient and better exchange of *information*. As a result, the need for better integration of *data*, more flexible sharing of information and good tools for supporting Integrated Operations became evident. Based on concept studies and clarifications, a detailed design project was initiated to look into specifics on how to extend the present control system on Draugen through an improved IT Infrastructure within the so-called Process Control Domain (PCD). The establishment of this infrastructure is one key enabler for the Draugen Operation Centre established by Shell.

Scope of the detailed design project covered:

- Organizing the data streams from the main offshore production systems,
- Marshaling these streams in historian databases and alarm/event databases,
- Publishing user interfaces via terminal server computers and extending the offshore-located PCD to shore.

The offshore-to-shore communication link from Draugen is comprised of a wireless telecommunication link, which logically resides in the Shell Office Network domain.

The main focus of the project was to interface the existing control system without any negative interruption while at the same time providing the desired data and information flow. Through detailed design it was decided that as much as possible of the new equipment should be located onshore, i.e. on the other side of the telecommunication link, in the Shell locations at Råket, Kristiansund in Norway.

The projects related to establishment of the new infrastructure were managed directly between ABB and Shell, without an intermediate engineering contractor.

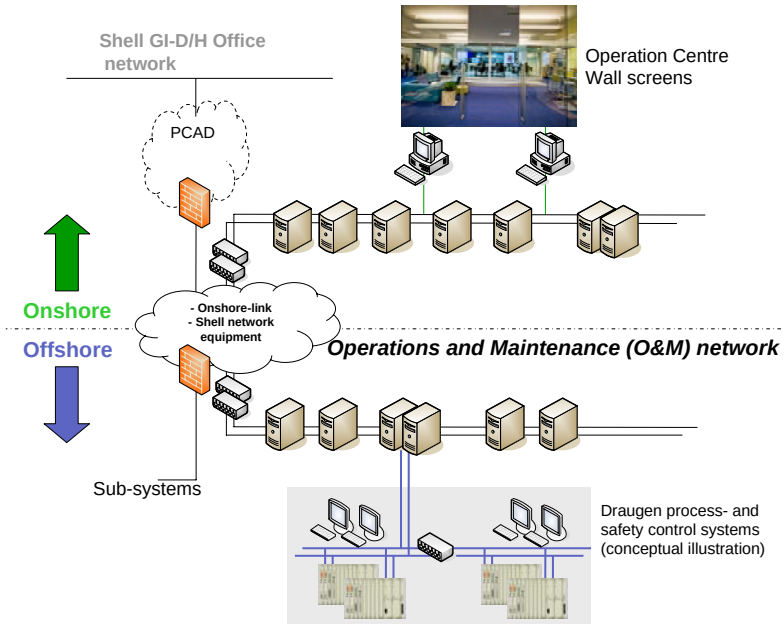


**Figure 5 Draugen control system extended with Operation & Maintenance Network.**

***Solution compilation and Remote Services solution integration***

The integration solution was to introduce a network level on top of the existing process control system network; an Operation & Maintenance (O&M) network. As a result of the requirement to locate relevant equipment onshore, this O&M network had to be extended through the communication link to shore. In solving this issue Shell was challenged on pure technical clarifications and also clarifications related to Shell standards, as the traditional boundaries between Process Control Domain and Office Domains were pushed.

A successful technical solution was established that covered security and encryption issues through Shell managed equipment and network transparency from offshore to shore through network router equipment managed by the project. See Figure 5 for illustrations.

As for Ormen Lange, remote services are managed through the Shell PCAD system in combination with terminal servers on the O&M network. The terminal servers provide read-only access to operator stations located on the process control network, and also access to rich-client subsystem applications. There is one terminal server located offshore and one terminal server located onshore to minimized network load on the communication link to shore.

There are two servers dedicated to processing of Advanced Process Control (APC) applications and one server for information management and distribution of real-time process data to the plant historian.

Other servers are present for backup management and connectivity to the Draugen process control network. Finally, there are two desktop clients for use in the Shell Operation Centre, whereof one is interfaced to the large wall screens in the Operation Centre.

The backup regime is similar to Ormen Lange, where system images are copied to the local backup server, which in turn copies all the images to a tape station. Due to the offshore-onshore distributed topology, there is one backup system on the Draugen offshore platform and one for the server farm on shore at Råket.

Anti-virus and Windows patch management are handled similarly to Ormen Lange.

The new Operation & Maintenance network was operational in July 2007 with APC applications operating on real-time data and also read-only access to offshore process graphics made available in the Shell Operation Centre in Råket, Kristiansund. Real-time data streaming to the plant historian database has been active since October 2007.

At Draugen the PCAD access was installed and activated in February 2007, enabling remote access and support.

## Remote Support

Both the plant operator and the process control system vendor have established operation rooms for remote access and collaboration towards the two plant.

### Shell Operation Centre

In parallel with the Ormen Lange and Draugen projects on process control systems integration Shell has managed a project on establishing an Operation Centre for supporting Integration Operations on Ormen Lange and Draugen. See Figure 6 for illustration of the Operation Centre.

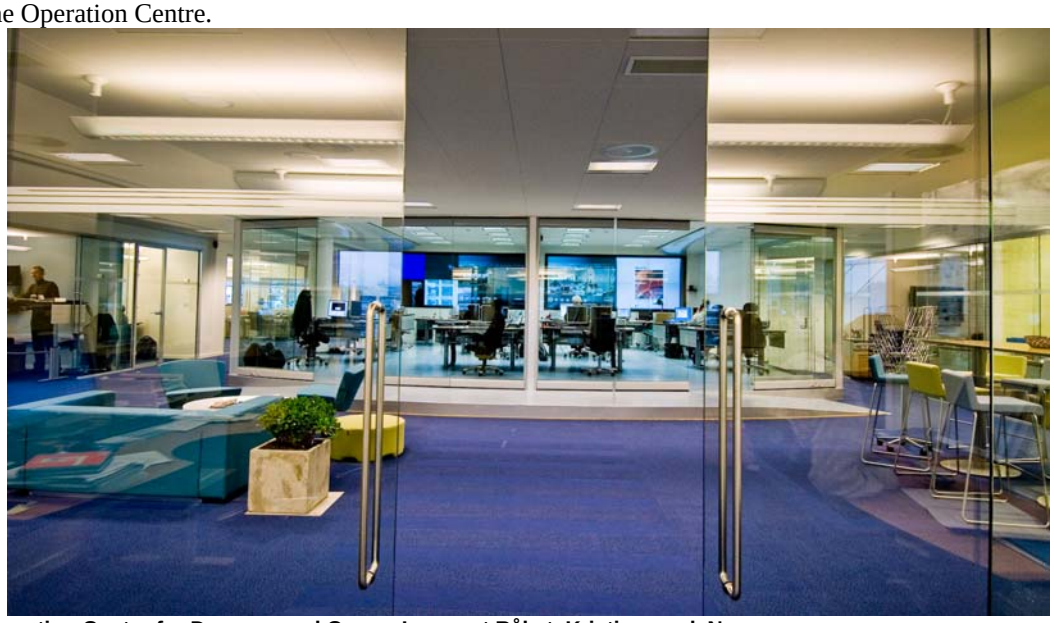

**Figure 6 Shell Operation Centre for Draugen and Ormen Lange at Råket, Kristiansund, Norway.**
**Draugen operation room left of centre-line,**
**Ormen Lange operation room right of centre-line.**

**Vendor Remote Support**

For supporting Ormen Lange and Draugen, ABB has implemented a dedicated ABB Remote Monitoring and Operation Room (ARMOR) in the Oslo offices. The ARMOR room consists of two parts, a compact work station room with a large wall screen, and a multifunction meeting room. Both parts of the room have video conference capabilities. See Figure 7 for illustrations of the two rooms.

**Figure 7 Shell ARMOR room**
**Left: Compact work station room,**
**Right: Multifunction room**

From the Shell ARMOR room the following vendor service are performed:

- Service; regular commitments that does not require customer involvement
- Support; handling of customer enquiries.
- Modification projects; Minor plant modifications that does not require presence at site.

Remote access to Ormen Lange and Draugen from the ARMOR room is done through PCAD.

## Conclusions

We have implemented IT architectures for supporting Integrated Operations on two oil and gas plant assets that are different in nature; one new onshore facility and one offshore facility with 14 years of operational history. The implementations have been done in close cooperation with the plant operator; A/S Norske Shell.

In the two projects we have created tailored solutions for the individual assets, from a generic solution basis. The technical state of plants, the required level of integration, and the customer requirements have been taken into account. Both projects have been through processes of evaluation for compliance with Shell corporate standards.

The development of good solutions for network integration from process control networks to the office network have facilitated establishment of both owner and vendor collaboration solutions towards the two plants.

Specially, through the implementation process we have experienced that close cooperation with the end-user company encourages good solutions to complex technical tasks.

## References

Norwegian Ministry of Justice And The Police: Et sårbart samfunn. NOU 2000: 24, 3. juli 2000, ISBN 82-583-0537-9

OLF (The Norwegian Oil Industry Association) Guideline No. 104 – Information security baseling requirements for process control, safety and support ICT systems. 01.04.2007. Rev 03. www.olf.no/?50182.pdf

Using McAfee VirusScan® Enterprise with System 800xA. 2007. ABB Automation Technologies 3BSE048631 A

IS Security Considerations for Automation Systems. 2005. ABB Automation Technologies. 3BSE032547 A