A secure future

ABB's Remote Monitoring and Operation Services are changing the way process automation systems are controlled

Ragnar Schierholz, Bjarte Birkeland, Martin Naedele

Information technology (IT) is now being used by most companies as a way of effectively controlling and monitoring their process automation systems. While modern information and communication technologies allow access to remote and confidential information simply by clicking a button, the danger that unauthorized personnel can illegally gain access is ever-present. Significant efforts are being made by these companies to protect their automation systems against cyber-attacks and other information security related threats. These efforts are also necessary to comply with industry standards and the increasing number of regulatory requirements that are coming into effect. The downside, however, is that many companies must build-up substantial expertize in the field of IT security, and this can be very costly.

Another way of approaching this is to find a reliable partner who can provide the services which allow them to be compliant without having to invest in new resources. One such company who can do this is ABB. Using its Remote Monitoring and Operations Services, ABB can guarantee the secure operation of a company's process automation system while the customer concentrates on the important business of increasing its profit line.

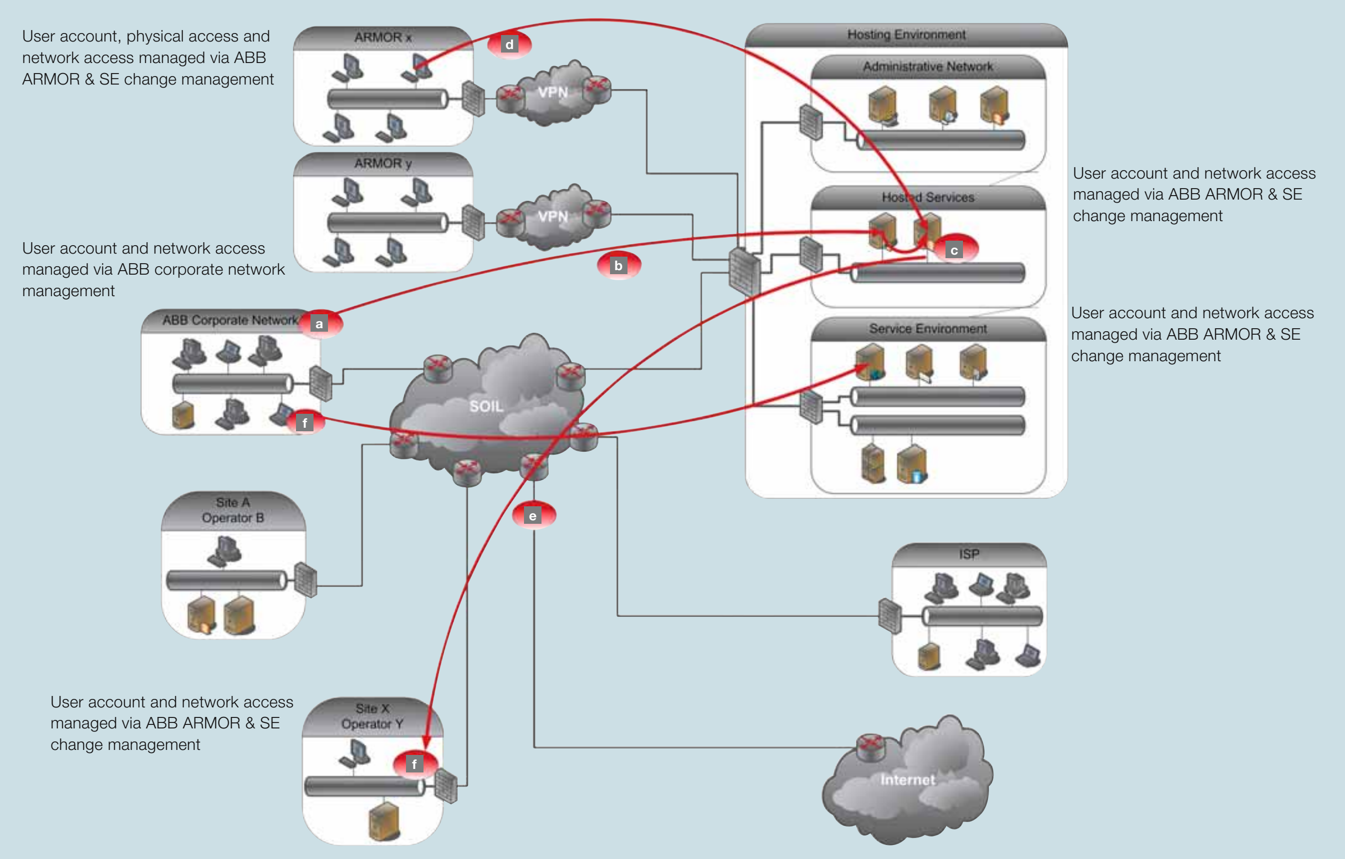
Information technology (IT) is helping many businesses to streamline their processes, and those who have gone down this road have seen an increase in productivity and higher profits. The Norwegian Oil and Gas industry, under the heading of “Integrated Operations (IO)[1]” , is currently on this journey. Integrated Operations, as defined by The Norwegian Oil Industry Association, the OLF, is “the use of information technology to change work processes to reach better decisions, remote-control equipment and processes, and to move functions and personnel onshore.” The main idea of IO is therefore to streamline all work processes (ie, planning, production, and maintenance) across organizations (such as oil producers and their suppliers) and locations (on-shore and off-shore). The expected benefits include an increase in the amount of oil recovered, the acceleration of production, and the reduction of operational costs. OLF reckons that implementing IO will require an investment of approximately 25 billion NOK (US $ 4.6 billion), while the potential value of the investment over the next 15 years is estimated at 250 billion NOK (US $ 46 billion).

Modern information and communication technologies are the foundations

Footnote

[1] http://www.olf.no/english/news/?52210 (December 2007)

1 Sample process for remote work: A typical process flow, with the relevant security mechanisms for remote work on customer sites. An example scenario of updating a locally installed application, involving both file transfer and interactive access to the target host is depicted.



User account, physical access and network access managed via ABB ARMOR & SE change management

User account and network access managed via ABB corporate network management

User account and network access managed via ABB ARMOR & SE change management

User account and network access managed via ABB ARMOR & SE change management

User account and network access managed via ABB ARMOR & SE change management

a Input:
  Newly discovered vulnerability & patch
  Configuration data
Activities:
  Analyze vulnerability
  Assess criticality
  Test patch & develop action plan
  Identify relevant assets
  Approve action plan in CAB
Connected processes:
  Field alert management
  Configuration management

b Activities:
  Upload patch files to file server
Connected processes:
  Change management – user accounts on file server

c Activities:
  Automatic virus check on file server
  Transfer to user environment on terminal server

d Activities:
  User entry to ARMOR
  User logon to terminal server
Connected processes:
  Change management – access to ARMOR
  Change management – user accounts on ARMOR host and terminal server

e Activities:
  File transfer to target at customer site
  User logon to target at customer site
  Local install of patch on targets according to approved workplan
Connected processes:
  Change management – access to connectivity to customer site
  Change management – user accounts on target host at customer site
  Change management – approved workplan

f Activities:
  Update of configuration data in CMDB according to performed workplan actions
Connected processes:
  Change management – approved workplan
  Change management

upon which IO depends. However, establishing separate connections to remote sites, such as oil rigs in the Norwegian Sea or gas fields at the North Cape, for each operator and each supplier is wholly inefficient. The most economical solution, therefore, uses a shared infrastructure based on current Internet technology. Connectivity based on Internet technology or even to the Internet itself requires a much higher level of information security than previous isolated control system installations. The OLF has addressed this by issuing a set of baseline requirements for information security (ISBR) in oil and gas production. In fact, these requirements are aligned with many international security guideline initiatives.

Remote Monitoring and Operation

ABB is no stranger to the world of IT. Its Remote Diagnostic Service offering has been successfully helping customers increase the return on their assets by optimizing plant operations and reducing maintenance efforts. Now ABB has gone a step further to ensure secure operation within the process automation domain. By adapting its IT Service Management approach to the IT Infrastructure Library (ITIL)[2], ABB has extended its service portfolio to include Remote Monitoring and Operation Services. With this set of services, aspects such as incident management, maintenance of a site inventory database[3], system setup and maintenance, as well as remote condition monitoring for ABB and third-party equipment, secure client and server management, or on-site and remote backup are covered 1. If all these services are contracted out to ABB, an operator not only obtains remote automation system maintenance services that are secure and regulation compliant, but he also benefits from ABB's IT security and management expertize without having to invest in new in-house resources. In other words, the security and well-being of the entire system becomes the responsibility of ABB.

A safe and secure environment

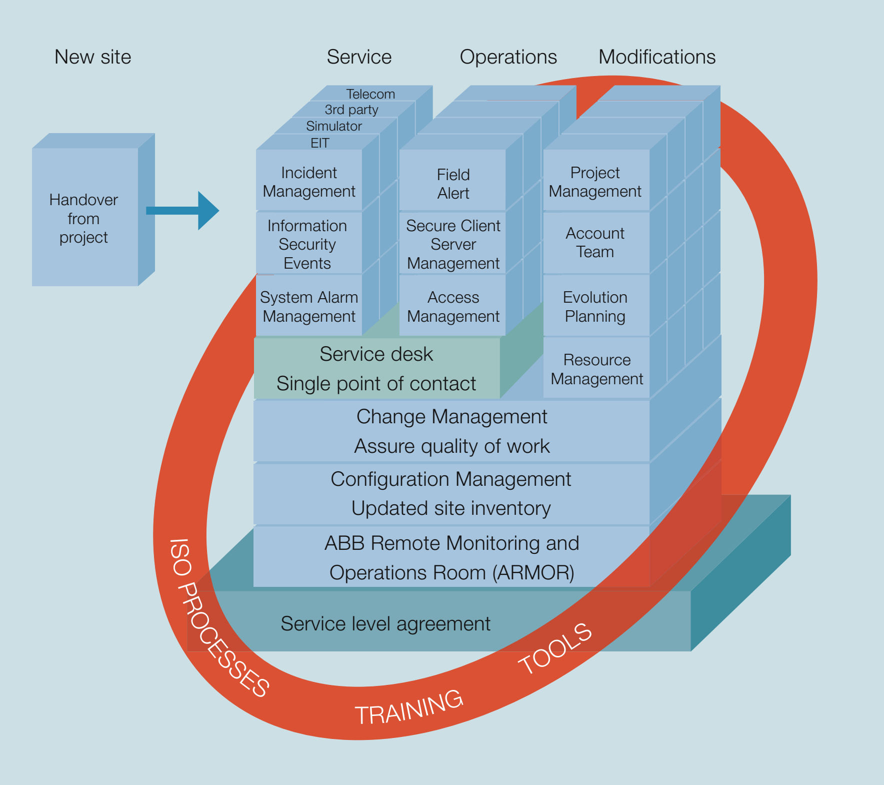
In providing such a service, ABB uses an infrastructure that consists of four high-level components:

- Remote access to on-site automation systems including interactive access via terminal services, as well as file transfer facilities.
- Specially secured on-shore operator rooms, known as ARMOR (ABB Remote Monitoring and Operations Room), in multiple locations. Remote work on "hot" installations can only be performed from within these special rooms.
- A multi-tenant[4] service desk application suite (Service Environment, SE). This suite offers all the functionality required for the management of service requests and other incidents. It also features a Configuration Management Database (CMDB) which forms the basis of the site inventory service and provides data for various other services.
- An office environment in which service desk staff works and where test environments for product configurations are available.

With ABB's Remote Monitoring and Operating Services, an operator obtains remote automation system maintenance services that are secure and regulation compliant.

Connectivity between these components is established via a Secure Oil Information Link (SOIL) and dedicated

2 The main customer support and modification processes within the Service Environment



Footnotes

[2] The IT Infrastructure Library (ITIL) is a comprehensive process framework for IT service management, originally developed by the UK Government's Central Computer and Telecommunications Agency (CCTA). It combines multiple previous approaches into a coherent set of processes. However, the processes are described on a generic level and a more detailed, organization-specific definition has to be developed to implement the ITIL approach. For more information on ITIL see http://www.itil-official-site.com/ or http://www.itil.org/.

[3] Each site, such as an oil rig, has its own inventory, and all site inventories are separately stored in a centrally operated database.

[4] Multi-tenant refers to the ability of a hosting site to hold data and provide functionality to multiple customers at the same time. It behaves as if it were a separate system for each customer. This allows for lower operational costs and higher efficiency and scalability.

virtual private networks (VPN). SOIL is an extranet operated by a consortium of all major players in the Norwegian oil and gas market. It provides network connectivity and basic network services to its members in the North Sea Oil & Gas industry, and its use is being extended to include other players around the world.

The security requirements for any service infrastructure are mainly influenced by two things: The security of the customer's automation system and automation network must not be endangered; and the remote access infrastructure, ARMOR and SE, has to be protected against malicious interference. In both cases, perimeter protection, account management and access control, malware protection, and patch management are therefore required. These solutions must be compliant with standards and regulations for general and process automation system security. Besides technical security controls, operational procedures that ensure continuous security management and secure operations must also be in place.

The application of ABB's infrastructure in a process automation system environment is described in the following paragraphs.

ARMOR and the SE architecture

Remote access to on-site systems is realized through a multi-tiered architecture. The first tier consists of the ARMOR rooms. Access to these rooms is only possible with a PIN-protected magnetic swipe card, which is issued after the employee has undergone special training[5]. The computers in each ARMOR room are located in a locked cabinet. Access is limited to administration staff only and is not allowed during remote work. User accounts on these workstations are managed via ABB's Secure Client and Server Management service. Each ARMOR network is connected to the hosting environment via a dedicated VPN connection, and the perimeter of each network is protected by a firewall. Only network connections between the ARMOR rooms and dedicated servers in the hosting environment are allowed.

The second tier is a server infrastructure in the hosting environment. Included in this environment are: terminal servers, which the users in the ARMOR rooms connect to; file servers that allow file transfers between sites; a web server; an application server; and a database server. Additional servers for administrative purposes, such as domain controllers and backup servers, can also be found in the hosting environment. A set of firewalls protect the hosting environment and only clients in authorized network segments (eg, from ARMOR or registered customer sites) using authorized protocols can connect the servers. Servers with different functionalities are separated by VLANs, and connection is only possible through a firewall. In doing this, different security levels can be applied to the various servers.

For interactive access to customer sites, screen mirroring applications, such as Citrix or Microsoft Terminal Services are used. Inbound connections to the terminal server are allowed only if they originate in the ARMOR rooms. Outgoing connections are only permitted to registered terminal servers at customer sites using the protocol registered for the respective server. Each authorized user has an individual account on the terminal server. Individual user profiles will contain information concerning only the terminal servers at a customer site that the user is authorized to use. The authorization and registration of customer sites is managed via the change management process.

Besides technical security controls, management processes are key elements of common information security standards and regulations.

For file transfers between customer sites, the same authorization is applied. Users cannot place data on the ARMOR workstations. Instead, data required for remote work on customer systems must be transferred to a file server in the hosting environment via SSL-secured sessions. On the file server, the data is scanned for viruses and other malware. If the scan is negative, the data is made available in the user's terminal server session and can be transferred to customer systems.

Customer systems, which constitute the third tier, may be servers, such as OPC servers, or System 800xA nodes or clients, such as System 800xA operator workstations. A typical customer system may consist of sub-tiers. Interactive access to, as well as file transfer to and from on-site systems is performed according to procedures defined by customer security policies. These may mandate technical details, such as file transfer mechanisms via secured FTP or encryption endpoints, with detailed logging under customer control[6].

Besides technical security controls, management processes are key elements of common information security standards and regulations. These typically include incident management, change management, configuration management, field alert management and business continuity management 2. Process definitions and operational guidelines that comply with relevant standards are in place for the ARMOR and SE operations.

Management processes – an overview

Field alert management covers both the customer system and the external environment. Using the Asset Optimizer component of the System 800xA product line, the customer's process automation system is continuously monitored so that failures can be prevented. Data is sent from the system to the service desk application where it is processed and viewed by operations staff. This data includes information about the security status of the process control system, for example the number of failed login attempts, the number of active sessions, or if there has been an excessive number of denied connection attempts on the firewalls. The operator is alerted to any data that meets predefined condi-

Footnotes

[5] Refresher courses must be taken once a year

[6] For accountability purposes

tions (eg, a certain number of failed login attempts) or deviates from normal behavior. When this happens, the data is dealt with using *incident management*. As regards incidents stemming from the external environment[7], a list of products – both ABB and third party – used on any contracted site is maintained. For these products, information, such as update notifications or vulnerability disclosures, is monitored. The disclosure of vulnerabilities, new updates or patches is evaluated by a service team, which then derives some form of implementation plan. Using the CMDB, the service team identifies affected systems and initiates a *change management* process to take any necessary action. Incident management can also be triggered by service requests submitted by customers, and how these are dealt with depends on the nature of the incident. Some cases will be handled by the service desk application, while others will be referred to the change management process.

In the change management process, all change requests and their associated documentation (eg, test reports for updates or patches) are reviewed and approved by a site-specific Change Advisory Board (CAB). Besides incident management, release management may also trigger the change management process.

Effective changes in a system's configuration are handled in a configuration management process. All relevant information for system operation and service, including configuration items such as network nodes, applications or users, is maintained in the CMDB. The *configuration management* process ensures that all configuration items are properly registered and updated, enabling ABB to present an accurate inventory of the entire process automation system at any time.

Customers in other industries, such as power utilities or process plants, will soon be able to reap the benefits of ABB's service environment.

Vision for the (not so distant) future

In recent years, ABB has consistently shown itself to be aware of and concerned about IT security issues in automation systems. The goal of ABB's Remote Monitoring and Operations Service offering is to translate this expertize into a comprehensive set of services that will not only assist ABB customers in operating and securing their automation systems and plant networks, but it will also ensure they are in compliance with standards and regulations, as well as industry best practices. This assistance could extend right up to the remote operation of the entire process automation system by ABB service staff. For this purpose, the company plans to install ARMOR-type facilities around the globe, beginning in regions with strong oil and gas industries, such as the Gulf of Mexico or the Middle East. In doing this, ABB will be able to provide efficient and expert assistance around a clock to a larger number of customers.

ABB's service environment is not limited to the Oil & Gas industry alone. Customers in other industries, such as power utilities or process plants will soon be able to reap the benefits of these services. Using the expertize acquired in the Oil & Gas Industry, ABB Corporate Research is currently working on a reference architecture for secure remote access infrastructure that is suitable for other industries, as well as other business units.

Shell has entered into a full Service Environment contract with ABB. Signing the contract are Shell's Director of Operations, Gunnar Ervik, and Bjarte Pedersen, Director, ABB Oil & Gas

Ragnar Schierholz
Martin Naedele
ABB Corporate Research
Baden-Dättwil, Switzerland
ragnar.schierholz@ch.abb.com
martin.naedele@ch.abb.com

Bjarte Birkeland
ABB AS
Bergen, Norway
bjarte.birkeland@no.abb.com

Footnote

[7] "External environment" in this context refers to external information relevant to a system component that triggers an incident (as opposed to an alert coming from a system component).