Chapter 7

REDUCING RISK IN OIL AND GAS PRODUCTION OPERATIONS

Stig Johnsen, Rune Ask and Randi Roisli

Abstract Remote operations are commonly employed in oil and gas installations in the North Sea and elsewhere. The use of information and communications technologies (ICT) has resulted in process control systems being connected to corporate networks as well as the Internet. In addition, multiple companies, functioning as a virtual organization, are involved in operations and management. The increased connectivity and human collaboration in remote operations have significantly enhanced the risks to safety and security.

This paper discusses methods and guidelines for addressing different types of risks posed by remote operations: technical ICT-based risks, organizational risks and risks related to human factors. Three techniques are described: (i) ISO 27001 based information security requirements for process control, safety and support ICT systems; (ii) CRIOP, an ISO 11064 based methodology that provides a checklist and scenario analysis for remote operations centers; and (iii) CheckIT, a method for improving an organization's safety and security culture.

Keywords: Oil and gas production, remote operations, information security, human factors

1. Introduction

Remote operations of offshore oil and gas installations are increasing in the North Sea and elsewhere [12]. The main motivations for remote operations are the potential for cost reduction, higher yields from fields, improved collaboration and increased safety. However, projects focused on implementing remote operations (especially moving personnel onshore) have often been scaled back or delayed due to higher degrees of complexity than originally anticipated.

The technologies used in remote operations are changing from proprietary stand-alone systems to standardized PC-based IT systems and networks, which, in turn, may be connected to the Internet. The reliance on commercial off-the-

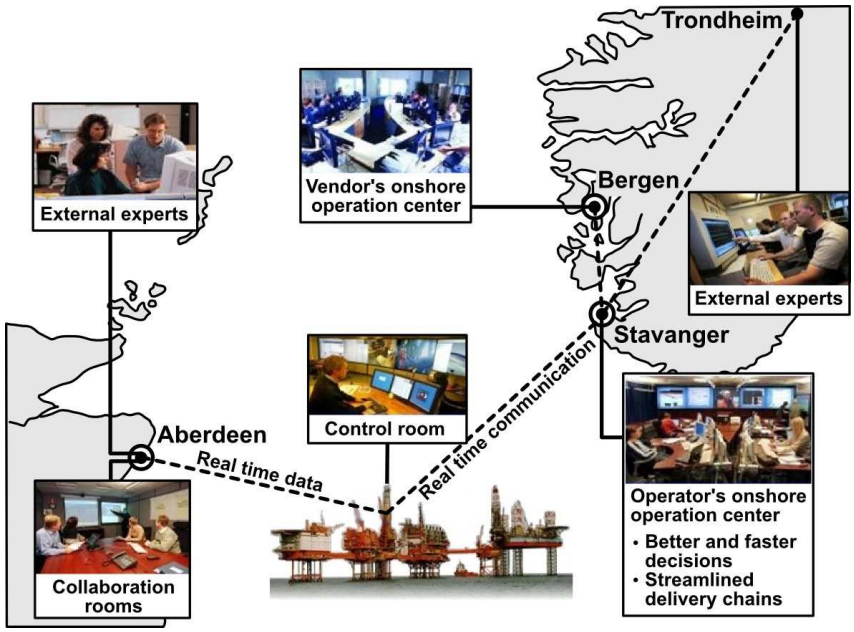

Figure 1. Key actors involved in remote operations [12].

shelf (COTS) operating systems increases the connectivity between process control systems (or supervisory control and data acquisition (SCADA)) systems and the general information technology and telecommunications (ICT) infrastructure. (Note that we refer to process control systems as SCADA systems in this paper.) This also increases the overall vulnerability. SCADA systems are fundamentally different from ICT systems. Several challenges are introduced when ICT and SCADA systems are integrated, including the need for anti-virus solutions, patches and enhanced information security.

There has been an increase in security incidents related to SCADA systems, some of which have significantly impacted operations [15]. However, security breaches are seldom reported and detailed information is almost never shared. The traditional view in North Sea operations was that SCADA systems were sheltered from threats emerging from public networks. This perception still seems to be widespread in the automation profession, which raises serious questions about the safety and security of remote operations [15].

The operating environment has changed. Remote operations involve the collaboration of experts at different geographical locations. Operations and maintenance tasks are being outsourced to suppliers and vendors, a trend that will likely increase. This situation coupled with enhanced connectivity increases the likelihood of accidents and malicious incidents, which can result in significant economic losses and, in the worst case, loss of lives. Figure 1 illustrates the scale of remote operations and identifies the key actors and their roles.

Security incidents and accidents can lead to costly production stoppages. The costs of a stoppage on the Norwegian Continental Shelf are usually in the two or three million dollar range, but can be much higher if a key production facility is affected [13]. It is widely acknowledged that human errors contribute significantly to accidents and casualties [4, 11], and must therefore be included when discussing the challenges posed by remote operations. History shows that personnel involved in remote operations have a tendency to focus too much on technology, often at the expense of organizational and cultural issues. Virtual organizations and the increased number of vulnerabilities create the need for a common risk perception and a pervasive safety and security culture to reduce risks. All elements of risk mitigation must be addressed in order to establish the appropriate depth and breadth of defenses.

2. Remote Operations

This paper identifies several key challenges related to remote operations in the oil and gas industry, especially those involving the integration of SCADA and ICT systems. The challenges, which cover technology, organizations and human factors, are listed in Table 1. Major challenges include reducing the new vulnerabilities introduced by organizational changes, integrating SCADA and ICT systems, and addressing human factors issues related to the involvement of actors from multiple organizations, often with different cultural views.

Integrating SCADA and ICT systems is difficult because the two types of systems differ in many respects. Availability is the most important factor for SCADA systems (key processes must be managed in milliseconds), followed by integrity, and then confidentiality. In contrast, confidentiality and integrity are crucial for ICT systems used in business settings. Availability is less important as response times are typically measured in seconds and short delays or outages are generally not critical to business operations.

SCADA systems generally have complex, specially-designed architectures. Anti-virus software is difficult or impossible to deploy and must be manually updated; there are often long delays in patch deployment, requiring complex testing and certification by vendors. Furthermore, SCADA system changes are rare, and are typically local and informal. SCADA systems have long lifecycles of five to twenty-five years. On the other hand, ICT systems are usually standardized and centrally managed in terms of their architecture and deployment of anti-virus software and patches. Also, automated tools are widely used, changes are frequent and centrally managed, and system lifecycles are much shorter at three to five years.

Despite the differences between the SCADA and ICT systems, systematic testing of integrated SCADA-ICT systems is not always performed. This can lead to operational problems – 30% of SCADA components in one facility broke down when exposed to high ICT traffic loads [10]. The scope and inherent complexities of the systems to be integrated and the organizational challenges faced by technical support personnel should not be underestimated.

Table 1. Organizational challenges in remote operations.

Present Status	**Local Operations**	**Changes Related to Remote Operations**
Integration	Large degree of segregation of SCADA systems	Increased need to integrate SCADA and ICT systems offshore and onshore
Standardization	Local, complex tailor-made solutions	Increased standardization for cost-effective, secure management of remote installations
Virtual Organizations	Operations are performed locally using local resources	Operations are performed by a virtual organization with geographically distributed entities
Generalization vs. Specialization	General expertise centered at a local installation	Experts available at any time remotely; reduced local expertise
24/7 Responsibility	Local responsibility; actors are available 24/7	Dispersed responsibilities must be defined for actors involved in 24/7 operations
Mode of Operations (Local vs. Remote)	Operations team close to the operational environment	Operations team isolated from the operational environment
Proactive vs. Reactive	Reactive	Focus on planning and proactive management
Culturally Driven	Managed by procedures and work orders; inter-personal trust	Focus on attitudes, knowledge, perceptions and improvisation; distributed competence and technology
Organizational Change Management	Few fundamental changes; focus on safety and costs/ benefits	Large changes to organization and work processes (new technology and moving functions onshore); fear of reduced safety

Systematic checklists should be used in addition to thorough risk analysis such as hazard and operability (HAZOP) studies to establish common risk perceptions. Testing should be performed to ensure resilience against denial of service (DoS) attacks, viruses, worms and other malicious code. The probabilities and consequences of likely incidents should be documented in a risk matrix. The risk matrix should be developed in close collaboration between management, ICT personnel, operations personnel and human factors experts to ensure common risk perceptions. A new industry best practice named ISBR (Information Security Baseline Requirements for Process Control, Safety and

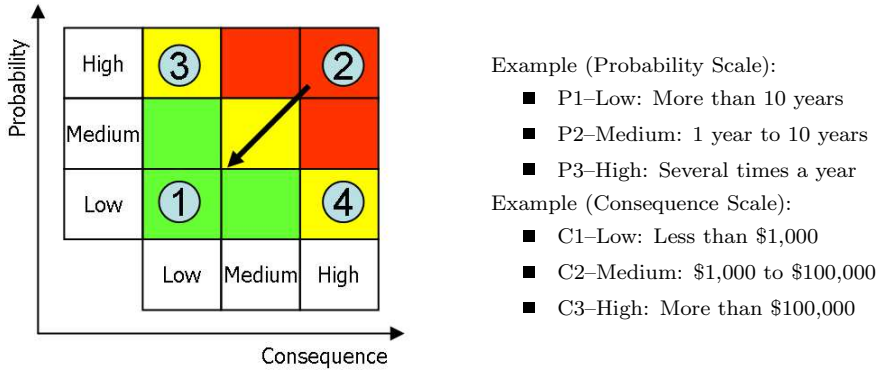

Figure 2. Common risk matrix in the oil and gas industry.

Support ICT Systems) [3] based on ISO/IEC 27001:2005 has been developed by the Norwegian Oil Industry Association (OLF) to aid in this process.

The differences between SCADA and ICT systems based on organizational and human factors are important, but are not considered adequately. For SCADA systems, responsibility and expertise often reside locally and solutions are not well documented. Risk management and hazard analysis are done explicitly and emergency shutdown systems are essential. For SCADA systems, while knowledge about vulnerabilities and threats (and information security skills) is quite poor, the potential risk impact is significant (loss of control, loss of production, loss of life). For ICT systems, responsibility and knowledge are centralized, tasks are outsourced and safety is rarely an issue. Furthermore, knowledge about ICT vulnerabilities and threats is moderate to high, and the potential risk impact is mainly restricted to the loss of data.

Cooperation between SCADA and ICT staff is not well established due to differences in technology and system separation. However, remote operations require integration, which is difficult to implement because of differences in organization, terminology and expertise in addition to the technical differences. Key mitigation factors include cooperation, increased training, establishing common goals and understanding the risks. To this end, a common risk matrix should be established that documents the technical, organizational and human factors issues. This is achieved using the methods and tools described in this paper: ISBR, information security baseline requirements for process control, safety and support ICT systems; CRIOP scenario analysis for remote operations centers; and CheckIT, a questionnaire-based method for improving an organization's safety and security culture.

3. Major Risks

Security incidents should be analyzed and placed in a risk matrix (Figure 2) to help stakeholders focus on the major risks. A risk matrix creates a foundation

for the development and prioritization of mitigation actions, including security guidelines and procedures.

Ideally, all the risks in a risk matrix should be in first quadrant, corresponding to low probability and low consequence. In the real world, however, many of the risks are in the second quadrant, high probability and high consequence. By implementing security controls, the organization can reduce the probability or the consequence or, better still, both. Risks in the third quadrant have a high probability of occurrence, but do not necessarily cause serious harm; security measures should be implemented based on a cost/benefit analysis. The fourth quadrant corresponds to unwanted incidents that fortunately occur very rarely; mitigation measures for these incidents are generally too costly and not worthwhile. Instead, organizations should develop contingency plans for these eventualities.

Based on interviews and discussions with oil and gas industry experts, we have documented common risks and security incidents related to remote operations in oil and gas facilities. Some of the risks lie in the high probability/high consequence quadrant of the risk matrix:

- **Poor Situational Awareness:** A remote operations system does not give a comprehensive overview of the situation, resulting in poor situational awareness. This can lead to communication problems, misunderstanding and, ultimately, serious safety or security incidents.

- **ICT Traffic Impact:** A SCADA system crashes due to unexpected or unauthorized traffic from ICT systems. This could be caused by excessive ICT traffic affecting a key communication component between onshore and offshore systems, resulting in a shutdown of remote operations. Tests at CERN have demonstrated that 30% of SCADA components crashed when they were subjected to large volumes of ICT traffic or erroneous ICT traffic [10].

- **Virus/Worm Attacks:** A virus or worm causes unpredictable behavior or shuts down key SCADA components, disrupting production processes. This can occur if a PC or other IT equipment is connected to a network without screening it for malware. In mid August 2005, the Zotob.E worm attacked a major Norwegian oil and gas company. By September 15, 2005, 157 computers were infected, many of which were located in offshore facilities. The ICT staff had to explain the consequences to operations personnel at some length before adequate mitigative actions (patching computer systems used for safety-critical operations) could be implemented. Fortunately no accidents occurred as a result of the worm infection [14].

As described above, the major risks to remote operations at oil and gas facilities are poor situational awareness, denial of service and virus/worm attacks. A human factors approach to mitigating these risks involves working

with technology, organizations and humans. The following three sections describe strategies for addressing technical ICT-based risks, organizational risks and risks related to human factors.

4. Information Security Baseline Requirements

Legislation and business practices related to health, safety and the environment for offshore operations have existed for decades, but information security issues have been largely ignored until very recently. As increasing numbers of companies set up remote operations and interconnect with vendors and suppliers, a need for a common information security baseline has emerged. Responding to this need, the Norwegian Oil Industry Association (OLF) has developed ISBR – information security baseline requirements for process control, safety and support ICT systems [3]. The guidelines, which came into force in July 2007, include the following sixteen requirements:

- An information security policy for process control, safety and support ICT systems shall be documented.
- Risk assessments shall be performed for process control, safety and support ICT systems and networks.
- Process control, safety and support ICT systems shall have designated system and data owners.
- The infrastructure shall provide network segregation and all communication paths shall be controlled.
- Users of process control, safety and support ICT systems shall be knowledgeable about information security requirements and acceptable use of ICT systems.
- Process control, safety and support ICT systems shall be used for designated purposes only.
- Disaster recovery plans shall be documented and tested for critical process control, safety and support ICT systems.
- Information security requirements for ICT components shall be integrated in engineering, procurement and commissioning processes.
- Critical process control, safety and support ICT systems shall have defined and documented service and support levels.
- Change management and work permit procedures shall be followed for all connections and changes to process control, safety and support ICT systems and networks.
- Updated network topology diagrams that include all system components and interfaces shall be available.

- ICT systems shall be kept updated and patched when connected to process control, safety and support networks.
- Process control, safety and support ICT systems shall have adequate, updated and active protection against malicious software.
- All access rights shall be denied unless explicitly granted.
- Required operational and maintenance procedures shall be documented and kept current.
- Procedures for reporting security events and incidents shall be documented and implemented.

The baseline requirements represent information security best practices that have been adapted to the oil and gas sector from the ISO/IEC 27001:2005 (formerly BS7799-2) specifications. The requirements are supposed to be implemented over and above a company's information security policies subject to national legislation; consequently, the requirements are neither pre-emptive nor exhaustive. Implementation guidance for requirements is available, and a self-assessment tool for companies to verify compliance has also been developed [3].

5. CRIOP Methodology

CRIOP [6] is a methodology for verifying and validating the ability of a control center to safely and efficiently handle all modes of operations. It can be applied to central control rooms; drillers' cabins, cranes and other types of cabins; and onshore, offshore and emergency control rooms. CRIOP has been used with much success in the Norwegian oil and gas sector since 1990 to provide situational awareness, clarify responsibilities in distributed teams and mitigate risk in cooperating organizations.

A CRIOP analysis takes between two and five days. The methodology was improved in 2003 to support and validate the ISO 11064 standard (Ergonomic Design of Control Centers). CRIOP was further enhanced in 2004 to assess the influence of remote operations and integrated operations. These changes have been tested and are scheduled to be fully implemented in 2007.

The key elements of CRIOP are:

- A learning arena where operators, designers, management and other actors can meet and evaluate the optimal control center during design, construction and operations
- Checklists covering relevant areas in the design of a control center
- Analysis of key scenarios

The CRIOP methodology attempts to ensure that human factors issues are emphasized in all aspects of remote operations. The primary human-factors-based principles are to: form interdisciplinary teams, ensure systematic end-user participation, conduct human factors analyses (e.g., function and task

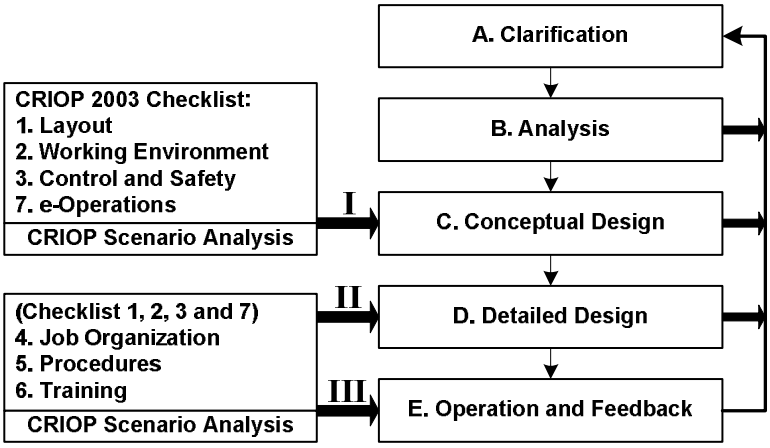

Figure 3. Suggested use of CRIOP based on the ISO 11064 phases.

analyses), and improve design through iteration and documentation of the process.

Figure 3 presents the suggested use of CRIOP based on the ISO 11064 phases. Several Norwegian oil and gas companies use CRIOP on a regular basis. In particular, they recommend using CRIOP in three stages (I, II and III) in design and operations processes.

CRIOP's scenario analysis is a dynamic approach that helps assess control room actions in response to possible critical scenarios. An example scenario is exception handling involving offshore and onshore control centers during remote operations. The main steps in scenario analysis are: (i) selection of a realistic scenario; (ii) description of the scenario using a sequential time event plotting (STEP) diagram [6]; (iii) identification of critical decisions and analysis of the decisions; and (iv) evaluation of possible barriers. Scenario analysis is typically performed by a group of participants from the control center or central control room along with key personnel from offshore operations centers.

The CRIOP methodology uses a checklist to identify relevant scenarios related to remote operations [8]. The principal elements of the checklist are:

- **E1:** Is the term "remote operations" defined precisely?
- **E5:** Are the major stakeholders identified, analyzed and involved in the change project?
- **E8:** Are the requirements for establishing common situational knowledge for participants in remote operations established?
- **E10:** Are all interfaces and organizational areas of responsibility clearly defined?
- **E11:** Has a risk assessment been performed prior to and after the implementation of remote operations?

- **E11.3:** Are all remote accesses documented, analyzed and protected from unauthorized use?
- **E12:** Have all security and safety incidents been documented, analyzed and treated?
- **E13:** Has a thorough scenario analysis been performed for accidents, incidents and the effects of remote operations?
- **E14:** Has necessary training on remote operations been conducted?

Prior to the use of the CRIOP methodology, systematic risk analysis and scenario analysis related to remote operations was rarely performed. Furthermore, there was a lack of awareness of information security incidents among control room personnel as well as actors from the participating organizations.

6. CheckIT Tool

Personnel involved in remote operations have a tendency to focus on technology, often at the expense of organizational and cultural issues [2]. The reliance on virtual organizations and the presence of vulnerabilities create the need for common risk perceptions and a safety and security culture [1] in the involved organizations in order to reduce risk.

The CheckIT [7] tool was developed to help organizations improve their safety and security cultures. The CheckIT questionnaire has 31 questions, each of which has three alternative answers corresponding to distinct cultural levels:

- **Level 1:** Denial culture
- **Level 3:** Rule-based culture
- **Level 5:** Learning/generative culture (application of best practices)

The goal is to rate an organization on a five-point numerical scale. The scale provides a normalized score for the organization, which makes it possible to compare results over time or between organizations.

Using CheckIT could be a challenge in a technology-driven industry; therefore, organizations should attempt to build support for the process among stakeholders and document short-term improvements along the way [9].

The first step in the CheckIT process is to identify key indicators and goals to be improved (e.g., number of security incidents). The next step is to perform an assessment of the safety and security culture using the CheckIT questionnaire to identify challenges. The challenges and areas for possible improvement should then be discussed by a group of stakeholders. Finally, the stakeholder group should agree on and implement the actions needed to achieve the goals.

The structure and layout of the questionnaire is inspired by the work of Hudson and van der Graaf from BP [5]. An example question is: "To what extent is experience used as feedback in the organization?" The following responses were provided to this question at each of the three major cultural levels:

- **Denial Culture (Level 1):** A large number of incidents are not reported. A database of serious incident reports exists, but it is incomplete and not useful. The system does not have open access. Management is not informed about serious incidents.
- **Rule-Based Culture (Level 3):** A database with detailed descriptions of incidents and near incidents exists and is used internally. Efforts are made to use the database actively, but it is not fully established as a useful tool.
- **Proactive/Generative Culture (Level 5):** A company's experiences and other companies' experiences are used to continuously improve the safety and security performance, as well as the performance of the industry as a whole. Interfaces are seen as an important learning arena. Simulators are used as a training tool to gain experience across interfaces and create understanding.

Some of the other CheckIT questions are:

- To what extent is senior management involved and committed to information security?
- To what extent are employees and suppliers involved in developing information security?
- To what extent are training and sharing of common stories appreciated?
- To what extent are information security incidents analyzed and used as learning experiences for all actors?
- To what extent is reporting of unwanted incidents appreciated?
- To what extent are incidents and accidents used to improve operations rather than blaming individuals?
- To what extent are rules and procedures continuously adjusted to reduce the risks related to ICT?
- To what extent are key personnel given extensive system insight?
- To what extent is there precise and good communication related to situational awareness?

Use of the CheckIT tool has demonstrated that vendors, suppliers and other members of virtual organizations must be more involved in information security. Furthermore, information security is often problematic in large-scale projects because of the tendency to incorporate security as an add-on. CheckIT has also shown that risk analyses of individual systems and integrated SCADA/ICT systems have not been performed. Finally, the use of the tool has highlighted the fact that information sharing of incidents and best practices is poor both

within and outside organizations. A CheckIT analysis can be completed in one to two days. However, improvements to the safety and security culture must be treated as an ongoing process.

7. Conclusions

Remote operations in oil and gas facilities increase system vulnerabilities and the likelihood of safety and security incidents. Oil and gas industry experts have identified three main challenges that impact safety and security: poor situational awareness, negative interactions caused by ICT traffic on SCADA systems, and virus/worm attacks.

Mitigating these risks requires a holistic approach that addresses technical ICT-based risks, organizational risks and risks related to human factors. Specifying baseline information security requirements and applying the CRIOP and CheckIT methodologies are promising approaches for addressing these different types of risks. These methods and guidelines are currently being implemented in the oil and gas sector with much success. Our future research will focus on obtaining quantitative evaluations of the impact of these strategies on the safety and security of remote operations in oil and gas facilities.

Acknowledgements

This research was supported by the Center for E-Field and Integrated Operations for the Petroleum Industry at the Norwegian University of Science and Technology (NTNU). We also acknowledge the participation of the Norwegian National Security Authority (NNSA) in the development of CheckIT.

References

[1] Advisory Committee on the Safety of Nuclear Installations, *Third Report of the Advisory Committee on the Safety of Nuclear Installations: Organizing for Safety*, Health and Safety Commission Books, Norwich, United Kingdom, 1993.

[2] S. Andersen, Improving Safety Through Integrated Operations, Master's Thesis, Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, Trondheim, Norway, 2006.

[3] R. Ask, R. Roisli, S. Johnsen, M. Line, T. Ellefsen, A. Ueland, B. Hovland, L. Groteide, B. Birkeland, A. Steinbakk, A. Pettersen, E. Hagelsteen, O. Longva and T. Losnedahl, Information security baseline requirements for process control, safety and support ICT systems, OLF Guideline No. 104, Norwegian Oil Industry Association (OLF), Stavanger, Norway, 2006.

[4] G. Chadwell, F. Leverenz and S. Rose, Contribution of human factors to incidents in the petroleum refining industry, *Process Safety Progress*, vol. 18(4), pp. 206–210, 1999.

[5] P. Hudson and G. van der Graaf, Hearts and minds: The status after 15 years research, *Proceedings of the SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production (SPE 73941)*, 2002.

[6] S. Johnsen, C. Bjorkli, T. Steiro, H. Fartum, H. Haukenes, J. Ramberg and J. Skriver, CRIOP: A scenario method for crisis intervention and operability analysis (www.criop.sintef.no/The%20CRIOP%20report/CRIOP Report.pdf), 2006.

[7] S. Johnsen, C. Hansen, Y. Nordby and M. Line, CheckIT: Measurement and improvement of information security and safety culture, *Proceedings of the International Conference on Probabilistic Safety Assessment and Management*, 2006.

[8] S. Johnsen, M. Lundteigen, H. Fartum and J. Monsen, Identification and reduction of risks in remote operations of offshore oil and gas installations, in *Advances in Safety and Reliability (Volume 1)*, K. Kolowrocki (Ed.), Taylor and Francis/Balkema, Leiden, The Netherlands, pp. 957–964, 2005.

[9] P. Kotter, *Leading Change*, Harvard Business School Press, Boston, Massachusetts, 1996.

[10] S. Luders, CERN tests reveal security flaws with industrial networked devices, *The Industrial Ethernet Book*, GGH Marketing Communications, Titchfield, United Kingdom, pp. 12–23, November 2006.

[11] D. McCafferty and C. Baker, Human error and marine systems: Current trends, *Proceedings of the Second Annual IBC Conference on Human Error*, 2002.

[12] Norwegian Oil Industry Association (OLF), Integrated operations on the Norwegian Continental Shelf, Stavanger, Norway (www.olf.no/?22894 .pdf), 2004.

[13] Norwegian Petroleum Directorate (NPD), The NPD's fact pages, Stavanger, Norway (www.npd.no/engelsk/cwi/pbl/en/index.htm).

[14] Petroleum Safety Authority (www.ptil.no/English/Frontpage.htm).

[15] K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security – Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.