Chapter 12

MITIGATING ACCIDENTS IN OIL AND GAS PRODUCTION FACILITIES

Stig Johnsen

Abstract Integrated operations are increasingly used in oil and gas production facilities to improve yields, reduce costs and maximize profits. They leverage information and communications technology (ICT) to facilitate collaboration between experts at widely dispersed locations. This paper discusses the safety and security consequences of implementing integrated operations for oil and gas production. It examines the increased accident risk arising from the tight coupling of complex ICT and SCADA systems, and proposes technological, organizational and human factors based strategies for mitigating the risk.

Keywords: Oil and gas production, integrated operations, accident mitigation

1. Introduction

This paper discusses the safety and security consequences of using integrated operations for oil and gas production. Integrated operations leverage modern information and communications technology (ICT) in planning, organizing and performing tasks. The goal is increased value creation through collaboration across disciplines, corporations and geography [1].

The implementation of integrated operations is a large-scale change process involving technology, human resources and organizational factors. It is leading to organizational changes and new work processes both onshore and offshore. Significant segments of operations are being moved to a geographically distributed network where the actors are from a variety of organizations, reside in different locations and are interconnected by ICT systems. A key technological challenge is to integrate ICT and SCADA systems so that real-time data can be shared by the various actors and organizations.

This paper presents the results of a theoretical investigation and interviews with key personnel from the Norwegian oil and gas industry. In particular, it focuses on the increased risk of "normal accidents" due to the complexity

Please use the following format when citing this chapter:

Johnsen, S., 2008, in IFIP International Federation for Information Processing, Volume 290; *Critical Infrastructure Protection II*, eds. Papa, M., Shenoi, S., (Boston: Springer), pp. 157–170.

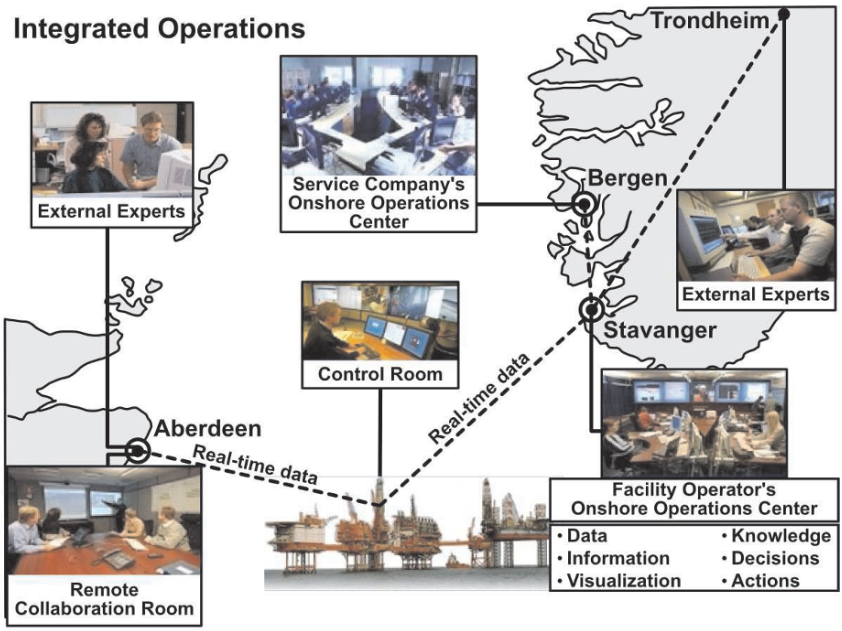

Figure 1. Interconnectivity and actors involved in integrated operations.

and tight coupling of ICT and SCADA systems. It also examines the theory of normal accidents [10] and related work in resilience engineering and high reliability organizations.

Our hypothesis is that the safety and security of integrated operations can be improved by focusing on resilience and performing mitigating actions that reduce the probability of normal accidents. We also argue that it is important to analyze, report and share incidents based on perspectives involving organizational, human and technical factors.

2. Integrated Operations

Integrated operations are attractive because they reduce costs, increase income and improve the yield from oil and gas fields. Several operations and maintenance tasks are being outsourced and this trend is likely to increase. Integrated operations provide for better utilization of expertise, facilitating interactions between professionals at widely dispersed sites. The increased connectivity, geographical distances, outsourcing and use of suppliers lead to a network of actors, which by accident, misunderstanding or intention can cause unforeseen incidents or accidents that could result in significant economic loss, environmental damage and casualties.

Figure 1 shows the interconnectivity and principal actors involved in integrated operations. The trend has been to move from teams located near the operational environment to large-scale remote operations. In remote operations,

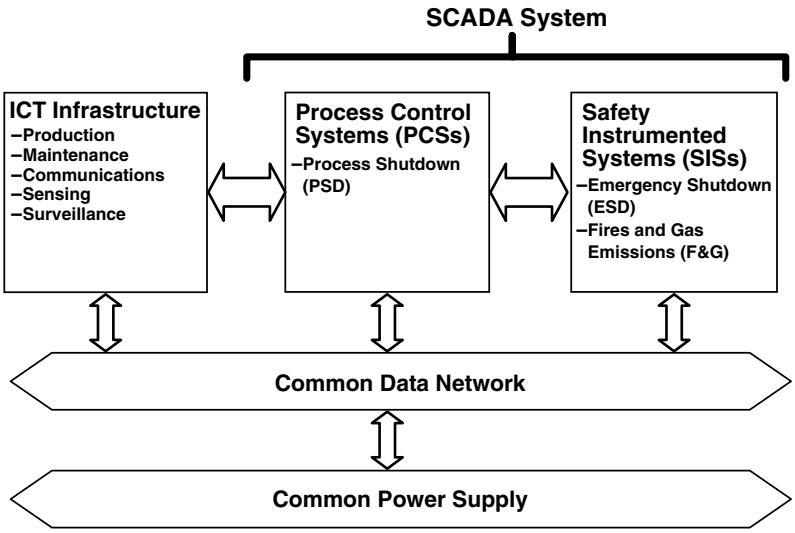

Figure 2. Systems used in integrated operations.

most team members may not be located at the site of operations, eliminating personal contact with other workers and the awareness of operating conditions (e.g., sound of mechanical equipment and smell of leaking gas) and environmental conditions (e.g., storm or calm). This situation poses great challenges because technical expertise and situational awareness must be shared to conduct production operations and to avoid incidents and accidents. Thus, it can be very difficult to maintain the safety and security of integrated operations.

The technologies used to manage production are changing from proprietary stand-alone systems to standardized IT systems and networks, which are often connected to the Internet. The standardization and increased interconnectivity of production systems, SCADA systems and ICT infrastructures increases the likelihood of undesirable incidents. Indeed, there has been an increase in the number of incidents related to SCADA systems, but the incidents are seldom reported. The incidents range from reduced production at oil and gas platforms to significant health, safety, security and environmental (HSSE) events. A production stoppage of just one day at a Norwegian Continental Shelf facility can result in a loss of two to three million dollars.

Figure 2 presents the major technical systems used in integrated operations. They include the ICT infrastructure, process control systems (PCSs) and safety instrumented systems (SISs). The ICT infrastructure consists of networks and supporting systems used for production (e.g., SAP), maintenance, communications (telephones and videoconferencing systems) and sensing and surveillance (radar and CCTV). PCSs are used for production; they include sensors and process shutdown (PSD) systems. SISs are used for emergency shutdown (ESD) and to deal with fires and gas (F&G) emissions. PCSs and SISs are collectively called "safety and automation systems" or SCADA systems.

We define an undesirable incident as one that leads to a loss of availability or integrity in ICT or SCADA systems. The incident may reduce or disrupt oil and gas production or may have a health, safety, security or environmental impact.

3. Accidents in High Reliability Environments

This section examines several theoretical studies in an attempt to identify the challenges and the mitigating actions used to improve safety and security in integrated operations. In *Normal Accidents: Living with High Risk Technologies* [10], Perrow explored the effects of system interaction and coupling and their impact on safety. When the interactions between systems are complex and the couplings tight, Perrow argued that an accident could represent the "normal" outcome. This perspective is relevant because integrated operations lead to increased complexity and increased coupling. Perrow's theory is based on "What can go wrong," but it is also useful to consider "What goes right."

The study of high reliability organizations (HROs) is beneficial in this context. HROs are entities that have (or are required to have) very few incidents and accidents. The three original HRO entities in the United States were the air traffic control system, nuclear power stations and U.S. Navy nuclear aircraft carriers. U.S. Navy nuclear aircraft carrier operations are based on the assumption that errors have catastrophic consequences. In general, the carriers have managed their tasks well despite the technical complexity and the pressure to perform [12].

HROs may be defined (somewhat imprecisely) as "hazardous systems that produce near accident-free performance" [9]. It is difficult to use the available data to support the claim of near accident-free performance in HROs. Nevertheless, it is recommended that the oil and gas industry strive for near accident-free performance in integrated operations.

Resilience is also an important concept in the context of integrated operations. Resilience is "the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress" [4].

Perrow defines two dimensions of normal accidents, "interaction" and "coupling." Interactions between systems range from linear (expected or familiar sequences) to complex (unexpected or unfamiliar sequences). Complex systems are characterized by proximity, common mode connections, interconnected subsystems, limited substitution, feedback loops, multiple and interacting controls, indirect information and limited understanding. A goal for integrated operations should be to design systems whose interactions are closer to linear than complex.

Coupling between systems ranges from loose to tight. Loosely coupled systems have flexible performance standards and can handle failures, delays and changes without destabilization. Tightly coupled systems have no buffering; consequently, what happens in one system directly impacts the other. These systems cannot accommodate delays in processing. They are characterized by

invariant sequences and little to no slack with respect to supplies, equipment and personnel. A goal in integrated operations should be to design systems that have tight coupling as opposed to loose coupling (e.g., by incorporating buffers and redundancies). Also, it is important to ensure that loosely coupled systems do not drift to tightly coupled systems due to breakdowns in buffering or loss of redundancy.

Empirical investigations of HROs have identified several key characteristics [9, 12]. HROs generally operate in environments with the potential for conflicting goals; however, when there is an absolute safety commitment from the top, conflicting goals are prioritized to ensure safety. HRO operations are distributed, but there is a focus on shared beliefs and values among the distributed teams; good communication among team members is critical. Public attention focused on HROs ensures that the key actors are always alert. Also, there is a strong focus on proactive learning about accidents and dormant faults. HROs generally have relatively abundant resources to deal with change; however, the organizations should be flexible and should handle unplanned activities in a safe manner. The organizations operate under the assumption that no individual is perfect; organizational redundancy is maintained in key areas. Although a high degree of system complexity and tight coupling exist, there is extensive system insight and errors are not tolerated.

Ideals such as commitment to safety should be communicated from top management when integrated operations are implemented. The distributed environment requires the establishment of common shared values and beliefs among actors. The two issues are also an important part of a safety and security culture [11]. Communication must be tailored to all the groups within and outside the organization.

Extensive system insight is a mitigating factor [10] as limited understanding often contributes to incidents in complex systems. Proactive learning is an excellent way to gain system insight and maintain readiness. Every undesirable incident should, therefore, be reported and analyzed to foster learning by the various actors. To avoid incidents and accidents, it is important to be ever alert and to avoid complacency. Errors should not be tolerated in tightly coupled systems; this helps ensure a preoccupation with failures [15].

Reason [11] describes four components of a safety culture: a just culture, a reporting culture, a learning culture and a flexible culture. Together, these four components create an informed environment where managers and operators have the most current knowledge about human, technical, organizational and environmental factors that determine the safety of the system as a whole. A just culture fosters an atmosphere of trust where personnel are encouraged to provide essential safety-related information, and a clear line exists between acceptable and unacceptable performance. A reporting culture encourages personnel to report their errors and near misses. A learning culture creates an environment where there is the willingness and competence to draw the right conclusions, and the will to implement major reforms when needed. A flexible

culture ensures that control passes to experts during a crisis and reverts to the traditional bureaucratic hierarchy when the emergency has passed.

Drawing on studies of HROs, Johnsen, *et al.* [7] have developed the CheckIT tool that attempts to measure and improve the safety and security culture through group-based discussions and actions. The idea is to improve the culture from one of denial to a rule-based culture to the ideal proactive reporting culture. Cultural improvements can be achieved in many ways; two key elements are management commitment and group discussions that nurture shared beliefs and values.

Weick [15] has identified five characteristics of HROs: (i) preoccupation with failures, (ii) reluctance to simplify, (iii) sensitivity to operations, (iv) commitment to resilience, and (v) deference to expertise.

- **Preoccupation with Failures:** Long periods of accident-free operations often breed complacency, but it is during these periods that one should be preoccupied with potential failures. HROs scrutinize incidents and search for possible errors because they may provide signals of precursors to larger failures. Turner [14] notes that a major disaster is often preceded by several serious incidents that are ignored due to complacency. Research in the area of safety also makes the same claim (see, e.g., [11]). An important aspect is a reporting culture where personnel report errors, near misses and unsafe acts. This culture is important in integrated operations because of the dependence on technical systems. Unfortunately, there is very limited reporting of ICT and SCADA incidents by the oil and gas industry [5]; this may increase the risk to integrated operations.

- **Reluctance to Simplify:** Simplification increases the likelihood of surprises because key details are overlooked or ignored. It is important to obtain accurate information and create a mental model that is complete and nuanced. In HROs, redundancy in personnel and systems are treated as vital for collecting and interpreting information that is necessary to avert disasters. In a complex environment such as integrated operations, it is important to establish a redundant set of communications systems.

- **Sensitivity to Operations:** In HROs, the entire workforce strives to maintain situational awareness, to understand what can go wrong and how to recover when things go wrong. HRO personnel attempt to maintain a perspective of the entire situation, not just the segments for which they are responsible. In integrated operations, situational awareness must be shared among all the relevant actors in the virtual organization and should be leveraged when incidents occur.

- **Commitment to Resilience:** HROs anticipate errors and are not disabled by them because they can quickly mobilize themselves to deal with errors. This should be a goal for integrated operations that is generally achieved by extensive training using realistic scenarios.

- **Deference to Expertise:** In critical situations, decision-making tasks often migrate to personnel with the most expertise, even if they are low in the organizational hierarchy. Learning activities must be supported throughout the organization. During an incident, decision-making power should be transferred to personnel who are the most knowledgeable.

Decisions and their premises must be evaluated and explored in a learning environment where the guiding variables are questioned and adjusted [2]. Second-order learning [2] should be explored when implementing integrated operations. This is because experience must be built continuously when new technology is implemented and the guiding variables influencing the organization should be continuously monitored and adjusted.

Resilience [4] requires that an organization be constantly watchful and ready to respond. Also, the organization should continuously update its knowledge, competence and resources by learning from successes as well as failures. Several issues should be considered in order to design for resilience.

- **Looking Ahead:** This involves anticipation (knowing what to expect) as well as looking for threats and having a constant sense of unease.
- **Looking Out:** This involves constant attention to detail, looking at performance indicators, having the time to think and perform actions.
- **Responding:** This involves effective response, maintaining plans, procedures, resources, readiness and flexibility.
- **Learning:** This involves knowing what has happened, having reporting schemes and accident models, and focusing on communication and feedback.

The studies we have examined provide a foundation for discussing the safety and security of integrated operations. The principles discerned from our study are listed below. Note that the principles overlap in many respects and, thus, appear to validate each other.

- Commitment to safety and security must come from the top; safety and security are goals.
- Focus on communication; establishment of shared beliefs; reluctance to simplify.
- Focus on proactive learning; preoccupation with failures; creation of a reporting culture.
- Commitment to resilience; importance of being alert and responding appropriately; flexible organizations.
- Extensive system insight; sensitivity to operations; focus on interactions ranging from simple to complex.

- No complacency related to coupling; avoidance of drift from loose coupling to tight coupling; implementation of necessary buffers and barriers; non tolerance of errors.

It is difficult to prove that these principles lead to error-free operations. Nevertheless, it is clear that in practically every incident or accident, one or more of the principles mentioned were violated.

4. Accidents and Integrated Operations

The consequences of an accident in the oil and gas industry can be very serious. The 1988 fire at the Piper Alpha production platform on the North Sea, which was caused by an oil and gas leak, resulted in the loss of 169 lives.

Production processes involved in integrated operations are complex and tightly coupled. Offshore oil and gas production, in particular, is highly complex. The complexity is increased by the presence of interconnected systems with unintended feedback loops and multiple, interacting controls.

Oil and gas production processes are also tightly coupled. They are based on invariant sequences, delays are unacceptable, and there is often only one method to achieve the goal. However, it is possible to shutdown the production process using at least two independent systems, the process shutdown (PSD) system that completely shuts down production, and the emergency shutdown (ESD) system.

Three main subsystems are used to manage production, the ICT infrastructure, PCSs and SISs. Our interviews with operators and suppliers have revealed that ICT systems, PCSs and SISs often use common networks and power supplies. PCSs and SISs also share the same operator interfaces on workstations (HMIs). Moreover, when PCSs and SISs are delivered by the same supplier, the systems have many common elements and are very tightly integrated.

PCSs and SISs are interconnected with ICT systems in order to obtain real-time production data and to perform control actions. It is often the case that failures in ICT components disrupt PCSs. In one incident on a North Sea platform, a malfunctioning computer system flooded a network with error packets, which caused the PCS to crash [5]. In fact, according to data from CERN [6], unanticipated ICT traffic could cause as much as 30% of SCADA network components to malfunction. The interconnections between ICT systems, PCSs and SISs are seldom tested or certified. A dangerous situation can arise if an SIS is rendered non-operational due to erroneous ICT traffic. This may cause the ESD to be locked, leading to a serious accident.

The scenario we used to explore what could happen in a production system is based on a real incident where a supplier connected a laptop infected with a virus to a production network. We applied the STEP methodology [3] to describe this scenario:

- **Actors:** The actors involved in the incident are identified. These actors are drawn under each other on the left-hand side of the STEP diagram (Figure 3).

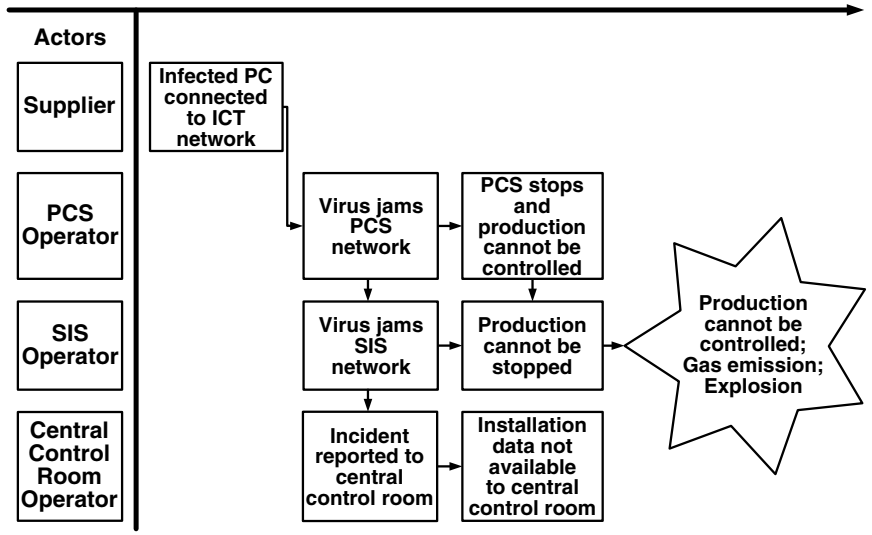

Figure 3. STEP diagram for a SCADA scenario.

- **Events:** The events that influenced the incident and how it was handled are identified. The "who," "what" and "how" of events are described. The events are placed in the correct locations of the time-actor sheet.
- **Causal Links:** The relationships between events and their causes are identified. Causal links are expressed in the diagram by drawing arrows between the events.

The STEP diagram is analyzed to identify the weak points. Next, barrier analysis is performed to identify the (existing and missing) barriers that hinder the root causes and threats, as well as the (existing and missing) barriers that reduce negative consequences and impacts.

Analysis of the STEP diagram in Figure 3 identifies several weak points and actions and barriers associated with the weak points:

- **Virus Scanning:** All computers must be scanned for viruses and other malware before being connected to the network. A staging facility must be used to scan the computers. Personnel should take steps to ensure that viruses and other malware are not introduced into computers and networks.
- **Patch Management:** All computer systems, software and network components should have the latest patches.
- **SIS-PCS Connectivity:** A firewall should be positioned between an SIS and PCS.
- **SCADA System Expertise:** Detailed documentation and training about SCADA systems and their operation should be provided to techni-

cal personnel to ensure that they can manage normal operations as well as crisis situations.

Integrated operations require a variety of systems to be interconnected and large amounts of information to be shared. ICT and SCADA systems are integrated, and some subsystems have common mode connections. In general, the implementation of integrated operations renders the overall system more complex than linear.

The couplings between ICT and SCADA systems are such that delays are undesirable, mainly because real-time data is required to manage production. Typically, there are at least two independent ways of shutting down production (PSD and ESD).

The integration of ICT and SCADA systems results in the overall system becoming more complex and more tightly coupled, which increases the probability of normal accidents. This probability can be lowered by reducing the complexity of system interactions and by reducing tight coupling.

The following actions can be taken to reduce system complexity:

- **Common Mode Connections:** Common mode connections should be reduced by separating networks, system components and power supplies. The separation of PCSs and SISs should be mandatory, but this is seldom enforced and the status of common faults is rarely explored.

- **Interconnected Systems:** Systems have to be interconnected in order to share information, but the interconnections should be simplified to the extent possible. For example, "one-way" connections could be established for data exchange. Also, data exported from SCADA systems to ICT components should be designated as read-only to enhance security. Furthermore, changes to SCADA data should be implemented using redundant systems with human intervention and/or supervision.

- **System Understanding:** It is important to establish a good understanding of the systems used in integrated operations. ICT and SCADA systems should undergo comprehensive testing and evaluation under normal and abnormal scenarios, including virus infections and denial-of-service attacks. Information collected about systems and incidents should be disseminated to improve understanding and awareness.

The following actions can be taken to reduce tight coupling between systems:

- **Processing Delays:** The need for real-time data should be critically evaluated. Processing delays should be introduced, if possible.

- **Equipment and Personnel:** The introduction of slack with regard to equipment and personnel should be explored. Additional resources may be needed to provide slack.

- **Redundancy:** Redundancies may be incorporated (e.g., independent shutdown systems) to reduce tight coupling. It is important that the redundant systems are tested regularly.

5. Interview Results and Mitigating Actions

We interviewed personnel from several large oil and gas companies in Norway to identify the key issues relating undesirable incidents in ICT and SCADA systems used in production. Several incidents involving virus and worm infections occurred annually. However, these incidents mainly affected ICT systems. In installations implementing integrated operations, there was at most one incident each year that impacted offshore SCADA networks.

In practically every installation, ICT and SCADA professionals belong to different parts of the overall organization; they have different educational backgrounds and apply different standards and methods. For example, ICT personnel adopt standards such as ISO/IEC 27002 (Information Technology – Code of Practice for Information Security Management (formerly ISO/IEC 17799)). On the other hand, SCADA personnel comply with the IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems) and ISA SP99 (Manufacturing and Control Systems Security) standards.

Our interviews with industry experts have identified several key safety and security issues along with mitigating actions:

- **Incident Reporting:** Incidents are seldom reported or analyzed. There does not appear to be an open reporting culture; information about undesirable accidents is not shared with and between organizations. Clearly, incidents should be analyzed thoroughly and disseminated using a standardized reporting scheme that documents all the major issues. Key actors such as the control room operators should be alerted to incidents as they happen. Proactive scenario analyses, as illustrated by the STEP diagram in Figure 3, should be explored. These analyses should be used to raise incident awareness and develop mitigation strategies.

- **Technical, Organizational and Human Factors Issues:** Unwanted incidents are regarded as technical issues; organizational and human factors issues are rarely considered. ICT and SCADA professionals adopt different standards and practices. Clear responsibility, unambiguous work procedures and common situational awareness are important when incidents develop into dangerous situations. Common situational awareness must be maintained under normal operations as well as during incidents. It is important to focus on organizational and human factors issues such as common goals, beliefs and values. Incidents should be analyzed and reported using a standardized scheme that documents technical, organizational and human factors issues.

- **Probability of Normal Accidents:** Implementing integrated operations increases the probability of normal accidents. ICT and SCADA have different architectures, and SCADA systems are vulnerable to unanticipated ICT traffic. The integration of ICT and SCADA systems results in shared networks, power supplies and operator interfaces for ICT, PCS and SIS systems, leading to common cause failures. Integrated systems

are rarely tested and certified for independence and resilience. It is important to perform thorough testing and certification of all systems, and to ensure that all normal accident scenarios are reported and analyzed.

Based on our analysis of the theory and interactions with industry experts, we have identified several barriers that should be explored during accident analysis. The following questions should be considered as a starting point when identifying the barriers in an organization:

- **Organizational Barriers:** Is there a management commitment to safety and security from the top of the organization? Has an open reporting culture been established among operators and suppliers? Has a risk assessment been performed for process control, safety and ICT systems and networks? Has a practice been established for remote access that ensures human supervision from the central control room? Has an incident handling team been established and has a short, precise incident handling plan been established? Is there clear responsibility for ICT/SCADA network operations? Are there procedures in place for reporting security and safety incidents? Has a scenario analysis been performed between the operator and suppliers? Have all incidents been documented and analyzed by teams with the relevant actors?

- **Technical Barriers:** Have proactive indicators been established to indicate the level of attacks? Have the interconnections between ICT and SCADA systems been tested and certified, and has the SCADA network been tested and certified for ICT traffic? Have firewalls been implemented based on a best practice scheme and are firewall logs analyzed systematically? Do the process control, safety and ICT systems have adequate, updated and active protection against malware?

- **Human Factors Barriers:** Have all the involved actors been informed about relevant incidents and have there been open discussions about incidents and vulnerabilities in the various systems? Has an analysis of safety culture (knowledge, awareness and actions) been performed among the relevant actors? Have suppliers and other operators been educated about information security requirements, do they know how incidents should be handled and do they know about acceptable ICT system use and operations?

6. Conclusions

The implementation of integrated operations in oil and gas production facilities in the Norwegian Continental Shelf has contributed to increased complexity and tight coupling between ICT and SCADA systems. Our research has identified three areas of concern: the increased probability of normal accidents due to the integration of ICT and SCADA systems, the inadequate reporting and analysis of ICT and SCADA incidents, and the designation of undesirable incidents

as technical issues that are rarely analyzed in the context of organizational and human factors issues.

Normal accidents can be mitigated by building resilient systems and creating high reliability organizations. This can be accomplished by developing defensive strategies and performing barrier analyses that consider human factors, organizational factors and technical solutions. Incident reporting is also critical; strong efforts should be undertaken to document, analyze and share information about incidents among the various actors.

References

[1] K. Andersen, IO in StatoilHydro – Drilling and well, presented at the *Forum for Human Factors in Control* (www.criop.sintef.no/Participants%20and%20projects/0–HFC%20-%20M%C3%B8tereferat%20april%2008.pdf), 2008.

[2] C. Argyris and D. Schon, *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley, Reading, Massachusetts, 1978.

[3] K. Hendrick and L. Benner, *Investigating Accidents with STEP*, Marcel Dekker, New York, 1986.

[4] E. Hollnagel, D. Woods and N. Leveson, *Resilience Engineering*, Ashgate, Aldershot, United Kingdom, 2006.

[5] M. Jaatun, S. Johnsen, M. Line, O. Longva, I. Tondel, E. Albrechtsen and I. Waero, Incident Response Management in the Oil and Gas Industry, SINTEF Report A4086, SINTEF, Trondheim, Norway (www.sintef.no/upload/10977/20071212_IRMA_Rapport.pdf), 2007.

[6] S. Johnsen, R. Ask and R. Roisli, Reducing risk in oil and gas production operations, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 83–95, 2007.

[7] S. Johnsen, C. Hansen, M. Line, Y. Nordby, E. Rich and Y. Qian, CheckIT – A program to measure and improve information security and safety culture, *International Journal of Performability Engineering*, vol. 3(1), pp. 174–186, 2007.

[8] S. Johnsen, M. Lundteigen, E. Albrechtsen and T. Grotan, Trusler og muligheter knyttet til eDrift, SINTEF Report A04433, SINTEF, Trondheim, Norway (www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/STF38%20A04433.pdf), 2005.

[9] T. LaPorte and P. Consolini, Working in practice but not in theory: Theoretical challenges of "high-reliability organizations," *Journal of Public Administration Research and Theory*, vol. 1(1), pp. 19–48, 1991.

[10] C. Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, Princeton, New Jersey, 1999.

[11] J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot, United Kingdom, 1997.

[12] K. Roberts, New challenges in organizational research: High reliability organizations, *Organization and Environment*, vol. 3(2), pp. 111–125, 1989.

[13] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[14] B. Turner and N. Pidgeon, *Man-Made Disasters*, Butterworth-Heinemann, Oxford, United Kingdom, 1997.

[15] K. Weick and K. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, California, 2001.