Presented at the 5th International Conference on Autonomic and Trusted Computing, Oslo, Norway, June 23-25 2008 (Springer LNCS 5060)
https://link.springer.com/chapter/10.1007/978-3-540-69295-9_42

A Study of Information Security Practice in a Critical Infrastructure Application

Martin Gilje Jaatun[1], Eirik Albrechtsen[2], Maria B. Line[1], Stig Ole Johnsen[2], Irene Wærø[2], Odd Helge Longva[1], Inger Anne Tøndel[1]

[1] SINTEF ICT, NO-7465 Trondheim, Norway
{Martin.G.Jaatun, Maria.B.Line, Odd.H.Longva, Inger.A.Tondel}@sintef.no
[2] SINTEF T&S, NO-7465 Trondheim, Norway
{Eirik.Albrechtsen, Stig.O.Johnsen, Irene.Waro}@sintef.no

Abstract. Based on multiple methods we have studied how information security practices, and in particular computer security incident response practices, are handled in the Norwegian offshore oil and gas industry. Our findings show that there is still insufficient awareness regarding the importance of information security in the offshore industry, and that increased vigilance is required in order to respond to mounting threats of tomorrow.

Keywords: Incident Response Management, Information Security, Process Control, Security Practice

1 Introduction

During the last years the concept of Integrated Operations (IO), i.e. use of information technology and real-time data to operate petroleum processes, has been implemented in the oil and gas industry on the Norwegian Continental Shelf [1]. This implies that new technologies and new ways of working and communicating are implemented to create remote operations, control and support; e.g. through merging ICT systems and Supervisory Control And Data Acquisition (SCADA) systems. This development is still in progress, and the integration of industrial processes, technology and different actors is likely to continue and even tighten up in the years to follow. On the one hand, integrated operations represent a major opportunity for increased and more efficient production and reduced operational cost as well as improved safety performance [1]. On the other hand, implementation of new and supplementary information systems increases the systems' vulnerability to breakdowns due to information security breaches. Breaches can lead to consequences such as production stops; disabling of critical safety barriers and problems of providing oil and gas to customers [2]. It is thus necessary for the petroleum industry to implement adequate information security measures to contribute to a stable production and sale as well as safety for its employees.

This paper gives a picture of information security practices in the Norwegian oil and gas industry by presenting empirical findings from the research project "Incident

Response Management" (IRMA), funded by the Research Council of Norway and the Norwegian Oil Industry Association.

The IRMA research project developed a framework for incident response management [3]. The management framework includes the following three phases (see Fig. 1): prepare (planning and preparation of incident response); detect and recover (detection of incidents and restoration to normal operation); and learn (experience sharing and learning afterwards). There are several standards and good practice documents that describe incident handling (e.g. [4, 5]). The management system developed in IRMA differs from the traditional incident handling approaches in two ways: It focuses on both reactive and proactive learning; and it is tailored to the oil and gas industry.

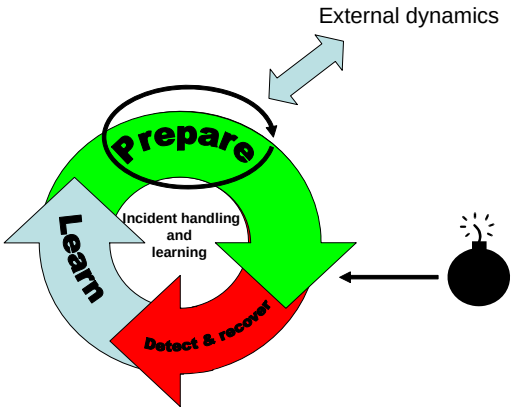

Fig. 1. Incident Response Management Phases

The complex processes of oil and gas producing installations are monitored and controlled by Supervisory Control And Data Acquisition (SCADA) systems which are traditionally operated by personnel with a different background than administrators of traditional computer systems. This implies that there is a situation of disparate cultures that also results in information security challenges.

The paper is structured as following: Section 2 presents the empirical sources and methods we have used, section 3 presents our findings, which are discussed further in section 4, while section 5 concludes and summarises our study.

2 Empirical Sources and Methods

The development of the incident response management (IRMA) framework for the petroleum industry presented in Jaatun et al. [3] required a combination of different empirical sources of information security practices in this industry:

- An interview study with key personnel in the Norwegian oil and gas industry
- A case study of incident response management practice at an oil and gas installation in the North Sea

- A risk and vulnerability assessment of infrastructure and work processes at an offshore installation
- A study of cultural aspects of information security by using a tool for assessing information security culture at a particular installation
- A workshop on information security and integrated operations
- A workshop on the main findings of IRMA in the Norwegian offshore industry
- System dynamic workshops

In addition, the IRMA project team has been represented in Norwegian Oil Industry Association's (OLF) workgroup on information security for the entire duration of the project. The workgroup meetings have provided the project with important background information and firsthand access to operator and contractor personnel who are actively involved with offshore safety and security work. The workgroup meetings have also been used to discuss preliminary results from IRMA, and have provided us with useful feedback. Furthermore, the fact that we had contributed to the workgroup meetings made it significantly easier to recruit participants for our workshops and interviews.

Although the empirical studies had a main emphasis on incident handling, other parts of information security were also uncovered during the study, which are presented in the subsequent sections.

The bulleted list above also shows that a combination of different qualitative social science methods was used for collecting information about information security practices in the oil and gas industry. Information security practices in this particular industry have previously not been the subject of many research attempts. In that way, qualitative research methods proved to be a good methodological approach due to the explorative nature of qualitative research. In general, qualitative research provides understandings of social phenomena by proximate studies of the local contexts of the study [6]. By close interaction between researchers and informants, the researchers will get an understanding of the processes studied rather than only a description of the processes [7], which proved to be useful for the present study.

Qualitative research results should not be treated as generalized facts, but understandings of processes in the particular context of the study [6]. As a consequence, the findings presented in this paper are not necessarily generalized facts, but a representation of information security practices in the Norwegian oil and gas industry.

3 Findings

This section presents the main findings from the different data sources mentioned in the previous section.

3.1 Interviews

Nine interviews of personnel with knowledge and experience of information security in the oil and gas industry were conducted by phone in the period of March-June 2007. The interviews aimed at exploring how incidents were handled in the

Norwegian oil and gas industry, and were approached by looking at how incidents were practically dealt with and how the informants believed a best practice for incident response management should look like. The interviews were analyzed according to [8] by structuring the information in matrices and looking for patterns in the structured data (see [9] for a detailed result matrix).

In general, the interviews showed that the informants experienced very few information security incidents that have impact on production. It was assumed that it could be between one and two years between each incident.

Information security measures tend to have a main focus on technology. Technical issues are often covered exclusively, while there are seldom discussions of defenses in breadth; covering organisational and human factors in addition to technical issues.

There are many plans for different parts of incident response in the studied organisations, with different level of details. A short and common plan, documenting specific incident response management incorporated in the organisation, is missing among most of the interviewees. Scenario training, which is widely used in other loss prevention areas in the industry, for handling information security breaches is seldom performed. Furthermore, the interviews showed that individual awareness and proactive unrest related to information security could be improved. Knowledge and understanding of information security could be improved among employees, especially among suppliers.

The learning phase after an incident has occurred is considered to be important. However, some informants were worried whether learning actually had any effect for future activities, and feared that learning was quickly forgotten. The learning is thorough. Root causes are not always identified, discussions do not always involve information and communication technology (ICT) and process professionals together, and lessons learned are not published.

The interviewees' organisations' reporting systems are seldom tailored to information security, and there are often many different reporting systems, leading to a lack of a unified system for reporting incidents. The interviews also indicate a lack of frankness about real incidents. A change of focus is demanded in the industry to make experience transfer both inside the organisation and to external organisations possible.

3.2 A Case Study at an Oil and Gas Installation in the North Sea

In the early stages of the IRMA project, a case study at an oil and gas installation was performed. The case study aimed at describing how incident response management was performed in practice at a selected offshore installation. Interviews, meetings and document studies were used in the case study.

In general, the incident response management at the studied installation has a potential to be more systematic and planned, as the current management approach seemed scattered and randomly made. The study showed that the only incident handling procedure at the installation was a procedure for handling virus infections[1];

[1] This procedure was not immediately available at the start of the case study, and might actually have been developed as a result of our inquiry.

there were no other relevant procedures for incident response. There were some awareness-creating activities at the installation, which among other subjects also included information security. Our findings indicate that if there is a virus infection in the SCADA systems, it might take weeks before the infection is detected; even if the system is not operating normal.

When incidents happen, there is limited learning in the organisation from these incidents, and there is moderate communication within the organisation about real incidents.

3.3 Risk and Vulnerability Assessment

To gain more insight into ICT-related risks involved in integrated operations, a risk and vulnerability assessment was conducted based on the work process of daily production optimization of an offshore installation. Small-scale workshops with managers were performed to identify incidents and assess the risk of these incidents.

This assessment and the knowledge attained by analyzing the coupling and dependencies of ICT systems, vulnerabilities, responsibilities, possible consequences of various incidents and how incidents are usually detected and recovered, gave a basis for further work as well as implications for the assessed installation.

The most critical incidents identified in the risk assessment were: the operation centre goes down jamming the SCADA system; the SCADA system goes down; a virus/worm infects the system from external sources; and missing situational awareness from central control room operator.

The risk assessment suggested the following risk reducing measures relevant for incident response management: monitoring the stability of the SCADA equipment when it is integrated with ICT infrastructure; external PCs should be scanned and checked prior to being allowed in technical network or offshore network, or supplier should guarantee that the equipment are without viruses; incident reporting and learning from incidents should be improved; the responsibilities related to technical network and the integration of ICT/SCADA systems should be unambiguous and monitored; awareness, safety and security culture should be improved onshore and offshore; common risk assessment among the actors in the organisational network should be established and sustained; and emergency response plans should incorporate information security incidents.

3.4 Assessment of Information Security Challenges at an Installation

A tool for assessing organisational aspects of information security, Check-IT [10, 11], was used to identify some key challenges related to an integrated operation installation in a half-day workshop with ten managers and staff members. CheckIT consists of a set of questions regarding organisational aspects of information security, including alternatives for answers. Although it is a questionnaire, the questions are so open-ended that they function well for group discussions as well, which results in both an assessment of the current status as well as improved awareness among discussion partners.

The study showed that information security is not satisfactorily integrated in projects and new installations. Furthermore, suppliers and service providers are not satisfactorily involved in incident planning, detection and learning. The identification of critical ICT systems is not satisfactorily in developing integrated operations; HAZOP analysis [12] (risk analysis) of ICT/SCADA systems is seldom done.

Productivity goals are sometimes prioritized ahead of information security requirements, as rules and procedures related to information security are sometimes ignored in situations with conflicting demands.

In general, the personnel on offshore installations have a low level of awareness related to information security (e.g. regarding spyware and virus). This is partly explained by lack of communication of information security issues in the organisation. This lack of communication is also reflected in unsatisfactorily sharing of information security incidents between organisations in the industry.

3.5 Workshop on Information Security and Integrated Operations

A workshop on information security in integrated operations was arranged by the Norwegian Petroleum Directorate, the Petroleum Safety Authority Norway, The Norwegian Oil Industry Association (OLF) and SINTEF in November 2006 [13]. The workshop aimed at 1) creating awareness on information security in integrated operation among different organisational groups (ICT, Health, Safety, Security and Environment (HSSE), automation and operations); 2) creating an arena for experience transfer and networking; and 3) identifying possible measures. About fifty participants from the oil and gas industry, the power supply industry; public agencies and research institutions attended the workshop.

Several information security issues in integrated operations were discussed in parallel groups, including topics on incident response management. One result of the workshop was that there is a need for more measurement of information security (key performance indicators) to evaluate whether the security level corresponds to policies and regulations; to evaluate effects of measures and to integrate information security with other business areas. Such measurements should be with some kind of reference point, e.g. the OLF Information Security Baseline Requirements (ISBR) [14].

There is a lack of willingness to report incidents in the industry; as a consequence more work is needed to study how to develop a reporting culture; how to inform about incidents; and how to develop a best practice regarding reporting and handling of incidents. Routines for reporting, including feedback on the reports, should be simplified.

Training and preparedness for ICT-related incidents is lacking. The industry has traditionally trained on defined hazard and accident situation scenarios in other loss prevention areas. Such scenarios are however lacking for ICT-related incidents. Furthermore, the workshop indicated that there is a gap in communication between different groups of professionals offshore, i.e. HSSE, ICT and process. This is reflected by ICT routines that are not adjusted to the offshore reality.

3.6 Workshop on Main Findings from IRMA

In October 2007 some of the main findings on IRMA project in the offshore industry were discussed at a workshop. 15 participants from the industry, governmental agencies, consulting companies and research institutions participated at the workshop.

Regarding the plan phase of incident response management it was emphasized that incident response management must appear as a proactive management approach in order to be prepared to handle and learn from whatever incidents that may occur. In this proactive approach, performing risk analysis should be the foundation for providing decision support to how incident response management should be planned and performed.

In the detect and recover phase, it is important that those who discover or suspect an incident know who to notify. One must define possible incidents and then see which channels for reporting are the most efficient for those incidents, e.g. perform a risk analysis.

To be able to learn from incidents, structures for reporting incidents must be in place. A module for information security incidents is needed in applied software for reporting incidents. Contractors fill out a form, which is registered in the incident reporting tool Synergi[2] by someone else. It is a challenge that different parts of the organisation have different traditions for reporting incidents. For example that control room operators do not report incidents, since they only handle the consequences of incidents, not the incident itself.

The workshop participants felt that an information security forum for experience transfer in the oil and gas industry is an interesting idea, but the industry must decide what such a forum should be used for. It is important to include different professions in such a forum.

The workshop also discussed whether historical data on incidents is relevant for IRMA in integrated operations. New technology and new ways of organizing work may change the relevance of historical data.

3.7 System Dynamics Workshops and Cooperation with the AMBASEC Project

In 2005 the IRMA project team in collaboration with the AMBASEC[3] research project team, carried out two system dynamic workshops, The objective of the workshops were to reach a deeper understanding of present risks in the transition to integrated operations and the implications for incident handling in this transition. The processes included building a system dynamic model for a particular integrated operation installation.

The results from the workshops and the collaboration between IRMA and AMBASEC are documented in two reports [15, 16] and several scientific publications [17-20]. The areas of discussion included identifying key indicators and dynamic system stories to anticipate change in a system's state over time.

---

[2] http://www.synergi.com

[3] AMBASEC (A Model-based Approach to Security Culture) is a project funded by the Research Council of Norway, anchored at Agder University College (AUC – now University of Agder). AMBASEC has had a formal collaboration with IRMA.

In the first workshop, a preliminary version of a system dynamics model for the transition to integrated operations was established, and a set of stakeholders[4] and their influences on possible outcomes for security in IO were identified. Two dynamic stories were developed with the intent to show the relationship between operational change, security and the stakeholders: "Virus exposure in virtual organisations" and "The effect of the introduction of compliance mechanisms to suppliers and contractors."

Workshop attendees discussed a risk and vulnerability analysis for the work process "daily production optimization", and came up with different views on how work processes will develop in the future of IO.

Findings from the first workshop included:

- Monitoring risk change should be given high priority when developing new policies in the industry related to incident reporting, creating CSIRTs[5] and raising awareness.
- Transitions from traditional to integrated operations create vulnerabilities. The timing of these vulnerabilities may depend on how well the organisation is able to change its operating processes, train its staff and contractors, and gain acceptance of the transition.
- Successful implementation of collaborative arenas reinforces their effectiveness. On the other hand, limited success will likely slow acceptance of this innovation, and increase the resources required for subsequent rollouts, or possibly derail the project.
- The transition from existing to new work processes will introduce new security issues and potential for security lapses. These problems, if not detected and mitigated, are expected to increase the resistance to further change and adoption.
- Delays in learning and reflection may reduce the migration to integrated operations. Development of a capacity to detect problems and learn from them may facilitate future transitions. Conversely, a limited capacity to detect problems as they occur will obstruct change and delay corrections, increase risk, and put the project at greater peril.

The second workshop was focused on the implementation of a new workprocess in the Brage oilfield. Simulation on the SD-model where the parameters were adjusted by the experts from Hydro brought forward a set of hypotheses:

- Maturation and adoption of technology enables work processes and transformation.
- Introduction of new technologies and work processes can create knowledge gaps and vulnerabilities.
- More communication off-platform reduces resistance to change, which enables adoption of mature processes.
- Incident reporting creates a stock of knowledge of incidents, which allows us to bring on mature work processes and improves rate of getting mature technology online, reducing vulnerabilities, incidents and damage.

[4] Examples of stakeholders are oil company (system owner), chief executive officer, platform chief, control room manager, incident response team manager, Ptil, media etc

[5] Computer Security Incident Response Team

While the effects of this work on the proposed integrated operations migration are not by any means clear, the group model building process achieved several important outcomes for the participants. The qualitative models identified several problematic areas in the transition. The potential for a Knowledge Gap and a Work Process gap reinforced the importance of timing and knowledge sharing. The long-term effectiveness of CSIRT activity on the ability of the firm to develop a strong security culture is dependent upon a move beyond damage repair and into active learning.

From a methodical perspective, the results had two additional important outcomes: Group model building engaged and focused a diverse set of experts and modellers to develop a holistic, systems view of a problem. This was particularly gratifying given the initial skepticism expressed during the planning of the meeting. Through the feedback models, a wide set of interrelationships emerged that influence the success or failure of both the integrated operations and the CSIRT initiatives. Though little hard data was available, the participants' knowledge of the general structures and behaviours in their environment was sufficient for credible and understandable causal modelling. This is a crucial finding in high-threat environments, as little data is ever made available outside the secure environment of the firm.

The state of information security in this domain is still relatively immature when compared to the state of safety. In the realm of safety there are numerous reporting systems, often mandated by law or if not directly by law, by high political pressure. Perhaps we will not see well-functioning incident reporting systems for information security before government intervenes or threatens to do so. Another reason for the relatively slow adaptation of incident reporting systems may be the singular focus on information security as a technical issue. Non-security personnel are often kept completely out of the loop and are instead presented with a set of prescribed rules. However, this is a limited approach to user education. Users must be kept 'in the loop'; only then will they see the necessity and usefulness of following the rules prescribed by information security specialists.

Simulation runs on the SD-model illustrate the potential for a successful incident reporting system. However, they also show that there is potential for partial or even complete failure if important factors, such as the quality of investigations and motivation, are not handled well.

4 Discussion

Traditionally, there has been, and still is, a greater focus on *safety* than on *security* in the offshore industry. This is due to the fact that the process control systems used to be proprietary, and the set of security threats applicable was clear and not very large, while working conditions for the people posed a greater overall threat to their lives.

4.1 Few Incidents are Observed

A general view in the industry is that there are few information security incidents occurring. A majority of employees therefore do not see why having a plan for incident response is important. It is perceived more as an unnecessary and expensive

hassle than an efficient measure which may save lots of time and money the day something happens.

It is claimed within the industry that loss of money is acceptable as long as no lives are lost. However, an offshore installation in full production generates so much money, that it is hard to believe that loss of money really is of no concern.

Because of the lack of a complete method for incident response, how can it be stated that not many incidents occur? In meetings where IT staff and process control staff have been together, we have seen several times that one of the groups have revealed stories about incidents that up till then was unknown by the other one. Communication of incidents seems to be absent, and also the ability to discover incidents can be questioned. This leads us to conclude that improved indicators for information security are needed.

4.2 Combining Two Different Worlds

Regarding the two groups IT staff and process control staff, there is clearly a gap between them which may pose great security challenges. This is especially relevant now when process control systems change from being nearly completely proprietary, or at least not connected to any external networks, to include more commercial off-the-shelf hardware and software and being connected to the Internet, although with several layers of security mechanisms. Where process control staff used to be in total control and manage their systems without any help from IT staff, there is now need for a close interaction where IT staff need to manage and maintain systems in production. This requires a mutual understanding for each other's fields of expertise. In the world of the IT staff, computers crashing from time to time are normal; rebooting is sometimes necessary and often this also fixes the problem; and installing patches can usually be done at any time. In the world of the process control staff, keeping the production systems running without interruption is crucial, as a system crash may result in stop in production, which again leads to loss of money. This means that patches should not be installed before there is a 100% certainty they will work without any compatibility problems. Rebooting computers may be the same as stop of production as well as disable safety systems. And backup systems are rarely tested, if at all, because what if they do not work? These different mindsets can be explained by different objectives in the loss prevention approaches [21]. The IT world typically sees confidentiality and data integrity as the main objective, while the industrial control systems aim at system availability and data integrity to ensure plant safety and occupational injury prevention.

It is a challenged to combine the mindsets of IT staff and process control staff is a in a successful way, but collaboration between them is necessary. This means that there is a need for communication and skills development for both groups of people. To integrate different perceptions of risk and risk mitigation, Klinke and Renn [22] suggest a discourse-based management approach where the involved actors interact and discuss risk issues. Workshop methods such as seek conferences and focus groups might prove useful for this purpose.

4.3 Learning Based on Few Incidents

As long as we do not have proof of anything else, we need to base our work on the perceived fact that few incidents actually occur. However, as we believe that this will change in the near future, with the ongoing transition to integrated operations and the use of new technologies, we see a clear need for improvement of incident response management. First and foremost, having a plan for how to deal with different kinds of incidents, including reporting procedures and responsibilities, is a good starting point. A greater challenge is how to implement learning of incidents as there are so few to learn from.

Sharing experiences and knowledge between companies within the same industry is a good way of gathering information about incidents which again can be used as a basis for learning. It is important that the employees can relate to the referred incidents, which can be achieved by collecting information from similar companies. A challenge in such cross-organisational learning is openness about the incidents. Embarrassing and threatening aspects is known to be major obstacles for learning [23] , most security incidents are in its nature threatening and embarrassing, so a a key challenge in future sharing of inexperience and learning is to create an environment for openness on these incidents. We see that the work group organized by OLF has succeeded in this type of information exchange. This group has now existed for three years, and is based on trust and openness. This has been a good first-step-on-the-way in improving communication about information security within the industry. However, in the long run it is not sufficient that only Chief Information Security Officers (CISOs) communicate. Information needs to be spread throughout a larger part of each company, and there must be communication present across company limits on several layers.

5 Conclusion

We have presented the findings of an empirical study of information security practices in oil and gas operations on the Norwegian Continental Shelf, with a special focus on computer security incident response. Our findings show that there is still insufficient awareness regarding the importance of information security in the offshore industry, and that increased vigilance is required in order to respond to mounting threats of tomorrow.

Further work is required in order to instill this sense of vigilance on the oil and gas industry. We believe that increased effort should be put into developing information security indicators that proactively can measure (lack of) security for these installations, including near-miss type of indicators. If the industry allows itself to get lulled into a sense of security based on the currently small number of perceived incidents, it risks getting swamped by a future deluge of attacks.

Acknowledgements

This research was supported by the Research Council of Norway and the Norwegian Oil Industry Association (OLF). The authors thank all participants of OLF's workgroup on information security, and in particular StatoilHydro, for their cooperation.

References

1. OLF, "Integrated Operations on NCS," Norwegian Oil Industry Association 2004, http://www.olf.no/?22894.pdf.
2. Albrechtsen, E. and Hovden, J., "Industrial safety management and information security management: risk characteristics and management approaches," presented at European Safety and Reliabilty Conference 2007 (ESREL 2007), Stavanger, Norway, 2007
3. Jaatun, M.G., et al., "Incident Response Management in the oil and gas industry," SINTEF Report A4086, Trondheim December 2007, http://www.sintef.no/upload/10977/20071212_IRMA_Rapport.pdf.
4. "ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management.," 2004.
5. Grance, T., Kent, K., and Kim, B., "Computer Security Incident Handling Guide," NIST Special Publication 800-61 2004, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.
6. Thagaard, T., Systematikk og innlevelse: en innføring i kvalitativ metode. In Norwegian [Systematic and insight: introduction to qualitative methods] Bergen: Fagbokforlaget, 2003.
7. Kvale, S., Det kvaliative forskningsintervju. In Norwegian [Interviews: an introduction to qualitative research interviewing]. Oslo: Ad Notam Gyldendal, 1997.
8. Miles, M.B. and Huberman, A.M., Qualitative Data analysis: an expanded sourcebook. Thousand Oaks, Calif, : Sage, 1994.
9. Albrechtsen, E., et al., "IRMA - Interviews on incident response in the oil and gas industry," SINTEF MEMO November 22. 2007.
10. Nordby, Y. and Hansen, C.W., "Informasjonssikkerhet – atferd, holdninger og kultur. In Norwegian [Information security – behaviour, awareness and culture] " NTNU-rapport ROSS(NTNU)200504. 2005.
11. Johnsen, S.O., et al., "CheckIT – A program to measure and improve information security and safety culture," International Journal of Performability Engineering vol. 3(1 Part II), pp. 174-186, 2007.
12. "Hazard and operability studies (HAZOP studies) - Application guide," IEC 61882, 2001
13. Jaatun, M.G., "Arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner: Referat (in Norwegian) [Minutes from Workshop on ICT Security in IO]," 2007, http://www.sintef.no/upload/10977/sluttrapport.pdf.

14. "Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems," 2007, http://www.olf.no/hms/retningslinjer/?50182.pdf.
15. Rich, E., Andersen, D.F., and Richardson, G.P., "OLF IRMA-AMBASEC Group Modeling Report I," University at Albany, Albany, NY 2006.
16. Rich, E., Andersen, D.F., and Richardson, G.P., "OLF IRMA-AMBASEC Group Modeling Report II," University at Albany, Albany, NY 2006.
17. Rich, E. and Gonzalez, J.J., "Maintaining Security and Safety in High-threat in E-operations Transitions," presented at 39th Hawaii International Conference on System Sciences, Hawaii, 2006
18. Rich, E., et al., "Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning," presented at 40th Hawaii International Conference on System Sciences, Hawaii, 2007
19. Sveen, F.O., Rich, E., and Jager, M., "Overcoming organizational challenges to secure knowledge management," Information Systems Frontiers, vol. 9(5), pp. 481-492, 2007.
20. Sveen, F.O., et al., "Toward viable information security reporting systems," Information Management & Computer Security, vol. 15(5), pp. 408-419, 2007.
21. Stouffer, K., Falco, J., and Kent, K., "Guide to SCADA and Industrial Control Systems Security (draft)," NIST Special Publication 800-82 2006, http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf.
22. Klinke, A. and Renn, O., "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies," Risk Analysis, vol. 22(6), pp. 1071-1094, 2002.
23. Argyris, C. and Schön, D.A., Organisational learning II:Theory, method and practice: Addison-Wesley, 1996.