CHECKIT – A Program to Measure and Improve Information Security and Safety Culture

STIG O. JOHNSEN[1]*, CHRISTIAN WAALE HANSEN[2], MARIA BARTNES LINE[1], YNGVE NORDBY[2], ELIOT RICH[3] and YING QIAN[4]

[1]SINTEF, Norway
[2]NTNU
[4] Agder University College, Norway
[3] University of Albany, SUNY

Abstract: Remote IT-based support and operations of offshore oil and gas installations are increasing. The technology used to support operations is changing from proprietary closed process control systems to standardize IT systems, connected to internal networks and the Internet. In addition, a network of companies is increasingly performing operations and management. The standardized PCs using MS Windows have more vulnerability than the proprietary systems used earlier, and the increased connections and participants in the networks increase the vulnerability. This creates the need for improved information security.

Our hypothesis is that an important contribution to improved information security and safety is an improved safety and security culture and improved information sharing during operations and incident handling. Such a safety and security culture should be explicitly directed towards actions that support learning. We have developed a method called CheckIT, consisting of a questionnaire and a process to improve information security and safety culture based on group discussions of key issues. Future work in this area includes refinement of the questionnaire, as well as the use of system simulation to develop a holistic perspective on the causes and outcomes of their security policies.

***Key Words**: Information Security, Safety and Security Culture, SCADA systems, e-Operations, Systems Thinking*

1. Introduction

The amount of e-Operations, i.e. remote operations and remote control of offshore oil and gas installations, is increasing in the North Sea [1]. The main motivations for remote operations are the potential for operational cost reduction and increased income or yield from the fields, together with increased safety. However, initial projects that envisioned quick implementations of remote operations and remote support have not been carried through as easily as expected. Many of the projects have been changed, stopped or delayed significantly because the projects have been more complex and difficult than envisioned.

One of the complexities is related to the effect of e-Operations on security[1] and safety of the actual Operations. The technology used in process control systems (PCS) and

[1] By the term *security*, we mean *information security (IS)* throughout the paper.

supervisory control and data acquisition (SCADA) systems is changing from proprietary closed systems to standardized IT systems integrated in networks that may be connected to internal networks and to the Internet. Such changes must be reviewed quite carefully for their effects. For example, one important safety barrier are the emergency shutdown systems (ESD), ensuring that the operations are closed down in a safe manner. If the connection between the ESD and PCS is not safe and secure, an incident could impact the operation of the ESD system and thus platform safety.

E-Operations are also critical for the planned development of a virtual organization of suppliers, providing flexibility and economy to the industry. Several tasks in operations and maintenance are already performed outside of the operator's organization. Increased use of suppliers and the required inter-connectivity leads to a network of actors, which by accident, negligence or purpose can inflict unwanted incidents or accident on an operator, causing large economic loss.

Exploitation of vulnerabilities may lead to a production stop on an oil platform, with a financial loss in the order 3-5 Million-5 USD per day.

Traditionally, there has been the impression that PCS and SCADA systems were sheltered from the vulnerabilities related to the Internet, and this perception still seems to be widespread. These types of incidents and attacks is seldom reported and shared systematically. The British Columbia Institute of Technology has established an Industrial Security Incident Database (ISID), documenting an increase in attacks on SCADA systems, ref [2].

Personnel involved in e-Operations projects have a tendency to focus on technology, often at the expense of organisational and cultural issues. The reliance on virtual organisations and the increased number of vulnerabilities create the need for common risk perceptions and a common security and safety culture among several organisations to reduce the risk associated with remote operations. A discussion of these issues can be found in [3].

Based on studies and interviews conducted with major operators within the oil and gas industry on the Norwegian Continental Shelf (NCS), this paper identifies major challenges and proposes solutions related to measurement and improvement of security and safety culture, and subsequently improvement of security and safety through the use of CheckIT, a method to identify and focus attention on vulnerabilities and their effects.

1.1 Definitions

The following definitions apply to this document:

Remote control: Part of the operation is managed and operated from other places. This can cover a wide spectrum of possibilities, from control of parts of the process in a normal situation to total control of the installation in an emergency situation. Central control room operators are present at the installation.

Remote operations: The entire process is managed and operated from other places. This is the situation for the unmanned installations where all the control room functions and other operation functions are executed from a remote location. Today, this is the case for sub-sea installations.

Safety and security culture: The safety and security culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine commitment to, and the style and proficiency of, an organisation's health, safety and security management [4].

Virtual organisation: A virtual organisation is a group of people from different organisations located at different geographical locations working together in shared interdependent processes to achieve shared objectives within a defined timeframe. The authority and roles of the participants are clearly defined, ref [5].

2. Key challenges

Our studies and interviews have identified several key challenges related to e-Operations in the oil and gas industry. These challenges have also recently been supported by [6]. One challenge is that proprietary and closed control systems are replaced by standardized ICT systems based on PCs and COTS such as MS Windows connected to internal networks and Internet. CERT/CC publishes quarterly statistics at http://www.cert.org/stats/, reporting vulnerabilities in the IT systems. It was reported 22,716 vulnerabilities in the period 1995-2005, many caused by MS Windows. Based on the increasing reliance of Windows-based technology for control systems, we assert that their vulnerabilities have also increased as proprietary operating systems are replaced.

The awareness of these security vulnerabilities has not equally increased among the different professionals. There is a gap in experience and knowledge between the control automation profession and the ICT profession related to the new ICT vulnerabilities. Outsourcing and the use of multiple suppliers for platforms have increased. The need for communication and problem solving between different groups in different organisations are increasing. A focus on culture among these different groups can ensure that different professions and organisations share a common understanding of the new risks and can cooperate to improve communication and resolve incidents.

We have seen that there is a relationship between safety and safety culture. In [7], it was demonstrated a positive correlation between good safety culture and high safety. Based on the preceding points, we suggest that improvement of culture could be an important step to reduce the risk of e-Operations. Thus, developing a tool for the improvement of safety and security culture should be explored and CheckIT is a result of this work. But using a broad concept such as culture to establish common understanding is a challenge in a technology driven environment such as the oil and gas industry. The industry has a strong focus on technology and issues related to human factors and organisation is often prioritised after the technological issues.

3. Organisational Culture

American pragmatists and consultants primarily used the notion of "culture" in an organisational context in the early 1980s. The cultural metaphor was borrowed from anthropology; as it became obvious that organisations, just as nations and tribes, develop unique language, behaviour and perceptions of the world [8], [9]. Safety and security culture is a hot topic in safety work, but also one, which creates confusion, see [10].

We view culture as a property of collectives – e.g. groups, organisations or communities. Moreover, we emphasize action and interaction rather than theoretical constructs such as attitudes and values. This focus approaches Argyris and Schön's notion of *theories-in-use* – i.e. the values and principles that are reflected in actual actions, as opposed to the values and principles that are claimed (*espoused theory*) [11].

Two main approaches to organisational culture are evident in the literature and among practitioners: the functionalist approach and the symbolic/interpretive approach. Within the functionalist approach, there is a focus on improvement and the links between financial performance and culture. Within the symbolic approach, the focus is on description, and the notion of culture is used to describe and understand organisational life.

Our assumption in this paper is that culture indeed can be measured, managed and manipulated. But at the same time we have been influenced by the symbolic tradition, in that culture is difficult to change and that actors within the culture itself must participate in the change process. Thus triangulation has been our approach in that we have combined the best from the functionalistic tradition with the best from the symbolic tradition.

In 1986, Shell International Exploration and Production started sponsoring a research program to better understand why accidents occur. This resulted in Hearts and Minds [12], a tool for analyzing and improving safety culture. The Hearts and Minds program is influenced by previous work of Westrum [13], who has defined an evolutionary model comprising different levels of safety cultures.

4. CHECKIT

The Hearts and Minds project of Shell has been an inspiration for us when developing CheckIT. The aim of CheckIT is to assist oil and gas companies and other actors in identifying and solving security and safety problems that arise in a network of cooperating companies performing e-Operations. Our experience suggests that the method can also help actors to exploit the opportunity to share best practices and thus improve operations.

4.1 The development of CheckIT

Our approach in the development of CheckIT has been iterative. Feedback from participating organisations and workforce has been stressed.

Initially, a literature review of safety culture, high reliability organisations and other relevant topics was performed. The aim was to identify important issues related to safety and security culture, in order to specify relevant questions and processes to assess and improve the safety and security culture. Important aspects from [10], [12], [14] and [15] have served as a foundation for the succeeding work. Based on the work of [7] and [16] we identified issues that show a clear correlation between good safety and security culture and operational safety and security.

Based on the theoretical foundation, a tentative version was developed and distributed to participating organisations for review and comments. The method was subsequently discussed and adjusted with relevant industry experts in a workshop in 2005. At the same time we agreed on indicators that characterize IT safety and security. These indicators can be used as a baseline to discuss changes or improvement. The industry experts involved were from the oil and gas industry, the telecom industry, the research/consultancy fields and authorities (the Norwegian National Security Authority).

The first version of CheckIT has been used in the oil and gas industry and among other industry participants. We plan to improve the tool based on the experience gathered during its use, and follow-up with participants to determine its effectiveness.

We plan to explore the effect of using CheckIT periodically over a period of 2-3 years. Shell has experienced improvements in safety culture and safety in the years since their research started in 1986, see [12] and the goal with CheckIT is to achieve effects corresponding to these results.

4.2 The foundation of CheckIT

CheckIT has been based on organisational culture [8]. The framework for cultural assessment draws on Westrum's taxonomy of organisational cultures [13]. A possible development of safety and security culture from "bad" to "good" (i.e. from the pathological culture to the generative culture) is described and we have described three alternative examples of responses for each question. The alternatives correspond to the cultural levels in Westrum's work. This has been done to improve understanding and commitment to the use of culture as a concept. We also have tried to suggest that the "best" culture is the learning culture (the generative culture).

The levels of safety culture from Westrum are:

- *The pathological/denial culture* – organisations that fit this characteristic are self organized on a basic level and strive to maintain status quo. They will deny warning signals, punish those who bring them up and try to keep reporting at a minimum. Their focus is on doing business and maintaining the impression of everything being as normal.
- *The calculative/rule based culture* – These organisations are strongly rule oriented, and driven by management systems. They put great effort into forming and imposing rules, which are intended to cover both unwanted situations and external requirements. They have a limited repertoire of measures when an event occurs, and focus is mainly on simple deviation handling.
- *The generative/ learning culture* – organisations that are generative put great effort into active participation on all levels, and align organisational goals with safety oriented goals. They perceive safety and security as an opportunity and an inherent part of the business, rather than an imposition of costs. The company's own and other companies' experiences are actively used to continuously improve the safety performance. Attainment of this level is suggested as the goal in CheckIT.

A key foundation of CheckIT is the ability to exploit and try to influence (and change) fundamental values or root causes by establishing meeting arenas where double loop learning and organisational development can be performed as described in [11]. Through group discussions, root causes should be identified and the participants should be able to suggest changes and improvements in a meeting arena where the important actors are present. In this context, we apply the three-level model from [8] to describe the different levels within the organisation, i.e. artefacts, espoused values and underlying assumptions. CheckIT has an explicit focus on the top two levels of this model. The group process is important in that it can influence the basic assumptions of the organisation if double-loop learning is achieved. Double loop learning is achieved when we manage to change underlying values or common perceptions in the firm, as described in [11].

To establish discussion of underlying values it may be important to involve external participants in the process. External observers could more easily identify underlying values in a group discussion. To further aid in this discussion, scenario analyses of safety critical operations could be performed ref [17]. To analyze the different scenarios, it is suggested to use different accident investigation tools to aid in creating common mental models. The STEP method, see [18] or AcciMap method, see [19], could be useful.

We also assume that the culture may be influenced by sustained changes to routines and behaviour. This corresponds to the views on cultural change presented in [9], where cultural change is an effect of altered patterns of interaction and behaviour.

5. Overview of CheckIT

The basic package of CheckIT comprises of 31 questions. These questions are recommended, and constitute a minimum in the method. Additionally, 34 questions are provided in a supplementary package, which allows the user to configure the survey according to the specific needs of the organisation.

Each question is presented in a short and precise manner, and three alternative main answers are presented in a table next to the question. The aim is to develop a rating of the organisation on a numerical scale from 1 to 5, where alternatives one, three and five are textually described. The alternatives that are described correspond to the cultural taxonomy described by Westrum [13]. The utilization of a five-point scale provides a basis for a normalized score throughout the organisation and makes it possible to compare results and also benchmark against other organisations.

SINTEF has developed a similar tool to improve safety culture at interfaces, a project done for UIC (Union International de Chemin de Fer) [20], [17]. The tool SafeCulture is recommended by UIC and can be found at Railway Safety and Standards Board, UK [21].

5.1 The questions in CheckIT

Generally, the topics covered by CheckIT have been based on the following sources:

- Topics uncovered during the literature review with theoretical basis
- Root causes identified in accident analysis of relevant incidents
- Areas of special interest or focus from participating organisations

Many of the questions are based on work within the field of safety culture and high reliability organisations (HRO); [12], [14] and [15] have all had influence. Central topics include management involvement, establishing clear responsibilities, establishing a common risk perception, common manners of communication, and trying to build a common understanding. A focus on error free communication may have a positive influence on these aspects [15].

The reporting of incidents and learning from these are also integral parts in building a good information security and safety culture. This implies that there is an open reporting culture, facilitating an open discussion between the staff and management. The learning aspect also focuses on system insight. A reporting culture and open learning from incidents is a fundamental basis to be able to perform double-loop learning both within the organisation and among the industry.

The examples and descriptions in each question have been developed, tested and verified trough interviews and workshops and seem to represent best practice.

5.2Implementing and using CheckIT

The implementation and use of CheckIT in an existing organisation or in a network of organisation could be seen as implementing a fundamental change of the way things are done. To ensure that such a change can take place, we suggest following the best practices related to leading change as described by Kotter in [22], e.g.:

- Establish a sense of urgency among the participants in the organisation and in the cooperating organisations.
- Creating a Coalition, involving management and key stakeholders
- Developing a motivating vision that is relevant to the actual business and Communicating the change vision to empower broad-based actions
- Generating short-term wins, document the benefits, consolidating the gains and producing more change and anchoring new approach in the culture

The improvement of a complex concept such as culture could be a challenge. We have developed the tool to be subject of discussions, learning and understanding among broad base of participants. The suggested approach includes the following steps (Figure 1):

- *1. Identify key indicators.* Identify goals and key indicators to be improved by the use of CheckIT. A key indicator could be the number of security incidents that penetrates the security barriers. It is important to get management commitment of scope and effort of use of CheckIT. It is important to establish a learning arena among important stakeholders to support organisational learning. Prior to the use the questions should be discussed and adjusted to the vocabulary and terms used in the specific industry.
- *2. Perform assessment of safety and security culture* via the questionnaire to identify challenges. The questionnaire should be filled out individually and then discussed in a group setting. This implies that we view culture as a property of collectives – e.g. groups or organisations – rather than as an attribute of a single individual.
- *3. Reflection in groups:* Discuss and reflect on the answers in a group setting, to identify areas to be improved. During this discussion it is important to try to identify the root causes or fundamental changes to be implemented to improve the key indicators. Management should be a part of the group and key stakeholders outside the organisation that can influence the safety and security should be included.
- *4. Identify and agree on actions* based on good co-opting processes. (The term *co-opting process* is used to describe a decision process involving both management and work force where the issues are discussed freely prior to a decision.) Implement the suggested actions in a good co-opting process.

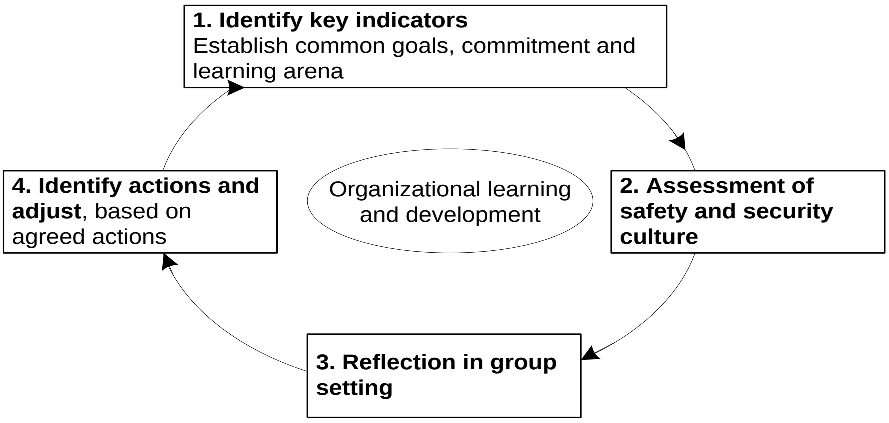

1. Identify key indicators
Establish common goals, commitment and learning arena
2. Assessment of safety and security culture
3. Reflection in group setting
4. Identify actions and adjust, based on agreed actions
Organizational learning and development

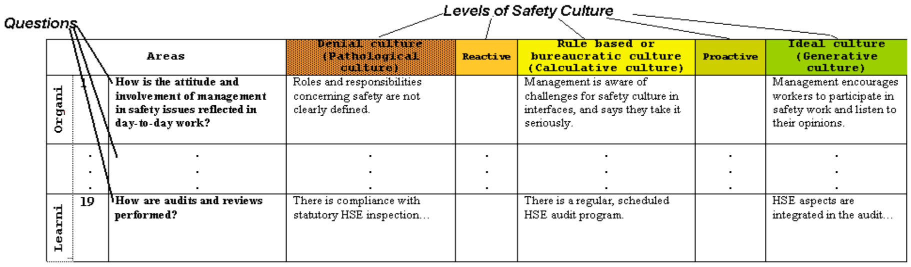
Fig. 1: Suggested approach to foster organisational learning

The assessment of security and safety culture should be carried out by using the questionnaire. For each question there are three described alternatives to be used representing differences in culture. The three described cultural levels are:

- Denial culture (Level 1)
- Rule based culture (Level 3)
- Learning/generative culture, seen as "Best practice" (Level 5)

This assessment should be done in two steps. First, the individual participants are to complete the questionnaire on their own. Then the result should be discussed in the workgroup with relevant stakeholders. If key safety and security operations are outsourced to a service firm, actors from the service firm should participate in the workgroup.

The participants should identify areas to be improved. Reasons to improve the culture are a result that shows that the cultural level is too far from "best practice" or differences in the cultural levels among the actors in the network are significant and may lead to misunderstandings or even an incident or accident. The structure and layout of the questionnaire is illustrated in Figure 2.


Questions
Levels of Safety Culture

		Areas	Denial culture (Pathological culture)	Reactive	Rule based or bureaucratic culture (Calculative culture)	Proactive	Ideal culture (Generative culture)
Organi	1	How is the attitude and involvement of management in safety issues reflected in day-to-day work?	Roles and responsibilities concerning safety are not clearly defined.		Management is aware of challenges for safety culture in interfaces, and says they take it seriously.		Management encourages workers to participate in safety work and listen to their opinions.
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Learni	19	How are audits and reviews performed?	There is compliance with statutory HSE inspection…		There is a regular, scheduled HSE audit program.		HSE aspects are integrated in the audit…

Fig. 2 Layout of the CheckIT questionnaire

The questions to be elaborated are documented in the appendix.

The main activities and resources to be used in a CheckIT analysis are:

- **Preparation and organisation (**½ day) – identify relevant key indicators and identify people to attend the workshop, go trough and adjust the questionnaire to the relevant industry, establish a sponsor from management, motivate and prioritize the work with safety and security, culture.
- **Workshop (**½ day) Assessment and reflection of security and safety culture in a group. Use CheckIT. Identify actions – as agreed in teamwork.
- **Follow-up (**½ day). Document improvements in security and safety culture and Information Safety in general. Document the development of key indicators, discuss the result with the relevant stakeholders.

Improvement of security and safety culture is not an activity that can be done only once; it is a continuous process. We propose that a CheckIT survey should be performed periodically. The development of key indicators should be assessed each period, and the effect of using CheckIT should be assessed. The use of the method does not require many resources but requires management commitment.

6. Key performance indicators

When using CheckIT in an organisation, one should be able to measure the result – to what degree has the security and safety culture actually been improved?

The result from CheckIT itself is a key indicator between 1 and 5, where 5 is the best possible result. We would like to change the actions of the organisation and the employees, not only the perceptions, and thus need additional indicators. The indicators must be identified by the organisation and should represent the most important issues regarding IT security and safety in the organisation. The chosen indicators must be measurable. During our work, we have suggested a set of indicators that can serve as a starting point:

- Consequences of each incident in terms of costs - health and environmental impacts (Should decrease if CheckIT is successful)
- Number of security incidents that penetrates the security barriers (Should decrease)
- Security incidents caused by insiders (Should decrease)
- Time to detection of security incidents (Should be earlier)
- Violations of security procedures/regulations. (Should decrease)

7. Experiences from using CheckIT

Our experiences show that thorough preparations are recommended. One should strive to develop a common understanding among the participants of what CheckIT tries to accomplish and what the results can yield. Important activities are:

- Establishing goals, scope, key indicators and target audiences of the assessment.
- Identify relevant modifications to the tool, e.g. reformulations to match the vocabulary used in the organisation and use a pilot group to test the selected approach
- Making sure leaders have a visible commitment to the survey, being committed to the results and stating the importance of good security and safety culture.

The participants having used CheckIT so far have given a positive assessment of the tool and also identified some challenges and suggestions for improvement. Our experiences indicate that the general coverage of the tool is good. The positive points have been that the participants have evaluated the questionnaire as useful especially since they had to focus on the subject and there has been an increase in awareness and some actual results for improvement in the organisations have been identified. Challenges and suggestions for improvement have been to document that the tool has improved safety and security related to key indicators and to simplify and make the questions relevant to personnel involved in the actual industry.

Some common issues identified by industry partners when using CheckIT has been:

- Suppliers and actors outside the operators are not sufficiently involved in IS.
- Poor handling of information security in large scale projects. Information security is discussed too late in the project phase leading to non-optimal solutions.
- There has not been performed a risk analysis of the ICT systems or the process control systems supporting production.
- The people in operations have not always been informed about unwanted ICT incidents and their consequences. (There is little knowledge about problems.)
- There has been almost no sharing of incident information and best practices.

Experiences from using the tool as an only web based questionnaire without group discussions are positive. This does not yield the benefits regarding double loop learning, but has proven a quick and easy way to identify areas of interest.

CheckIT has also been used in the Telecom industry and in Government and the involved users have been satisfied with the results of using the tool so far. In the National Risk Assessment performed in 2006 by the Norwegian National Security Authority, CheckIT (presented in [23]) was recommended used by organisations for improving security culture. The Telecom provider has used CheckIT in the international organisation, across borders. The results have been useful and during the second half of 2006 there will be performed a statistical evaluation of the result and the impact of CheckIT.

Our experiences are going to be explored in our future work in 2006 and 2007. The initial version of CheckIT has been documented in [24] and [25]. . We are trying to verify and validate the effect of the tool. Ideally there should be an increase in awareness and a decrease of incidents or a reduction of consequences when CheckIT is being used.

8. Areas to Be Explored In The Future and Possible Improvements

Some sort of a scenario analysis could be implemented to ensure better understanding of the challenges related to cooperation across organisational boundaries. In [17] it was documented that the scenario analysis improved understanding in a cross-cultural team. The scenarios should be illustrated by a STEP-diagram, see [18]. To ensure a committed discussion, the scenarios should represent significant areas of concern for the stakeholders. Experience from [26], indicates that scenarios derived from near misses can give a good generic coverage. It is, however, important to update the scenarios to cover new technology, changing regulations and new operational experience. Based on the relevant issues identified by industry partners when using CheckIT, scenarios could be:

- An unwanted incident involving suppliers and actors outside the operator, having different procedures and routines leading to misunderstandings that could escalate.
- Due to a missing risk analysis of the systems there is poor situational awareness of what can go wrong among the different actors. Due to poor situational awareness, an incident is developing into a full-blown incident.
- Due to poor knowledge of unwanted ICT incidents and their consequences, a weakness is exploited at several sites, leading to an unwanted incident.

Implementation of the CHECK-IT survey is more than a spot audit of corporate policies and individual behaviours. It also provides an opportunity to identify why security vulnerabilities persist even when they are known. Recognizing the factors that determine the state of an organization’s security culture may pave the way towards achievable solutions. One way to stimulate this examination is through the use of systems thinking. The systems thinking framework examines organizational behaviours as an outcome of interconnected structures that communicate through information or material feedback loops. These structures work in deliberate or unintentional ways that may achieve the desired objectives, provide limited benefit, or may produce results opposite the original intention [27]

Figure 3 presents a sample causal map that illustrates a common problem in implementing changes to security culture. The state of an organization's security culture at any time may be considered a dynamic balance between the pressure for security compliance and all other functions of the firm. If pressed by events to strengthen its security culture, the gap between the current and desired security culture increases emphasis on compliance, which is expected to improve the security culture, balancing the pressure to change and reducing the gap (Loop B1).[2]

A second and less desirable effect of an attempt to improve the security culture is its effect on productivity. The use of security short cuts (such as sharing of passwords) is a widely practiced activity that operations staff uses to improve productivity at little immediate risk [14]. Security experts recognize that the risk of this behaviour remains largely hidden or ignored until a loss occurs; the effects of the loss on productivity occur when the loss is exposed.

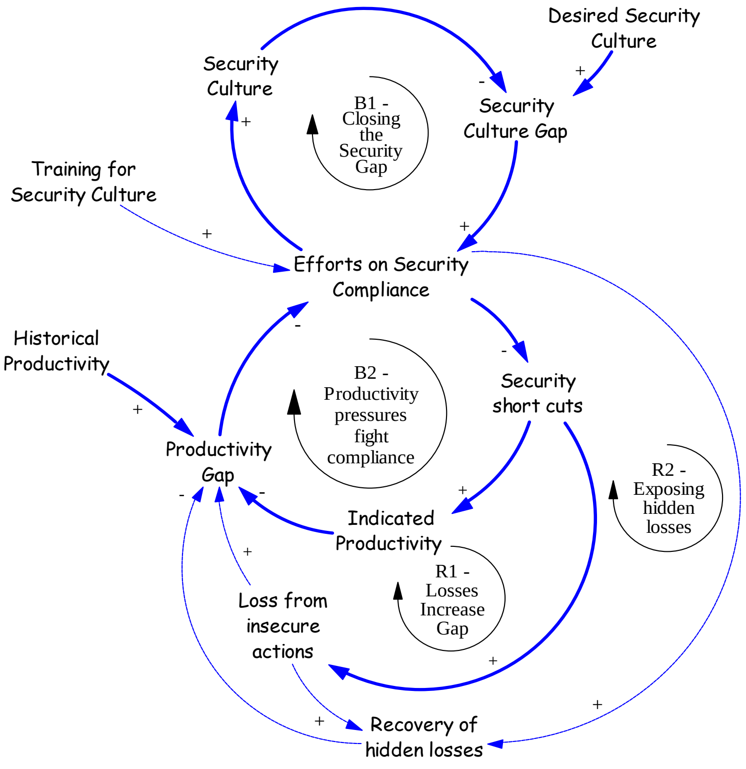

Desired Security Culture
Security Culture
B1 - Closing the Security Gap
Security Culture Gap
Training for Security Culture
Efforts on Security Compliance
Historical Productivity
B2 - Productivity pressures fight compliance
Security short cuts
Productivity Gap
R2 - Exposing hidden losses
Indicated Productivity
R1 - Losses Increase Gap
Loss from insecure actions
Recovery of hidden losses

Fig. 3 Feedback Model of Resistance to Security Culture

Increased security compliance discourages the sharing of passwords. In the minds of the staff, though, enforcement of a stronger password regimen would be

[2] In systems thinking, a loop that reduces the effects of imposed pressure is termed balancing; a loop that increases its effects in response to a change is termed reinforcing. Reinforcing loops may act in vicious or virtuous ways. See [28], chapter 4, for a discussion of these principles.

anticipated to reduce indicated productivity. This in turn would create another gap, one between perceived productivity and its historical levels. Production pressure might well be expected to reduce security compliance in another area, thus reducing the effect of the drive to improve security practices (Loop B2) as well as stimulating the search for additional security shortcuts, which increase hidden losses and widen the security gap (Loop R1).

This hypothetical causal model, though quite simple, does illustrate the value of a systems perspective on security compliance. The effects of Loops B1 and R1 that work against the desired increase in compliance are an unintentional consequence [29] of a system that focuses on perceptions of productivity without consideration of longer-term risks. A solution in this case might be security training exposing the effect and risk of hidden losses to the organization from insecure actions that – now or in the future – could have a dramatic effect on the firm's productivity and financial status. Recovery of those losses might be sufficient to counter concerns about short-term productivity losses, and reinforce the security efforts, leaving the firm in a stronger position over time (Loop R2).

A causal model provides one framework for analyzing the results of a CHECK-IT program and creating an action plan for cultural change. Our example provides some basis for organizing thinking about what truly influences security behaviours in organizations. This first model provides only limited value, in that it is not possible to tell which effect dominates the system: Our next step in this section of the analysis is the development of a formal simulation model, which will attempt to address these and other questions.

9. Conclusion

E-Operations may cause increased vulnerability within the oil and gas industry, this is supported research in USA by Homeland Security and the I3P consortium, see [6] and [30]. E-Operations create the need for building and continuously improving a culture for security and safety. We have developed a method, CheckIT, which may be used for the assessment and improvement of security and safety culture. Further work includes applying CheckIT to selected companies interested in working with safety and security culture. We would like to explore the theory in [31] to improve CheckIT. We are also developing system simulation tools to examine the effects and barriers to change that may emerge over time. CheckIT has freely been made available at www.checkit.sintef.no.

Acknowledgments:

The Research Council and The Oil Industry Association in Norway funded this work.

References

[1] OLF - Norwegian Oil Industry Association. (2004). Integrated Operations on NCS. Avaialble at http://www.olf.no/?22894.pdf

[2] Byres, E., *Process Control/Security testing of process control systems,* Presentation held at SPE Digital Oil and Gas Security event, Dec 8-9 2005.

[3] Johnsen, S.O.,Line, *Towards more secure virtual organisations by implementing a common scheme for incident responset,* PSAM8 in 2006, ISBN: 0-7918-0245-0.

[4] ACSN (1993) Third report of the Advisory Committee on the Safety of Nuclear Installations - *Organizing for Safety*, 1993 - ISBN 0-11-882104-0.

[5] Johnsen, S. O., A. Askildsen, K. Hunnes, *Challenges in remote control and co-operation of offshore oil and gas installations*, ESREL 2005, ISBN 0-415-38340-4.

[6] McIntyre, A., A. Lanzone, J. Stamp, *I3P Preliminary Risk Characterization Repor*t, I3P Research Report; no. 6, Sandia , March 13, 2006. At http://www.thei3p.org/

[7] Silva, S., and M. L. Lima, *Safety as an organisational value: Improving safety practices and learning from accidents*, ESREL 2005, ISBN 0-415-38340-4.

[8] Schein, E. H, *Organisational Culture and Leadership*, Jossey-Bass, 1992

[9] Rosness R., *Safety Culture: Yet another buzzword to hide our confusion?* Internal SINTEF-paper 2001, available at: www.risikoforsk.no

[10] Hale, A., *Editorial – Culture's confusion*, Safety Science, Vol. 34, pp. 1-14, 2000.

[11] Argyris, C. and D. Schon, *Organisational learning II:*-Wesley, 1996.

[12] Hudson, P. and G. C. van der Graaf, *Hearts and Minds: The status after 15 years Research*, Society of Petroleum Engineers (SPE 73941) Kuala Lumpur 2002.

[13] Westrum R.J: *Cultures with Requisite Imagination*, in: Wise, Stager and Hopkin (Eds.) *Verification and Validation of Complex Systems*, Springer, Heidelberg (1993).

[14] Reason, J. *Managing the Risk of Organisational Accidents*, Ashgate, 1997

[15] LaPorte T.R. and Consolini, *Working in practice but not in theory: theoretical challenges of high reliability organisations*, Journal of Public Administration 1991.

[16] Itoh, Andersen, Seki (2004), *Track maintenance train operators' attitudes to job, organisation and management and their correlation with accident/incident rate*, Cognition, Technology and Work, Vol. 6(2), pp. 63-78.

[17] Johnsen, et al, *Cross border railway operations: Building safety at cultural interfaces*, Cognition, Technology & Work, Springer ISSN: 1435-5558 (Paper)

[18] Hendrick, K., L. Benner, *Investigating accidents with STEP*, NY Dekker 1987.

[19] Rasmussen, J., I. Svedung, *Proactive Risk management in a dynamic society, 2000.*

[20] Johnsen S.O et al., *The Track to Safety Culture (SafeTrack), a toolkit for operability analysis of cross border rail traffic*, Sintef STF38 A04414, ISBN 82-14-02731-4.

[21] Railway Safety and Standards Board (RSSB), United Kingdom, project T143: http://www.rssb.co.uk/allsearch.asp?Ord=complete#pop

[22] Kotter, J.P., *Leading Change*, Harvard Business School Press, 1996.

[23] Nordby, Y.,C. W. Hansen , *Informasjonssikkerhet - atferd, holdninger og kultur*, (in Norwegian), Tapir, Trondheim, 2005, ISBN 82-7706-222-2

[24] Johnsen, S. O., C. W. Hansen, Y. Nordby, and M. B. Line, *Measurement and improvement of information security culture*, 2005 HKARMS ISBN 962-442-279-6.

[25] Johnsen, S. O., Hansen, Nordby, Line, *Check-It - Measurement and Improvement of Information Security and Safety Culture*, PSAM8 in 2006, ISBN: 0-7918-0245-0.

[26] Tinmannsvik, R., and R. Rosness, *From Incidents to Proactive Actions: A Bottom-Up Approach to Identification of Safety Critical Functions* ESREL/PSAM 2004.

[27] Senge, P. M.,*The fifth discipline: The art & practice of the learning organization*. New York: Doubleday, 1990.

[28] Sterman J.,*Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill/Irwin; 1 edition (February 23, 2000) ISBN: 007238915X

[29] Wolstenholme, E., *Using generic system archetypes to support thinking and modeling*. System Dynamics Review, Vol. *20*, pp. 341-356, 2004.

[30] Eisenhauer, J., P. Donnelly, M. Ellis, M. O'Brien, *The Roadmap to Secure Control Systems in the Energy Sector*, January 2006, At http://www.controlsystemsroadmap.net/

[31] Weick, K.E., and K. M. Sutcliffe, *Managing the unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass (Wiley) San Francisco, 2001.

Stig O. Johnsen is a senior researcher at SINTEF in Trondheim/Norway, department of Science and Technology/Safety and Reliability - closely cooperating with NTNU (Norwegian University of Science and Technology).

Appendix A: Questionnaire – some of the questions having been developed

Questions	Employees / Managers	Question:	1)**Denial culture (Level 1)**	Level 2	3)**Rule based culture (Level 3)**	Level 4	5)**Proactive /Generative culture (Seen as “Best practice” – Level 5)**
1	E/M	To what extent is senior management involved and committed to information security?	1-The management does not focus on information security and employees are given little information regarding this.	2	3-The management focus on information security, when there is an occurrence of an incident. They inform the employees, but there is one-way communication.	4	5-The management continuously focus on information security. There is a two-way communication with employees and partners regarding information security.
2	E/M	To what extent are employees and suppliers involved in developing information security?	The management and those responsible for the information security develop and decide the requirements and routines for information security without involving the employees or suppliers.		The management when developing the routines for information security uses report and suggestions from the employees and suppliers.		Employees and suppliers are directly involved in the process of developing procedures for information security and they are considered an important resource in this work. Some employees have been given responsibility regarding information security.

3	E/M	To what extent are rules and procedures continuously adjusted to reduce the risks related to information technology?	The companies make safety procedures when required by authorities. Rules are used by management to keep a retreat open, and in that way disclaim responsibility when accidents occur. Rules are not always used to increase safety, but also used politically.		There are many procedures, serving as ‘barriers’ to prevent incidents. The stringency of the rules is at the minimum required by authorities. Procedures are adjusted or “bent” to enable quick fixes or do the job faster.		Procedures are seen as an opportunity to improve the safety and security, and they are continuously refined in order to make them more practical. Common procedures are used cross interfaces, and are developed in cooperation with other organisations.
4	M	To what extent are unwanted incidents analyzed and used as a learning experience?	Unwanted incidents are rarely investigated. Only serious incidents with large potential loss are investigated.		The incident is analyzed to establish new routines in order to avoid such incidents in the future. Little are being done to investigate the root cause of the incident.		The incident is used as a learning opportunity. The organisation as a whole is trying to learn from the incident. Management and employees are discussing the incident in a meeting arena where ideas and experience can be exchanged.
5	E/M	To what extent are reporting of unwanted incidents appreciated?	There is no feedback, and I don’t know if anything has been done to improve what I reported. I usually prefer to solve the problem by myself. I never get feedback if I report an unwanted incident.		I only report incidents if they are serious and may have direct consequences for my work. I report to my superior and he/she report back to me that my report has been received and that someone will take care of the problem.		I know to whom I shall report and that all reports of unwanted incidents are taken seriously. I will be informed if action is taken to solve what I reported. I always report unwanted incidents regarding information security.
6	E/M	To what extent are individuals blamed if an accident or unwanted incidents occurs?	Individuals or partners are blamed in the case of unwanted incidents regarding information security.		A combination of technical and personal factors is seen as the reason for the occurrence of unwanted incidents. The system as		Who to blame is rarely an issue in such incidents. Individuals or partners are therefore rarely blamed.

					a whole is often blamed.		
7	M	To what extent are experience transferred between your company and other companies?	Few experiences are shared with other companies. Information security is regarded as an internal affair in the company.		There is little focus on measuring information security for comparison with other companies.		The company a part of a network for information security in order to learn from other companies' practice regarding information security.
8	M	How is experience feedback used in the organisation?	Many incidents are not reported. A database of serious incidents reports exists but it is incomplete and not considered being useful. The system does not have open access. Management is not informed about serious incidents.		There is a database with detailed descriptions of near incidents and incidents, which is used internally. Efforts are made to use it actively, but it is not yet fully established as a useful tool.		The company's own and other companies' experiences are actively used to continuously improve our own safety and security performance as well as the industry as a whole. Interfaces are seen as an important learning arena. Simulators are used as a training tool to gain experiences cross interfaces and create understanding.
Last	E/M	What is your opinion of this questionnaire?	Time consuming, unnecessary and not relevant.		OK. Not very interesting, but I did learn something from it.		Interesting. It made me see a new perspective and I gained knowledge.